Oracle® Audit Vault

Administrator's Guide

10*g* Release 2 (10.2.2)

B25321-02

August 2007

Oracle Audit Vault Administrator's Guide, 10*g* Release 2 (10.2.2)

B25321-02

Primary Author: Rod Ward

Contributing Author: Tsun-tsun Ho, K. Karun, Harish Butani, Jack Brinson, Srividya Tata, Janaki Narasinghanallur, Vipul Shah, Tammy Bednar, Janet Blowney

Contributor: Donna Keesling, Dongwon Park, Valarie Moore

Contents

4 Configuring and Managing Audit Vault

5 Administrative Tasks

6 Troubleshooting an Audit Vault System

A Audit Vault Configuration Assistant (AVCA) Reference

B Audit Vault Control (AVCTL) Reference

C Audit Vault Oracle Database (AVORCLDB) Reference

D REDO Collector Database Reference

E Audit Vault Error Messages

Glossary

Index

List of Examples

List of Figures

List of Tables

Preface

Oracle Audit Vault Administrator's Guide provides usage information for Audit Vault administrators who perform administrative tasks on an Audit Vault system.

Audience

This document is intended for Oracle Audit Vault administrators who perform the following tasks:

- Configure and manage an Audit Vault, including enabling authentication between the Audit Vault Agents and Audit Vault Server, configuring jobs to populate the warehouse, and enabling and disabling alerts.
- Configure and manage audit data sources across the enterprise for audit data consolidation.
- Configure and manage Audit Vault audit data collectors and their agents to collect audit data across the enterprise from Oracle Database sources.
- Monitor a running Audit Vault system, troubleshoot problems, and maintain all operational aspects of the Audit Vault system.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following documents in the Oracle Audit Vault release 10.2.2 documentation set (see also the platform-specific Audit Vault Server installation guides) or in the Oracle Database 10*g* release 2 (10.2) documentation set:

- *Oracle Audit Vault Server Installation Guide for Linux x86*
- *Oracle Audit Vault Agent Installation Guide*
- *Oracle Audit Vault Licensing Information*
- *Oracle Audit Vault Developer's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Database Vault Administrator's Guide*
- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle Data Guard Concepts and Administration*
- *Oracle Database Administrator's Guide*
- *Oracle Database Concepts*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction to Oracle Audit Vault

Oracle Audit Vault is a powerful enterprisewide audit solution that efficiently consolidates, detects, monitors, alerts, and reports on audit data for security auditing and compliance. Oracle Audit Vault provides the ability to consolidate audit data and critical events into a centralized and secure audit warehouse.

Why Use Oracle Audit Vault?

Compliance regulations and legislation such as the U.S. Sarbanes-Oxley Act (SOX), U.S. Gramm-Leach-Bliley Act (GLBA), U.S. Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Data Security Standard, Japan privacy laws, and European Union privacy directives require businesses to secure business and personal data related to customers, employees, and partners, and to demonstrate compliance with these regulations by auditing users, activities, and associated data.

Businesses use a wide variety of systems, databases, and applications that produce vast quantities of audit log data. Businesses must consolidate and monitor this data for a holistic view of enterprise data access. Auditors must analyze the audit log data in a timely fashion across disparate and heterogeneous systems. To facilitate the process, it is essential that audit data from all systems reside in a single audit data warehouse that is secure, scalable, reliable, and highly available.

Oracle Audit Vault solves these security and audit problems by:

- Consolidating audit information from multiple systems across the enterprise
- Detecting data changes associated with regular and privileged users
- Protecting audit data from modification and tampering

1.1 Overview of Oracle Audit Vault

Historically, audit data has resided in silo across the enterprise with the possibility that the powerful system users can tamper with the audit data. Audit data can be a strong deterrent to information theft, unauthorized access, and tampering if it can be securely collected and consolidated from multiple databases and sources to generate the required compliance and security audit reports. Oracle Audit Vault enables organizations to collect and consolidate audit data from multiple sources, store it in a secure audit warehouse, detect conditions of interest, and produce reports.

Auditing plays a key part in protecting sensitive business information. Tackling the compliance and security challenges requires an enterprise audit solution. Audit trails in the enterprise must be consolidated into an enterprisewide audit trail. In this regard, Oracle Audit Vault accomplishes the following:

- Consolidates audit trails by mapping various audit data to a common audit format
- Secures all audit data across the enterprise
- Offers centralized audit policy management
- Enables analysis of audit data, including timely detection of violations
- Facilitates regulatory compliance

Oracle Audit Vault provides the mechanisms to collect audit data. Oracle Audit Vault supports the collection of audit data generated by Oracle9*i* Database release 2, Oracle Database 10*g* release 1, and Oracle Database 10*g* release 2. The audit data can be collected from the Oracle Database audit trail tables, database operating system audit files, and database redo logs to capture before or after value changes.

The consolidation of audit trails and audit data enables the provision of value-added audit services for all systems in the enterprise in a consistent manner. It also enables enterprisewide capabilities that are impossible or very difficult to provide without a consolidated audit solution.

The increasingly sophisticated nature of information theft and insider security threats requires businesses to not only protect sensitive information, but also monitor access to sensitive information by privileged and powerful users (such as database administrators (DBAs), developers, and managers). As privileged users have ongoing and direct access to sensitive data, it is critical to implement monitoring controls to ensure compliance.

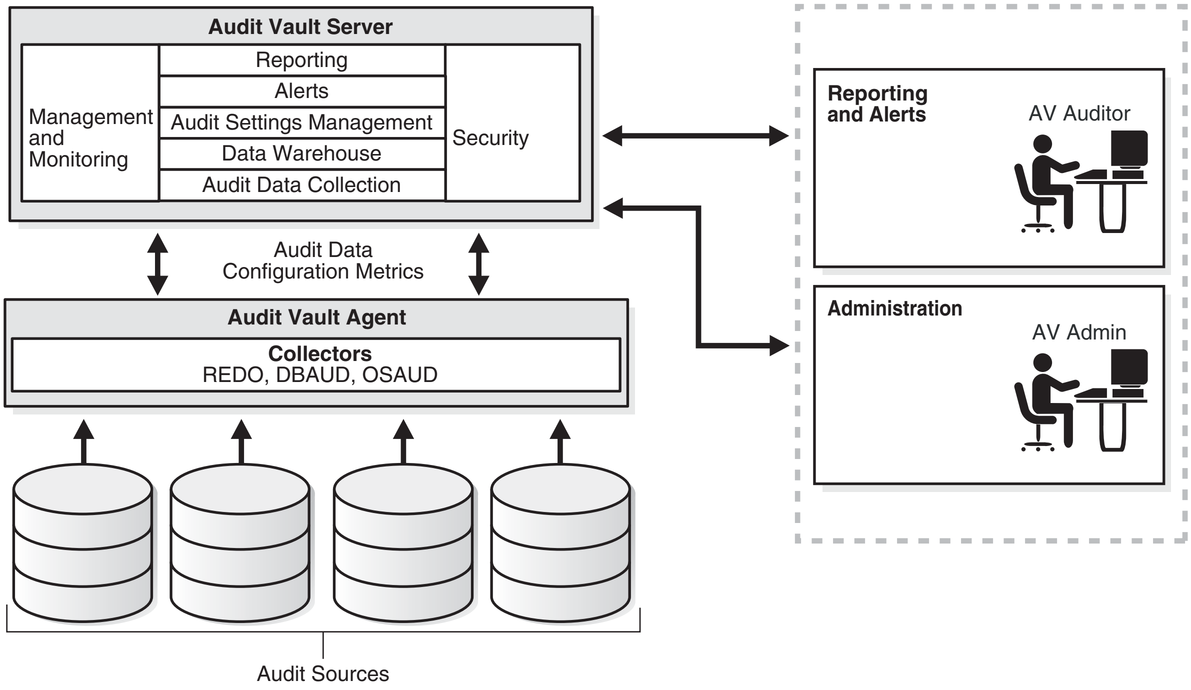
Oracle Audit Vault provides valuable insight into who did what, to which data, and when, including privileged users who have direct access to the database. Understanding who accessed, altered, updated, deleted, or merely viewed sensitive data is essential to protecting data and satisfying compliance requirements. Oracle Audit Vault provides the capability to detect, monitor, alert, and report the history of privileged user changes, schema modifications, and even data-level access. Audit policies and settings can be defined and managed from Oracle Audit Vault for the audit sources throughout the enterprise. In addition to improving security, centralized audit policy management reduces the cost and complexity of auditing across the business.

Oracle Audit Vault can be configured to provide alerts relating to suspicious activities. It provides an alert management capability to mitigate the insider security threat. It can generate alerts for system-defined events and user-defined events when they occur. For instance, an alert can be sent whenever a privileged user creates a user without permission or attempts to view sensitive data. Oracle Audit Vault continuously monitors the data collected, and generates alerts for any anomalies or abnormal activities.

1.2 Oracle Audit Vault Architecture

Figure 1–1 shows an overview of the Oracle Audit Vault architecture. The architecture consists of a set of services and its collection system working within an enterprise. This set of services helps to facilitate storage management, policy enforcement, alerting, analysis, reporting, and activities. The collection infrastructure enables the utilization of audit collectors that function as adaptors between an audit source and Oracle Audit Vault Server.

Figure 1–1 Oracle Audit Vault Architecture Overview



Audit Vault Server consists of:

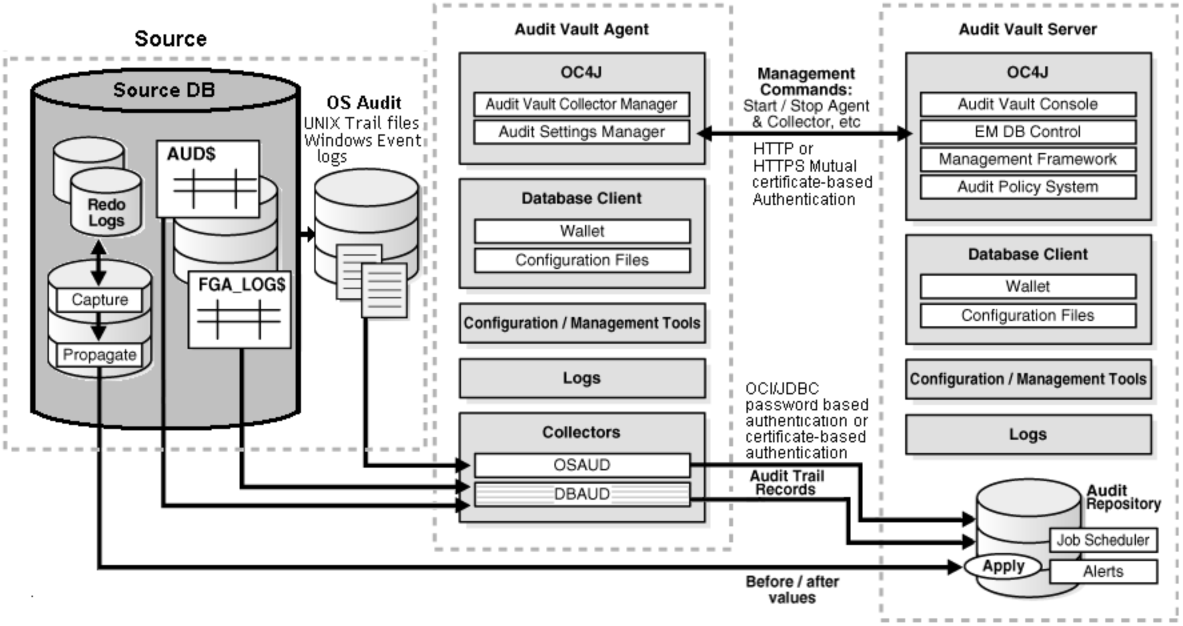
- Audit Data Store
- Audit Vault Console
- The following services:
  - Collector management and monitoring
  - Report management
  - Alert management
  - Audit settings management to establish your policy management
  - Published data warehouse that can be used with reporting tools like Oracle Business Intelligence Publisher to create customized reports
  - Audit data collection and storage management

  Configuration services assist in defining information about what sources are known to Oracle Audit Vault. Oracle Audit Vault stores information (metadata) about the sources of audit data and policy information (database audit settings).

An Audit Vault Agent provides run-time support for audit data collection by Audit Vault collectors. It also contains the audit data collectors for Oracle Database sources. The DBAUD, OSAUD, and REOD collectors are provided.

Figure 1–2 shows a detailed overview of the Oracle Audit Vault architecture for the Audit Vault Server and Audit Vault Agent components. As a source database, audit events captured in audit logs and tables for the Oracle Database are parsed into audit records and sent to the Audit Vault raw audit data store for storage and further analysis within a published data warehouse and from which reports can be generated.

Figure 1–2 Audit Vault Architecture (Detailed View)



Audit Vault Server

Audit Vault Server consists of:

- OC4J: Oracle container for Web applications consisting of:
  - Audit Vault Console – User interface to manage Audit Vault. Reports, Audit Policy Manager, and so forth
  - Oracle Enterprise Manager Database Control console – User interface to manage the raw audit data store or audit repository database
  - Management Framework – Sends management commands to the Audit Vault Agent to start or stop agents and collectors, collect metrics, receive management commands from AVCTL, AVCA, and AVORCLDB command-line interfaces using HTTP protocol or HTTPS mutual certificate-based authentication (see Section 2.1).
  - Audit Policy System – A service to retrieve and provision audit settings on the source; and a system to create and manage alerts raised by audit events as they are stored in the audit event repository
- Database Client: Infrastructure to communicate to the audit repository, consisting of:
  - Oracle Wallet – Contains credentials to authenticate Audit Vault users
  - Configuration Files – Files used by Audit Vault for networking, preferences, and so forth.
- Configuration and Management Tools – Utilities used to configure and manage Oracle Audit Vault, such as the AVCA, AVCTL, and AVORCLDB command-line utilities. They let you define and configure information about what sources are known to Oracle Audit Vault. Oracle Audit Vault stores information (metadata) about the sources of audit data and policy information (database audit settings and alerts).
- Logs: Informational and error messages for Oracle Audit Vault (see Section 6.1)

- Audit repository: Oracle database to consolidate and manage audit trail records, consisting of:
  - Raw audit data store – A table space with a single data file where audit records are inserted as rows into a set of partitioned tables
  - Warehouse schema – Open schema of normalized audit trail records. This is a published data warehouse that can be used with reporting tools like Oracle Business Intelligence Publisher to create customized reports
  - Job scheduler – Database jobs used to populate and manage the warehouse
  - Alerts – Queue maintains alerts
  - Apply – Process used by the REDO collector to insert before or after values of data

Audit Vault Agents

Audit Vault Agents consists of:

- OC4J: Oracle container for Web applications consisting of:
  - Audit Vault Collector Manager – Receives management commands from Audit Vault Server to start and stop collectors, collect and return metrics, and so forth
  - Audit Settings Manager – Receives commands from Oracle Audit Vault to extract audit settings from a source.
- Database Client: Infrastructure to communicate to the audit repository, consisting of:
  - Oracle Wallet – Contains credentials to authenticate Audit Vault users
  - Configuration Files – Files used by Audit Vault for networking, preferences, and so forth.
- Configuration and Management Tools: Utilities used to configure and manage Audit Vault, such as the AVCA, AVCTL, and AVORCLDB command-line utilities
- Logs: Informational and error messages for Audit Vault (see Section 6.1)
- Collectors: The type of collectors deployed by the Audit Vault Agents include:
  - OSAUD – Collector (for Linux and UNIX platforms) to extract to audit records from the operating system files (audit logs)

    Note: XML files are not supported in the OSAUD collector.

  - OSAUD – Collector (for Windows platforms) to collect audit records from the event logs. This EVTLOG collector type collects audit data only from the source installed on the same system where the Windows agent and this collector type are running.
  - DBAUD – Collector to extract audit records from the Oracle Database SYS.AUD$ dictionary table and SYS.FGA_LOG$ dictionary table
  - REDO – Collector using Oracle Streams technology to retrieve logical change records from the REDO logs

  OSAUD and DBAUD collectors send valid and invalid audit records, get configuration information, get and send recovery context, and send error records using OCCI/JDBC password-based authentication or certificate-based authentication (see Section 2.2).

Audit Vault Source

The audit data source consists of Oracle Database audit trails stored in:

- `SYS.AUD$` dictionary table and `SYS.FGA_LOG$` dictionary table that are collected by the DBAUD collector
- Operating system audit trail files stored on Linux and UNIX-based systems and event logs stored on Windows systems that are collected by the OSAUD collector
- Redo logs containing logical change records of before and after values in which a REDO collector using Oracle Streams technology utilizes a Capture process to read the data and a Propagate process to transmit it.

Oracle Audit Vault Interfaces and Administrator Access

Oracle Audit Vault provides an Audit Vault Console and a set of command-line utilities, the **Audit Vault Configuration Assistant (AVCA)** (see Appendix A), **Audit Vault Control (AVCTL)** (see Appendix B), and **Audit Vault Oracle Database (AVORCLDB)** (see Appendix C) to manage the system. These components provide the ability to manage and monitor agents and collectors, populate the data warehouse, and manage audit data storage.

Auditors, compliance, and information technology (IT) security can use built-in reports based on user access and activity such as failed login attempts, use of system privileges, and changes to database structures. The drill-down capability offered through the Oracle Audit Vault Console provides full visibility into the details of the what, where, when, and who of the audit events. In addition, the Audit Vault Console can be used to monitor the alerts and the audit events across the enterprise.

Audit Vault administrators are assigned different roles and gain access to Oracle Audit Vault to manage various components based on the role assigned. Table 1–1 describes the various Audit Vault administrator roles and the tasks permitted for each role.

Oracle Database Vault is used to protect the audit data warehouse from unauthorized access. See Chapter 2 and *Oracle Database Vault Administrator's Guide* for more information. Oracle Database Vault roles are essential for creating database user accounts and granting roles to Audit Vault administrators.

Table 1–1 Audit Vault Administrator Roles and Their Assigned Tasks

Role	When Is Role Granted?	Role Is Granted to Whom	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. A user is created and granted this role during the Audit Vault Server installation. Only the user granted the `AV_ADMIN` role can grant the appropriate role (`AV_ADMIN`, `AV_AUDITOR`, `AV_AGENT`, or `AV_SOURCE`) to other Audit Vault administrators.
`AV_AUDITOR`	During 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.

Table 1–1 (Cont.) Audit Vault Administrator Roles and Their Assigned Tasks

Role	When Is Role Granted?	Role Is Granted to Whom	Description
AV_AGENT	Before Agent installation	Agent software component	Manages agents and collectors by starting, stopping, and resetting them. 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.
AV_SOURCE	Before source registration	Collector software component	Manages the set up of the sources for audit data collection. A user is created prior to source and collector configuration and granted this role upon adding a source to Audit Vault using the AVORCLDB add_source command. The collector software uses this role at run time to send audit data to Audit Vault.
AV_ARCHIVER	Before archiving audit data	Audit Vault archiver	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	Database Vault owner	Manages Oracle Database Vault roles and configuration.
DV_ACCTMGR	During Server installation	Database Vault account manager	Manages database user accounts.

It is important to protect and ensure the integrity of the audit trail data against modification and tampering. Either external or internal intruders might try to "cover their tracks" by modifying audit trail records. Oracle Audit Vault delivers a "locked-down" audit warehouse that has been designed for the sole purpose of protecting and securing audit data. Access to the Oracle Audit Vault is only allowed for the predefined roles described in Table 1–1. All other roles, including the database administrator (DBA), are denied access to the audit data.

Figure 1–3 shows a detailed view of the various Audit Vault usage scenarios for which each of the Oracle Audit Vault administrator roles described in Table 1–1 plays an important role.

Audit Vault usage scenarios can be grouped as follows:

Monitor, Detect, Alert, and Report Usage Scenario

An auditor (the user granted AV_AUDITOR role) creates, views, and manages both internal and external, detail and summary types of reports for compliance purposes. A security officer inspects and further evaluates system-generated alerts logged to the alerts table raised by events that meet specific alert conditions. An auditor administrator also sets and views Audit Vault audit policies.

Archive Usage Scenario

An audit archiver (the user granted AV_ARCHIVER role) configures and manages the data life cycle to automate audit data life-cycle management on an ongoing basis as part of the archiving operation.

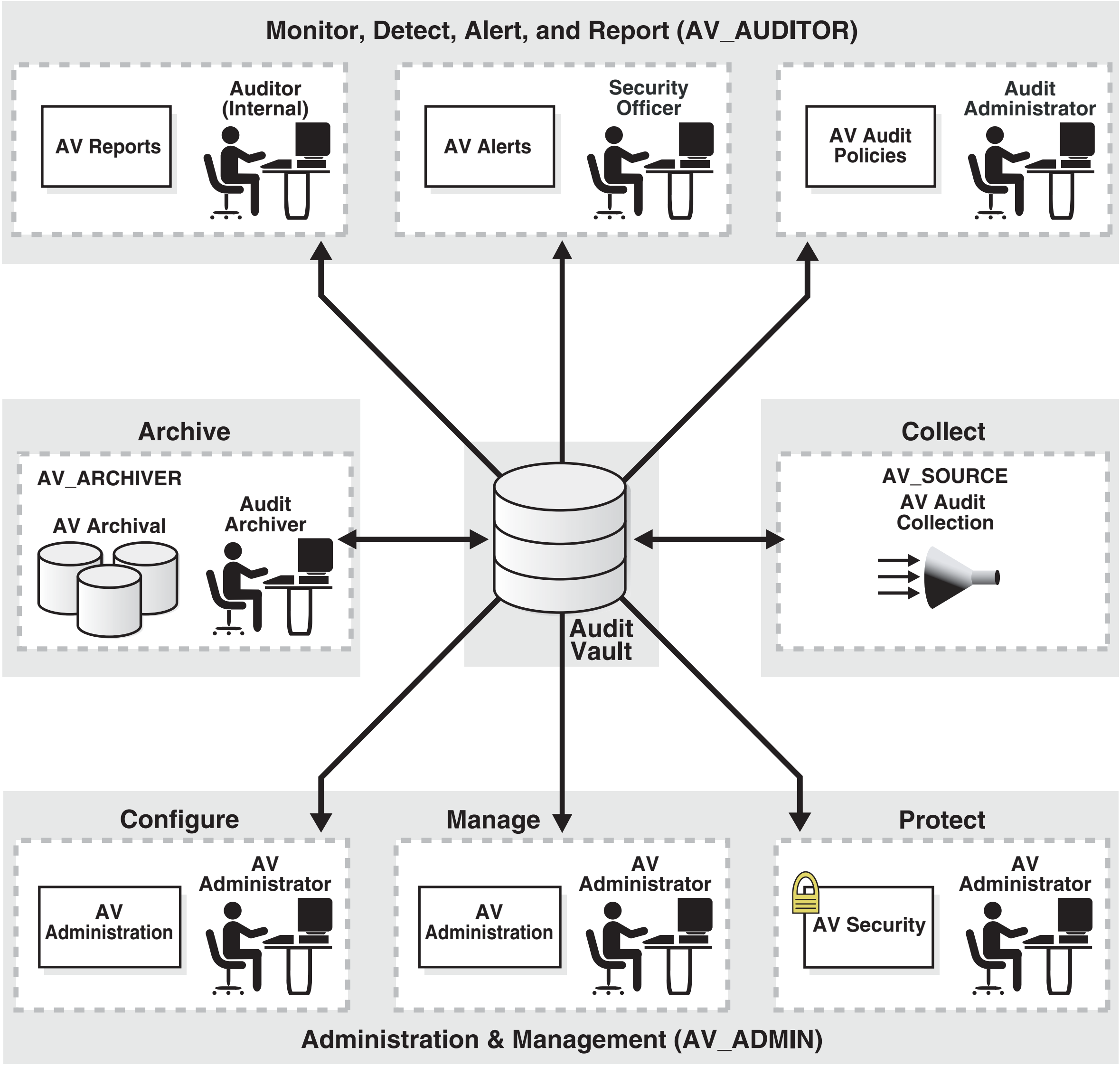
Collect Usage Scenario

A source user must first be created (the user granted AV_SOURCE role) before an Audit Vault administrator (user granted AV_ADMIN role) can add the source and collector to Audit Vault.

Administration and Management Usage Scenario

An Audit Vault administrator (the user granted AV_ADMIN role) oversees the monitoring and management of the audit data consolidation operation. This user also performs audit data collection tasks, configuring collectors (adding sources and collectors) to Oracle Audit Vault. This user monitors overall Oracle Audit Vault system security.

Figure 1–3 Usage Scenario Showing Important Roles of Audit Vault Administrators



1.3 Oracle Audit Vault Agents and Collectors

This section describes Oracle Audit Vault agents and collectors, the audit service, and the types of tasks performed by these services.

Agent – Provides run-time support for audit data collection by Audit Vault collectors. An agent loads the collectors, provides them with a connection to the Audit Vault audit service for sending audit data, handles calls from the Audit Vault management service and routes them to the appropriate collectors, and sends the Audit Vault management service run-time metrics on the collectors.

Collectors – Starts and stops the primary collection component between the audit source and Audit Vault. The collector will read or interpret native log records and send them to Audit Vault through the audit service. On startup or on a reset, the collector reads the audit configuration object provided by the audit service, which contains the recovery information, configuration information, and policy information sent to it from Oracle Audit Vault.

Oracle Audit Vault communicates with the audit data source through its agent. An agent is a program that runs on the Audit Vault Server system, on the system that hosts an audit data source, or on another independent system, and manages audit data collectors on behalf of the Audit Vault Server. Collectors rely on their agent to set up a connection with the Audit Vault service. Agents are also responsible for interacting with the management service to manage and monitor collectors. An agent reads the audit data from the audit data source, parses the data into audit records, and sends it to the raw audit data store within Audit Vault.

The management and monitoring service manages all collectors. It provides the ability to stop and start collectors based on a schedule, and stores metrics for each collector.

1.4 Selecting the Right Collector for Audit Data

Audit Vault implements an Oracle Database source type and three collector types that pull audit data from the database. The source type is called ORCLDB, and the three collector types are called DBAUD, OSAUD, and REDO. Each collector type retrieves audit records from different locations in the source Oracle database (see Figure 1–2). Table 1–2 lists the characteristics of the audit trail locations to help you determine for each Oracle Database source where to write the audit trail and which collector(s) should be deployed to move the audit data into the Audit Vault audit data repository.

Table 1–2 Characteristics of Oracle Database Audit Trail Locations

Audit Operation	Operating System Log	Database Audit Table	Redo Log
Select statements	Yes	Yes	Yes
Data manipulation language (DML)	Yes	Yes	Yes
Data definition language (DDL)	Yes	Yes	Yes
Before and after values	No	No	Yes
Successes and failures	Yes	Yes	No
SQL text	Yes (for SYS)	Yes	No
SYS auditing	Yes	No	Yes
Other considerations	Separation of duties	Fine-grained audit data	Supplemental logging for all values

Table 1–3 shows the audit data sources for the Oracle Database source, the audit settings to initiate Oracle Database auditing, what is being audited, and the collectors that collect this audit data.

Table 1–3 Audit Data Sources for the Oracle Database Source Type

Audit Data Sources of Oracle Database Source Type	Oracle Database Settings to Initiate Auditing	What Is Being Audited	Collector Name
Redo logs	Check output of `AVORCLDB verify` command on REDO collector at the agent for any recommended initialization parameter settings.	Committed data definition language (DDL) and data manipulation language (DML) statements, SYS privilege, before and after values, successes only	REDO

Table 1–3 (Cont.) Audit Data Sources for the Oracle Database Source Type

Audit Data Sources of Oracle Database Source Type	Oracle Database Settings to Initiate Auditing	What Is Being Audited	Collector Name
Database audit trail, where standard audit events are written to the database dictionary table `SYS.AUD$`	Set initialization parameter `audit_trail=db, extended`.	DDL and DML statements, SQL text, successes and failures	DBAUD
Fine-grained audit trail, where audit events are written to the database dictionary table `SYS.FGA_LOG$`	Set initialization parameter `audit_trail=db, extended`.	Value-based audit policies audit `SELECT` and DML statements (`UPDATE`, `DELETE`, or `INSERT`) on tables and views; allows monitoring data access based on content	DBAUD
Operating system files, where mandatory audit records are written and optionally, where Database audit trail (standard audit events) and fine-grained audit trail audit events are written to operating system audit logs	Set initialization parameter `AUDIT_TRAIL` parameter to `OS` and `AUDIT_FILE_DEST` parameter to the desired file in the directory specification.	DDL and DML statements, SYS privilege, successes and failures	OSAUD
Operating system-specific audit trails (system audit trail), where database audit trail records are written to Windows event log on Microsoft Windows systems or to a syslog on Linux systems	Set initialization parameters `AUDIT_SYS_OPERATIONS` to `TRUE` and `AUDIT_FILE_DEST` to the desired file in the directory, and on Linux systems `AUDIT_SYSLOG_LEVEL` to the valid `<facility>.<level>`.	DDL and DML statements, SYS privilege, successes and failures	OSAUD

See Also: "Overview of Database Auditing" and "Fine-Grain Auditing" in the Database Security chapter in *Oracle Database Concepts* for an overview of database auditing. The Database Auditing: Security Considerations chapter in *Oracle Database Security Guide* for more detailed information about database auditing.

Each database collector and channel type for the Oracle Database source type works as explained in the following sections.

Collector for Oracle Database OS Audit Logs (OSAUD Collector) for Linux and UNIX Platforms

Audit Vault invokes the OSAUD collector agent program on the client system where the source database is running. The OSAUD collector reads and parses the operating system log files generated by the source Oracle database and sends the audit records generated to the raw audit data store (see Figure 1–2).

Collector for Oracle Database OS Event Logs (OSAUD Collector) for Windows Platforms

Audit Vault invokes the OSAUD collector agent program on the client system where the source database is running. The OSAUD collector reads and parses the operating system (OS) event log files generated by the source Oracle database and sends the audit records generated to the raw audit data store (see Figure 1–2). The mode for this collector type is `EVTLOG`.

Collector for Oracle Database DB Audit Logs: AUD$ and FGA_LOG$ (DBAUD Collector)

Audit Vault uses the DBAUD collector to retrieve audit records from an Oracle database audit trail stored in the `SYS.AUD$` dictionary table and the fine-grained audit trail stored in the `SYS.FGA_LOG$` dictionary table (see Figure 1–2). The collector opens an Oracle Call Interface (OCI) connection to the source database, periodically retrieves new audit records from these tables, and sends these records to the raw audit data store.

Collector for Oracle Database Redo Logs (REDO Collector)

Oracle Audit Vault also provides a REDO collector. The REDO collector uses Oracle Streams technology to retrieve **logical change records** (**LCRs**) from the REDO logs. It then converts these LCRs into audit records and sends them to Audit Vault. On the source database, a Streams capture process uses LogMiner to extract new LCRs from the REDO logs based on capture rules that are defined by the user. A Streams propagate process then forwards the LCRs to Audit Vault over a database link. On the Audit Vault side, a specially written apply handler converts these LCRs into audit records and stores them in the raw audit data store (see Figure 1–2).

1.5 Oracle Audit Vault Event Categories

Audit records are grouped into event categories based on the meaning of events (see Table 1–4). Similar events are grouped into the same category. For example, LOGON and LOGOFF events are both grouped into the USER SESSION category.

Table 1–4 Audit Vault Event Categories

Name	Sample Events	Description
Account Management	Create User, Alter User	Management of user accounts and profiles
User Session	Login, Alter Session	Creation and use of user sessions on the system
Object Management	Create Table, Drop Index, Alter Index	Creation and management of data items and resource elements
System Management	Create Tablespace, Shutdown Database, Install Service, Alter System	Management of services that are system level
Application Management	Create Procedure, Alter Package, Drop Java	Management of applications or code on a system
Role and Privilege Management	Create Role, Grant Privilege	Management of roles and privileges granted to users or services
Data Access	Insert into Table, Select from View	Association with a data item or resource for its content or services
Service and Application Access	Execute Procedure, Import/Export	Use of service or applications
Peer Association	Create a database link	Management of association with peer systems
Audit Command	Audit Actions, Audit Privileges, Change Audit Policy	Management of audit service
Exception	Network Error, System Error	Error conditions or exceptional events
Uncategorized	Not applicable	Anything that does not belong to the previously mentioned categories
Invalid Record	Invalid audit records	Any audit records that are found to be invalid

1.6 Summary of Oracle Audit Vault Capabilities

Oracle Audit Vault has the following features that facilitate the task of managing audit data across an enterprise:

- Oracle Audit Vault provides the ability to create audit policies (audit settings) and provision the policies to the various audit sources within the enterprise. This feature, controlled by the user granted the `AV_AUDITOR` role, enables you to efficiently create and apply audit settings for compliance and security requirements.
- Oracle Audit Vault uses an alert mechanism that is especially useful when audit data must be monitored on a real-time basis for particularly sensitive systems. This capability, also controlled by the user granted the `AV_AUDITOR` role, provides the ability to configure and apply rule conditions for these types of systems when an alert action occurs, raise alerts, and enqueue alert records for prompt notice and processing. The alerting mechanism raises the level of early detection of problems, which enables administrators to act promptly rather than after the fact.
- Users granted the `AV_ADMIN` role schedule the refreshing, purging, and reloading from archives of audit data in the data warehouse for reporting and analysis purposes. Users granted the `AV_AUDITOR` role can then generate standard (out-of-the-box) reports on a regular basis to meet compliance guidelines. In addition, this same user can create specialized or custom reports to meet specific requirements.
- Oracle Audit Vault employs a highly secure model for its audit data warehouse, thus restricting access to audit trail and audit data to all system administrators. Oracle Database Vault is used to protect the audit data warehouse. Oracle Audit Vault allows only those very few select and trusted Audit Vault administrators access, as designated by their Audit Vault administrative role.
- Oracle Audit Vault provides command-line utilities: Audit Vault Configuration Assistant (AVCA), Audit Vault Control (AVCTL), and an Audit Vault Oracle Database (AVORCLDB) for configuration and management tasks. Oracle Audit Vault also provides an Audit Vault Console that mandates a separation of duties to facilitate administration and configuration tasks. Audit Vault provides administrators with an easy-to-learn interface to configure and manage Audit Vault. As an additional option during Oracle Audit Vault installation, an administrator granted the `AV_ADMIN` role can be granted the `AV_AUDITOR` role and manage the entire system.

1.7 Getting Started

After installing the Audit Vault Server and Audit Vault Agents, you should complete the following general sets of tasks in this order:

1. For Linux and UNIX platforms only: Check and set environment variables in the shells in which you will be interacting with the Audit Vault Server and the Audit Vault Agent (see Chapter 3).

   Check and set environment variables for `ORACLE_HOME`, `ORACLE_SID`, `PATH`, `LD_LIBRARY_PATH` (for Linux x86, Linux x86-64, and Solaris SPARC_64), `SHLIB_PATH` (for HP-UX), or `LIBPATH` (for AIX), as applicable in the shell in which you will be interacting with the Audit Vault Server. In the Audit Vault Server shell, you can run `coraenv` and `oraenv` scripts located in the `/usr/local/bin` directory to set these environment variables. Check and set environment variables for `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` in the shell in which you will be interacting with the Audit Vault Agent.s In the Audit Vault Agent shell, you must set these environment variables manually using the `setenv` command. (see Chapter 3).

2. Set up Audit Vault security (see Chapter 2).

   Security tasks include securing management communication between the server and agents, understanding Audit Vault roles, and encrypting network traffic between the server and client system. Before you go into production, Oracle recommends that you perform these tasks to secure management communications.

3. Get started by configuring and managing Audit Vault components (see Chapter 3).

   Initial required configuration and management tasks include creating source users and giving them privileges to perform policy management for the OSAUD and DBAUD collectors and to work with the REDO collector, creating an Audit Vault source user and granting proxy connect privilege to this user through the Audit Vault agent user, verifying that the source is compatible for the collector type in the Audit Vault Agent home, adding sources, adding collectors, setting up the database link from the source to the agent, and verifying the connection using the wallet.

4. Configure and Manage Audit Vault components (see Chapter 4).

   Additional configuration tasks can include adding, changing, and dropping agents, collectors, and audit data sources, scheduling data warehouse operations, setting up audit data storage management operations, and globally disabling and enabling alert processing for data warehouse load operations from an archive. Data warehouse scheduling tasks include setting the audit data refresh and purge schedules, as well as scheduling the reloading of archived audit data. Alert processing must be disabled when audit data is reloaded from an archive so that alerts are not reissued again and then enabled again when the warehouse is refreshed with fresh audit data. Perform these tasks initially to configure Audit Vault and thereafter only as components are reconfigured.

   Agents and collectors must be managed, such as stopping and starting them for maintenance purposes. Audit Vault administrators should view the history of refreshing, purging, and loading of the data warehouse with audit data. They can invoke immediate refresh, purge, and reload operations as needed. Audit Vault administrators should view the error message information and to monitor the general well-being of the system. These tasks are performed as needed.

1.8 Additional Resources

For more information about Oracle Audit Vault, see the following resources:

- See *Oracle Audit Vault Best Practices* for specific information and recommendations at the Oracle Audit Vault Web site

  `http://www.oracle.com/technology/products/audit-vault/index.html`

- See Oracle*MetaLink* at the Web site:

  `http://metalink.oracle.com`

  If you do not have a current Oracle Support Services contract, then you can access the same information at

  `http://www.oracle.com/technology/support/metalink/content.html`
- See the Oracle Audit Vault Discussion Forums at the Web site

```
http://forums.oracle.com/forums/forum.jspa?forumID=391
```

2 Managing Audit Vault Security

Oracle Audit Vault uses the industry leading security capabilities of Oracle Database Vault and Oracle Advanced Security features to protect audit data from the moment it is collected, transmitted, consolidated, and stored in a centralized, protected, audit data repository. This chapter provides an understanding of how to manage Oracle Audit Vault security. Audit Vault administrators should perform Oracle Audit Vault security tasks in this order of importance:

1. Secure management communication between Audit Vault Server and Audit Vault Agent (see Oracle Advanced Security – Secure Management Communication).
2. Encrypt network traffic between Audit Vault Server and Audit Vault Agent (see Oracle Advanced Security – Encrypt Network Traffic).
3. Manage user authentication metadata (see Oracle Advanced Security – Manage User Authentication Metadata).

This chapter also includes the following additional sections as background information to assist Audit Vault administrators in understanding how Oracle Database Vault protects audit data and provides strong access control:

- Oracle Database Vault – Protects Oracle Audit Vault
- Oracle Database Vault – Provides Strong Access Controls

2.1 Oracle Advanced Security – Secure Management Communication

Audit Vault administrators can further secure management communication between the Audit Vault Server and the Audit Vault Agent by using the HTTPS protocol to encrypt data (see Figure 1–2). In this case, X.509 certificates are provided by the Audit Vault administrator and are used for authentication. This is part of the postinstallation configuration of Oracle Audit Vault. Secure Sockets Layer (SSL) is configured for the mutual authentication between the Audit Vault management service on the server side and each agent over HTTPS. A Certificate Authority must provide these certificates to the Audit Vault administrator.

> **See Also:** *Oracle Database Security Guide* for more information about PKI-based authentication, digital certificates, and secure external password stores and *Oracle Database Advanced Security Administrator's Guide* for more information about Oracle wallets.

Once Audit Vault Server and Audit Vault Agent communication is secured using HTTPS, the browser must also use HTTPS to access the Audit Vault Console. There is no longer an HTTP protocol available for the browser user, because the browser to Audit Vault Console communication is also made secure.

Setting Up Mutual Authentication Between Audit Vault Server and Its Agents

See *Oracle Database Advanced Security Administrator's Guide* for information about using Oracle Wallet Manager to obtain X.509 certificates from a Certificate Authority for the Audit Vault Agent and importing them into the wallet. Use the keytool located at `$ORACLE_HOME/jdk/bin/keytool` to generate the key store if this becomes necessary. Once the key store and certificates are in place at the agent side, next set up mutual authentication between Audit Vault Server and its agents. To do this, use the AVCA secure_av command from the system where Oracle Audit Vault Server is installed. This operation secures Oracle Audit Vault Server by enabling mutual authentication with Oracle Audit Vault Agent.

The AVCA secure_av command takes the following arguments:

- `-avkeystore <keystore location>` -- The key store location for Audit Vault
- `-avkeystorepwd <keystore password>` -- The key store password for Audit Vault. The `-avkeystorepwd` argument can be omitted if the corresponding environment variable, `AVCA_AVKEYSTOREPWD` is set to *`keystore password`*. If the command-line argument `-avkeystorepwd` is specified, then the command-line argument overrides the environment variable.
- `-avtruststore <truststore location>` -- The trust store location for Audit Vault

The following AVCA secure_av command secures Oracle Audit Vault Server by enabling mutual authentication with Oracle Audit Vault Agent. In this example, the environment variable, `AVCA_AVKEYSTOREPWD` is set to `welcome_1` and the -avkeystorepwd argument is omitted from the example.

```
avca secure_av -avkeystore /tmp/avkeystore -avtruststore /tmp/avkeystore
```

From the system where Oracle Audit Vault Agent is installed, the AVCA secure_agent command secures the Oracle Audit Vault Agent by enabling mutual authentication with Oracle Audit Vault Server.

The AVCA secure_agent command takes the following arguments:

- `-agentname <agent name>` -- The name of the agent (by agent name) must be in secure mode
- `-agentkeystore <keystore location>` -- The key store location for this agent
- `-agentkeystorepwd <keystore password>` -- The key store password for this agent. The `-agentkeystorepwd` argument can be omitted if the corresponding environment variable, `AVCA_AGENTKEYSTOREPWD` is set to *`keystore password`*. If the command-line argument `-agentkeystorepwd` is specified, then the command-line argument overrides the environment variable.
- `-avdn <DN of Audit Vault>` -- The distinguished name (DN) of Audit Vault
- `-agentdn <DN of Agent>` -- The DN of this Audit Vault Agent

The following AVCA secure_agent command secures the Audit Vault Agent by enabling mutual authentication with Audit Vault. In this example, the environment variable, `AVCA_AGENTKEYSTOREPWD` is set to `welcome_1` and the -agentkeystorepwd argument is omitted from the example

```
avca secure_agent -agentname TTAGENT12 -agentkeystore /tmp/agentkeystore
-agentdn "CN=agent1, OU=development, O=oracle, L=redwoodshores, ST=ca, C=us"
-avdn "CN=av1, OU=development, O=oracle, L=redwoodshores, ST=ca, C=us"
```

2.2 Oracle Advanced Security – Encrypt Network Traffic

Because audit data is sensitive data and moves across the network as it is either collected by collectors from sources or is sent to the Audit Vault Server (see Figure 1–2), it is important to encrypt the network traffic to absolutely guarantee the security of this audit data.

Oracle Advanced Security encryption is used to set the encryption between a server and an agent. In this sense it is the server system on which Audit Vault server is installed and the agent system on which an Audit Vault Agent is installed.

The following sections describe a basic method of verifying that Oracle Advanced Security encryption is working, if it is to be used by your site. The easiest way to tell if Oracle Advanced Security encryption is working is to deliberately set wrong configuration parameters and attempt a connection between the server and agent. Incorrect parameters cause the connection to fail.

After receiving the expected failure message, set the configuration parameters to the correct settings and try the connection again. Oracle Advanced Security encryption is working properly if no further error messages are received.

The following procedures test Oracle Advanced Security encryption by this method. The incorrect parameter settings produce error 12660.

2.2.1 Setting Up Oracle Advanced Security Encryption as a Test of Your Site

Perform the following steps to set up Oracle Advanced Security encryption:

1. Set Oracle Advanced Security encryption parameters for the server.
2. Set Oracle Advanced Security encryption parameters for the agent.

2.2.1.1 Step 1: Set Encryption Parameters for the Server

Use the appropriate editor for the server platform to add the following parameters and values to change the `sqlnet.ora` file.

```
SQLNET.CRYPTO_CHECKSUM_SERVER = REJECTED
SQLNET.ENCRYPTION_SERVER = REJECTED
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA-1)
SQLNET.ENCRYPTION_TYPES_SERVER = (AES256)
SQLNET.CRYPTO_SEED = "abcdefg"
```

The value shown for `SQLNET.CRYPTO_SEED` is only an example. Set it to the value that you want. See *Oracle Database Advanced Security Administrator's Guide* for more information.

2.2.1.2 Step 2: Set Encryption Parameters for the Agent

Edit the listener configuration file on the agent system (`sqlnet.ora`) to add the following parameters:

```
SQLNET.CRYPTO_CHECKSUM_CLIENT = REQUIRED
SQLNET.ENCRYPTION_CLIENT = REQUIRED
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (SHA-1)
SLQNET.ENCRYPTION_TYPES_CLIENT = (AES256)
SQLNET.CRYPTO_SEED = "abcdefg"
```

The value shown for `SQLNET.CRYPTO_SEED` is only an example. Set it to the same value used on the server system.

2.2.2 Testing Oracle Advanced Security Encryption

After completing Steps 1 and 2 of the configuration procedure, you are ready to test the operation of the Oracle Advanced Security encryption.

2.2.2.1 Checklist for Testing Encryption

1. Connect the agent and server.
2. Reset configuration parameters on the server.

2.2.2.2 Step 1: Connect Agent and Server

Attempt a connection between the server and agent systems. You should receive the following error message:

```
ORA-12660: Encryption or crypto-checksumming parameters incompatible
```

2.2.2.3 Step 2: Reset Configuration Parameters on Server

Change the Oracle Advanced Security encryption parameters on the server to:

```
SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED
SQLNET.ENCRYPTION_SERVER = REQUIRED
```

Attempt the connection between the agent and server again. If no error message is returned and the connection completes, then encryption is working properly.

2.3 Oracle Advanced Security – Manage User Authentication Metadata

As part of the Oracle Audit Vault Server and the Oracle Audit Vault Agent installation, two wallets are created. One wallet resides on the Audit Vault Server and this one contains the `AV_ADMIN` user's credentials and is used by the Audit Vault Console to communicate to the Audit Vault database. This Audit Vault Console provides the management service that initiates the communication with agents using HTTP. Audit Vault Configuration Assistant (AVCA) modifies the Database Control console `server.xml` file and other related files to enable Audit Vault management through the Oracle Enterprise Manager Database Control console. The wallet is located in the `$ORACLE_HOME/network/admin/avwallet` directory.

The other wallet resides on the Audit Vault Agent and contains the `AV_AGENT` credentials and is used by the agent to get configuration data from the database. It is located in the `$ORACLE_HOME/network/admin/avwallet` directory. The agent-side wallet also contains the credentials used by the collectors to communicate to the source Oracle database. These credentials are used by the three ORCLDB collectors to connect to the source and to:

- Get audit records using the DBAUD collector
- Start and stop the REDO collector
- Get metadata for all the ORCLDB collectors
- Get audit settings as part of Audit Settings management

The Oracle wallet is a password-protected container that stores credentials, such as certificates, authentication credentials, and private keys, all of which are used by SSL for strong authentication. Oracle wallets are managed through Oracle Wallet Manager. Oracle Wallet Manager can perform tasks such as wallet creation, certificate request generation, and certificate import into the wallet.

This section describes managing metadata for Audit Vault administrators that includes:

- Creating Wallet Metadata
- Creating Certificate Metadata

2.3.1 Creating Wallet Metadata

A wallet holds credentials created using the AVCA create_credential command.

Provide the following information to create a wallet:

- `-wrl <wallet location>` – Wallet location
- `-wpwd <wallet password>` – Wallet password, needed to open the wallet. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVCA_WPWD` is set to *`wallet password`*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable.

Use the AVCA create_wallet command to create a wallet. However, before you run this command, create an environment variable named `AVCA_WPWD` set to `welcome1`, the wallet password. Then run the command. For example:

```
avca create_wallet -wrl $T_WORK/tt_1
```

See the AVCA create_wallet command for more reference information.

2.3.2 Creating Certificate Metadata

Oracle Audit Vault uses third-party network authentication services, PKI-based authentication, to authenticate its user clients. Authentication systems based on **public key infrastructure** (PKI) issue digital certificates to user clients, which use them to authenticate directly to servers in the enterprise without directly involving an authentication server. These user certificates, along with the private key of the user and the set of trust points of a user (trusted certificate authorities), are stored in Oracle wallets.

As part of the Oracle Audit Vault Server and Oracle Audit Vault Agent installation, Audit Vault creates the wallet and stores the certificates that are needed for users. The AVCA create_credential command is useful if a new certificate for an existing user must be created. For example, use the AVCA create_credential command to create a new certificate if someone changes the source user password on the source, thus eventually breaking the connection between the collector and the source.

Provide the following information to create a credential to be stored in the wallet:

- `-wrl <wallet location>` – Wallet location
- `-wpwd <wallet_password>` – Wallet password, needed to open the wallet. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVCA_WPWD` is set to *`wallet password`*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable.
- `-dbalias <db alias>` – Database alias
- `-usr <usr>/<password>` – Target user name and password to be secured and stored in the wallet. The `-usr` argument can be omitted if the corresponding environment variable, `AVCA_USR` is set to *`usr/password`*. If the command-line argument `-usr` is specified, then the command-line argument overrides the environment variable.

Use the AVCA create_credential command to create a credential. However, before you run this command, create an environment variable named AVCA_WPWD set to welcome1, the wallet password; and an environment variable named AVCA_USR set to scott/tiger. Then run the command. For example:

```
avca create_credential -wrl $T_WORK/tt_1 -dbalias inst1
```

After executing this command, you must modify the sqlnet.ora file as described in the AVCA create_credential command usage notes in Appendix A, and if needed, set the $TNS_ADMIN environment variable.

2.4 Oracle Database Vault – Protects Oracle Audit Vault

Oracle Database Vault provides realms, separation of duty, command rules and factors as features that are applicable to reducing the overall risk associated with specific provisions of regulations worldwide. These regulations have common themes that include internal controls, separation of duty, and strong access controls on access to sensitive information. Technical solutions are required to mitigate the risks associated with items such as unauthorized modification of data and unauthorized access.

Oracle Database Vault realms prevent database administrators (DBAs), application owners, and other privileged users from viewing application data using their powerful privileges. Database Vault realms put in place preventive controls, helping reduce the potential impact when a data breach does occur, enabling the DBA to perform his or her job more effectively. Oracle Database Vault realms can be used to protect an entire application or a specific set of tables within an application, providing highly flexible and adaptable security enforcement. Oracle Audit Vault audit data is protected in this way.

Oracle Database Vault prevents highly privileged users (DBAs) from accessing audit data. It enforces a separation of duty by not allowing the same user granted two or more administrator roles to perform different responsibilities in the same session and optimally to have different administrator users be granted respective roles to perform these responsibilities in separate sessions.

Oracle Database Vault provides two roles, DV_ACCTMGR to manage database user accounts and DV_OWNER to manage database roles and configuration. The security administrator granted DV_ACCTMGR role can create, alter, and drop users and this user creates all Audit Vault administrator users. The security administrator granted DV_OWNER role can grant Oracle Database Vault roles. The Audit Vault administrator user granted the AV_ADMIN role grants all Audit Vault roles. Thus, two different highly privileged users are required one to create Audit Vault users and the other to grant these users Audit Vault roles. In this way, Oracle Database Vault and Oracle Audit Vault protect audit data from access, enforce protection of database structures from unauthorized change, and set a variety of access controls to implement dynamic and flexible security requirements. See Section 2.5 for more information about these Database Vault security administrator accounts, Audit Vault administrator accounts, and the core database user accounts.

Using Oracle Database Vault, highly privileged database users can be prevented from accessing application data. In addition, access to applications, databases, and data can be tightly controlled based on such variables as time of day, IP address or subnet.

2.5 Oracle Database Vault – Provides Strong Access Controls

Audit Vault is a secure data warehouse that consolidates audit data across an enterprise. The data is only visible to Audit Vault auditors once it is moved into the Audit Vault data warehouse. No user can access the audit data before it is moved to the Audit Vault data warehouse nor after it is purged from there. Even a SYS user cannot access this secure audit data. The default privilege that a SYS user will have is the ability to lock and unlock the Audit Vault schema. This extremely tight security is necessary to prevent audit trail data, which is extensive, detailed, and sensitive information, from being compromised. Oracle Database Vault features guarantee this level of security.

Audit Vault predefined administrator roles include:

- AV_ADMIN – 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. Only the user granted the AV_ADMIN role can grant the appropriate role (AV_ADMIN, AV_AUDITOR, AV_AGENT, and AV_SOURCE) through SQL*Plus.
- AV_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 – 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.
- AV_SOURCE – Manages the setup of sources for audit data collection. A user is created prior to source and collector configuration and granted this role upon adding a source to Audit Vault using the AVORCLDB add_source command. The collector software uses this role at run time to send audit data to Audit Vault.
- AV_ARCHIVER – 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 – Manages Oracle Database Vault roles and configuration.
- DV_ACCTMGR – Manages database user accounts. Only the user granted this role can create Audit Vault administrator users.

Table 2–1 shows the roles and privileges an administrative user is granted when that user is granted one of the high level Audit Vault or Database Vault roles. Typically, one user is granted an AV_ADMIN role and one user is optionally granted an AV_AUDITOR role as part of installing the Audit Vault Server. The user granted the AV_ADMIN role can be granted the AV_AUDITOR role if that user is not created during the Audit Vault Server installation.

Because Oracle Audit Vault is protected by Oracle Database Vault, only the user granted the DV_ACCTMGR role can create, alter, and drop users.

Table 2–1 Roles and Privileges Granted to Administrators Granted a Specific Audit Vault or Database Vault Role

Role Granted to User	Roles Granted	Privileges Granted

AV_ADMIN	DV_PUBLIC
	AV_ADMIN
	SELECT_CATALOG_ROLE
	HS_ADMIN_ROLE
	AQ_ADMINISTRATOR_ROLE
	AQ_ADMINISTRATOR_ROLE
	AV_AUDITOR
	AV_AGENT
		CREATE SESSION
		CREATE ANY VIEW
		GRANT ANY ROLE
		MANAGE ANY QUEUE
		ENQUEUE ANY QUEUE
		DEQUEUE ANY QUEUE
		CREATE EVALUATION CONTEXT
		CREATE RULE SET
		CREATE RULE

AV_AUDITOR	DV_PUBLIC, AV_AUDITOR SELECT_CATALOG_ROLE HS_ADMIN_ROLE	CREATE SESSION

AV_AGENT	DV_PUBLIC
	AV_AGENT
		CREATE SESSION
		CREATE ANY VIEW

AV_SOURCE	DV_PUBLIC
	RESOURCE
	AV_SOURCE
	AV_USER_ROLE
		CREATE SESSION
		RESTRICTED SESSION
		UNLIMITED TABLESPACE
		CREATE TABLE
		CREATE CLUSTER
		CREATE SEQUENCE
		CREATE DATABASE LINK
		CREATE PROCEDURE
		CREATE TRIGGER
		CREATE TYPE
		CREATE OPERATOR
		CREATE INDEXTYPE
		MANAGE ANY QUEUE
		ENQUEUE ANY QUEUE
		DEQUEUE ANY QUEUE
		CREATE EVALUATION CONTEXT
		CREATE RULE SET
		CREATE ANY RULE SET
		ALTER ANY RULE SET
		EXECUTE ANY RULE SET
		CREATE RULE
		CREATE ANY RULE
		ALTER ANY RULE
		EXECUTE ANY RULE

DV_ACCTMGR	DV_PUBLIC CONNECT DV_ACCTMGR	CREATE SESSION CREATE USER ALTER USER DROP USER CREATE PROFILE ALTER PROFILE DROP PROFILE
DV_OWNER	DV_PUBLIC CONNECT DV_OWNER DV_ADMIN DV_SECANALYST	CREATE SESSION GRANT ANY ROLE ALTER ANY TRIGGER ADMINISTER DATABASE TRIGGER

The Audit Vault roles are granted or revoked through the SQL*Plus interface using the SQL GRANT and REVOKE commands in the following way. All granting or revoking of Audit Vault roles or privileges is done through SQL*Plus by the user who has AV_ADMIN role granted. To add more users, a user must connect having DV_ACCTMGR role to create the users; however, this user cannot also grant these roles to these users. Only the user granted the AV_ADMIN role can then grant the appropriate role (AV_ADMIN, AV_AUDITOR, AV_AGENT, or AV_SOURCE), through SQL*Plus.

An Audit Vault administrator with one of these predefined roles granted can assume only one administrative responsibility at a time in a given session. For instance, if the Audit Vault administrator must perform a different task in another role, the same administrator must begin a new session to start that task.

> **Note:** Users granted more than one Audit Vault role can only log in to the Audit Vault Console as a single role. They must log out and log in to an Audit Vault system again to use a different role. This security measure maintains a separation of duties within an Audit Vault system for each Audit Vault user.

Audit Vault allows incoming connections based on Secure Sockets Layer (SSL) protocol only and its listener can receive only TCP/IP with SSL (HTTPS) connections. Thus, all Audit Vault users are external SSL users. Audit Vault provides a **public key infrastructure** (PKI) if one is needed; otherwise, customers can use their existing public key interface. If using the Audit Vault public key infrastructure, users are required to regenerate wallets on a regular basis every few months as determined by the account refresh frequency (ARF).

Table 2–2 shows all other database core accounts created in the default Audit Vault installation. The operating system authentication to the database is disabled by default. In addition, connections to the database using the SYSDBA privilege (that is, those that use the AS SYSDBA clause) are disabled. This is a security feature and is implemented to prevent misuse of the SYSDBA privilege. You must connect to the database using the SYSOPER privilege (connections that use the AS SYSOPER clause) to manage the Audit Vault database; such as, shutting it down and starting it up. See "Postinstallation Tasks" in the Oracle Audit Vault installation guides for more information about unlocking and resetting user passwords and enabling or disabling connections with the SYSDBA Privilege.

Table 2–2 Database Core Accounts Created and Privileges In Use

Account	Privileges	Privilege In Use or Not	Password to Use
SYS SYSTEM SYSMAN DBSNMP	Many	Yes	Same password as user granted AV_ADMIN role for basic installation or password may be set separately in advanced installation. To use, user account must be unlocked and password reset.
/ AS SYS AS	SYSDBA	No, not allowed	To use, user must create password file to enable its use. Password is set when password file is created.
/ AS SYS AS	SYSOPER	Yes, allowed	Same password as user granted AV_ADMIN role.

The following example shows how to add a new Audit Vault administrator auditor account, grant this new user the AV_AUDITOR role, then check this user's granted roles and privileges.

```
sqlplus /nolog
SQL> connect avadmindva
Enter password: <avadmindvapassword>
Connected.
```

```
SQL> create user avauditor2 identified by Welcome_99;

User created.

SQL> connect avadmin
Enter password: <avadminpassword
Connected.
SQL> grant AV_AUDITROR to avauditor2;

Grant succeeded.

SQL> connect avauditor2
Enter password: <avauditor2password>
Connected.
SQL> show user
USER is "AVAUDITOR2"
SQL> select * from session_roles;

ROLE
------------------------------
DV_PUBLIC
AV_AUDITOR
SELECT_CATALOG_ROLE
HS_ADMIN_ROLE

SQL> select * from session_privs;

PRIVILEGE
----------------------------------------
CREATE SESSION
```

The following example shows how to connect as the SYS user with SYSOPER privilege (using the clause AS SYSOPER), shut down the Audit Vault database, and then start it up again.

```
sqlplus /nolog
SQL connect sys as sysoper
Enter password: <sysoperpassword>
Connected.
SQL> shutdown immediate
Database closed.
Database dismounted.
Oracle instance shut down.

SQL> startup
Oracle instance started.
Database mounted.
Database opened.
SQL> exit
```

3

Getting Started with Audit Vault

This chapter describes how to begin configuring Audit Vault components by performing the following tasks:

- Checking and Setting Environment Variables (Linux and UNIX Platforms)
- Adding a Source and Collectors
- Starting Up Agents and Collectors

Adding sources to Audit Vault and deploying collectors involves the following tasks:

1. For Linux and UNIX platforms, check and set environment variables in the shells in which you will be interacting with the Audit Vault Server and the Audit Vault Agent (see Section 3.1).
2. Add a source and collectors using the AVORCLDB command-line utility (see Section 3.2).
3. Start up agents and collectors using the AVCTL command-line utility (see Section 3.3).

3.1 Checking and Setting Environment Variables (Linux and UNIX Platforms)

As the last configuration step in an Audit Vault Server and each Audit Vault Agent installation, a `root.sh` configuration file is run under the super user. On the Audit Vault Server, this file drops three scripts in the `/usr/local/bin` directory. Two of these scripts, `coraenv` and `oraenv`, can be called by users to set environment variables on the Audit Vault Server. However, because these two scripts are not dropped as part of the Audit Vault Agent installation, you must set environment variables using the appropriate operating system shell command. The tasks to perform in the respective shells for interacting with the Audit Vault Server and the Audit Vault Agent are listed as follows:

Audit Vault Server Shell

At the command line, run the `coraenv` and `oraenv` scripts located in the `/usr/local/bin` directory that sets the following environment variables: `ORACLE_HOME`, `ORACLE_SID`, and `PATH`, `LD_LIBRARY_PATH` (for Linux x86, Linux x86_64, and Solaris SPAC_64), `SHLIB_PATH` (for HP-UX), or `LIBPATH` (for AIX), as applicable in the shell in which you will be interacting with Audit Vault Server.

`ORACLE_HOME` is set to the Audit Vault Server home directory. By default, this is the directory path down to and including `av_1`. `ORACLE_SID` is set to `av`, the unique service name (SID) for the Audit Vault database. If your SID is set otherwise, use that SID. The `PATH` appends `$ORACLE_HOME/bin` to your `PATH` environment variable.

Audit Vault Agent Shell

1. Check and manually set the ORACLE_HOME environment variable to the Audit Vault Agent home directory. By default, this is the directory path down to and including av_agent_1.
2. Check and set the LD_LIBRARY_PATH environment variable to include $ORACLE_HOME/lib.
3. Check and set the PATH environment variable to include $ORACLE_HOME/bin. Be sure that you append this information to the existing PATH information.
4. Ensure that the following environment variables are unset: ORACLE_SID, TNS_ADMIN, and TWO_TASK.

3.2 Adding a Source and Collectors

Perform the following steps to add a source and collectors:

1. Ensure that the source database has a password file set up. AVORCLDB connects to the source database with sysdba privileges. A connection to the source can succeed only if the password file is set up. See *Oracle Database Administrator's Guide* for information about the orapwd command used to create the password file.
2. Create users, one on the Oracle source database and one on the Audit Vault Server.

   a. On the Oracle source database

   Create a user, referred to as *srcusr*, on the source database for use by the collectors.

   ```
   SQL> create user <srcusr name> identified by <srcusr password>;
   ```

   The *srcusr* must have a set of required privileges granted to it. The required privileges are listed in $ORACLE_HOME/av/scripts/streams/source/zarsspriv.sql. This script is located in both the Audit Vault Server and the Audit Vault Agent Oracle homes after an installation.

   Run this script on the source database as SYS user to grant this *srcusr* the required privileges using the following syntax:

   ```
   zarsspriv.sql <srcusr> <mode>
   ```

   The argument *srcusr* is the user to be granted the privileges, and the argument *mode* is one of two keywords:

   – SETUP – For policy management for the OSAUD and DBAUD collectors

   – REDO_COLL – For the REDO log collector

   Example 3–1 shows how the *srcusr* named srcuser1 is granted the required privileges for policy management for the OSAUD and DBAUD collectors.

   Example 3–2 shows how the *srcusr* named srcuser1 is granted the required privileges for the REDO collector.

Example 3–1 Grant the Source User the Required Privileges for Policy Management

```
sqlplus / as sysdba
.
.
```

```
.
SQL> @zarsspriv.sql srcuser1 SETUP

PL/SQL procedure successfully completed.
```

Example 3–2 Grant the Source User the Required Privileges for the REDO Collector

```
sqlplus / as sysdba
.
.
.
SQL> @zarsspriv.sql srcuser1 REDO_COLL

PL/SQL procedure successfully completed.
```

b. On the Audit Vault Server

Create or use an existing user on Audit Vault Server to be used to insert audit data for this source. This user will be referred to as *avsrcusr*. For example, to create this user in the Audit Vault database, follow these steps:

– Log in to SQL*Plus as the Database Vault Account Manager.

For the Basic installation, log in as follows:

```
sqlplus/ nolog
SQL> connect <avadmin>dva
Enter password: <avadmin user password>
Connected.
SQL>
```

For the Advanced installation, log in as follows:

```
sqlplus /nolog
SQL> connect <dv_acctmgr user name>
Enter password: <dv_acctmgr user password>
Connected.
SQL>
```

– Create the Audit Vault source user.

```
SQL> create user <avsrcusr name> identified by <avsrcusr password>;
SQL> exit
```

Grant proxy connect privilege to *avsrcusr* through the user used in the installation of the Audit Vault Agent, referred to here as *agentusr*, as shown in Example 3–3. You must connect using the Database Vault account manager as shown in Step 2b to run this command.

Example 3–3 Granting Proxy Connect Privilege to <avsrcusr>

```
SQL> alter user <avsrcusr> grant connect through <agentusr>;
SQL> exit
```

3. From either the Audit Vault Server home or the Audit Vault Agent home shell, verify that the source is compatible for the collector type in the agent home. The AVORCLDB verify command checks the source database to see if the configuration on it would allow an Audit Vault collector to run against it.

To verify that the source is compatible with each of the collectors, use the AVORCLDB verify command in the agent home shell, as shown in Example 3–4.

However, before you run this command, create an environment variable named AVORCLDB_SRCUSR set to testdba/*password*. Then run the command.

Note: The -srcusr argument can be omitted if the corresponding environment variable AVORCLDB_SRCUSR is set to testdba/*password*. If the command-line argument -srcusr is specified, then the command-line argument overrides the environment variable.

Example 3–4 Partly Successful Verify Operation of Source Compatibility with the Collectors

```
avorcldb verify -src SRC1.US.ORACLE.COM:1521:orcl
                -colltype ALL
Verified source SRC1.US.ORACLE.COM for OS File Audit Collector
Verified source SRC1.US.ORACLE.COM for Aud$/FGA_LOG$ Audit Collector
Source database must be in ARCHIVELOG mode to use REDO Log collector
Incorrect database compatibility 9.2.0; recommended value is 10.2.0.0.0
Parameter _SPIN_COUNT not set; recommended value is 5000
Parameter _JOB_QUEUE_INTERVAL not set; recommended value range [4 - ANY_VALUE]
Parameter JOB_QUEUE_PROCESSES = 0 not in recommended value range [4 - ANY_VALUE]
Parameter SGA_MAX_SIZE = 155189248 not in recommended value range [209715200 - ANY_VALUE]
Parameter SGA_TARGET = 0 not in recommended value range [209715200 - ANY_VALUE]
Parameter UNDO_RETENTION = 900 not in recommended value range [3600 - ANY_VALUE]
Parameter GLOBAL_NAMES = false not set to recommended value true
Please set the above init.ora parameters to recommended values
```

If the AVORCLDB verify command returns an error message for a specific collector or some other message indicating a problem, examine the content of the error message, then try to fix the problem.

In Example 3–4, a number of initialization parameters on the source database must be set or modified to use the REDO collector. For a complete list of parameters used by the REDO collector, see Appendix D.

Retry the verify command, specifying the collector type in which there was a problem, as shown in Example 3–5. You can run this command as many times as needed until all problems are solved and this command returns a verified source message indicating success.

Example 3–5 Successful Verify Operation of Source Compatibility with the REDO Collector

```
avorcldb verify -src SRC1.US.ORACLE.COM:1521:orcl
                -colltype REDO
source SRC1.US.ORACLE.COM verified for REDO Log Audit Collector collector
```

4. From the Audit Vault Server home shell, add the source to Audit Vault using the AVORCLDB add_source command with the source user *srcusr*, created in Step 2a (srcuser1 in this example), and the Audit Vault source user *avsrcusr*, (avsrcuser1 in this example) created in Step 2b, as arguments in the AVORCLDB add_source command.

   Before you run this command, create two environment variables, one named AVORCLDB_SRCUSR set to srcusr/*password* and the other AVORCLDB_AVSRCUSR set to avsrcusr1. Then run the command. Example 3–6 shows how to add a source to Audit Vault.

> **Note:** The `-srcusr` argument can be omitted if the corresponding environment variable `AVORCLDB_SRCUSR` is set to `srcusr/`*`password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variables.

Example 3–6 Adding a Source to Audit Vault Database

```
avorcldb add_source -src lnxserver:4523:source1db.domain.com
                    -avsrcusr avsrcuser1 -desc 'HR Database'
                    -agentname agent1
Adding source...
Source added successfully.
source successfully added to Audit Vault

remember the following information for use in avctl
Source name (srcname): RODSRC1.US.ORACLE.COM
map_source_to_agent
map_source_to_agent
```

5. From the Audit Vault Server home shell, add the collector to Audit Vault using the AVORCLDB add_collector command with the source user *`srcusr`*, created in Step 2a (`srcuser1` in this example), and the Audit Vault source user *`avsrcusr`*, (`avsrcuser1` in this example) created in Step 2b, as arguments in the AVORCLDB add_collector command.

   Before you run this command, create an environment variable named `AVORCLDB_SRCUSR` set to srcuser1/*password*. Then run the command. Example 3–7 shows how to add the OSAUD collector to Audit Vault for UNIX platforms.

> **Note:** The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to `srcuser1/`*`password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.

Example 3–7 Adding the OSAUD Collector to Audit Vault for UNIX Platforms

```
avorcldb add_collector -srcname source1db.domain.com
                       -agentname agent1
                       -colltype OSAUD
source SOURCE1DB.DOMAIN.COM verified for OS File Audit Collector collector
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): OSAUD_Collector
```

Example 3–8 shows how to add the OSAUD collector to Audit Vault on Windows for the event log.

Example 3–8 Adding the OSAUD Collector to Audit Vault on Windows for the Event Log

```
avorcldb add_collector -srcname source1db.domain.com
                       -agentname agent1
                       -colltype EVTLOG
```

```
source SOURCE1DB.DOMAIN.COM verified for Windows Event Log Audit Collector
collector
Adding collector...
Collector added sucessfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): EVTLOG_Collector
```

Example 3–9 shows how to add the DBAUD collector to Audit Vault.

Example 3–9 Adding the DBAUD Collector to Audit Vault

```
avorcldb add_collector -srcname source1db.domain.com
                       -agentname agent1 -colltype DBAUD
source SOURCE1DB.DOMAIN.COM verified for Aud$/FGA_LOG$ Audit Collector collector
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): DBAUD_Collector
```

Example 3–10 shows how to add the REDO collector to Audit Vault and shows that values for both the `-avsrcusr` and `-av` arguments must be supplied for this collector type.

> **Note:** The `-avsrcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_AVSRCUSR` is set to `avsrcuser1/`*`password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.

Example 3–10 Adding the REDO Collector to Audit Vault

```
avorcldb add_collector -srcname source1db.domain.com
                       -agentname agent1
                       -colltype REDO
                       -av lnxserver:4523:hrdb.domain.com
source SOURCE1DB.DOMAIN.COM verified for REDO Log Audit Collector collector
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): REDO_Collector
initializing REDO Collector
setting up APPLY process on Audit Vault server
setting up CAPTURE process on source database
```

6. In the Audit Vault Agent shell, set up the source using the AVORCLDB setup command (as shown in Example 3–11) using the source user *`srcusr`* created in Step 2a (`srcuser1` in this example), the source name -srcname <srcname> previously used in Step 5, and the wallet password, which is the <agentusr> password. However, before you run this command, create an environment variable named AVORCLDB_WPWD set to *password*, the wallet password. Then run the command.

> **Note:** The -wpwd argument can be omitted if the corresponding environment variable, AVORCLDB_WPWD is set to *password*. If the command-line argument -wpwd is specified, then the command-line argument overrides the environment variable.

Example 3–11 Setting Up the Source at the Agent

```
avorcldb setup -verbose -srcname source1db.domain.com
updated tnsnames.ora with alias [SRCDB1] to source database
adding credentials for user srcdba2 for connection [SRCDB1]
Storing user credentials in wallet...
Create credential oracle.security.client.connect_string2
done.
verifying SRCDB1 connection using wallet
```

3.3 Starting Up Agents and Collectors

Steps to start up an agent and its collectors are described as follows:

1. Ensure that the agent is started.

   To check the status of the agent to see if it is started, on the Audit Vault Server shell, use the AVCTL show_agent_status command, as shown in Example 3–12. In this case the agent is not started.

Example 3–12 Checking the Status of the Agent

```
avctl show_agent_status -agentname agent1
AVCTL started
Getting agent metrics...
--------------------------------
Agent is not running
--------------------------------
Metrics retrieved successfully
--------------------------------
```

   If the agent is not started as indicated in Example 3–12, use the AVCTL start_agent command to start the agent, as shown in Example 3–13.

Example 3–13 Starting the Agent

```
avctl start_agent -agentname agent1
AVCTL started
Executing task start_agent
Starting Agent...
Agent started successfully.
```

2. In the Audit Vault Server shell, start the OSAUD, DBAUD, and REDO collectors.

   To start the OSAUD, DBAUD, and REDO collectors, use the AVCTL start_collector command for each collector, as shown in Example 3–14. If successful, each collector is moved to a RUNNING state.

Example 3–14 Starting the OSAUD, DBAUD, and REDO Collectors

```
avctl start_collector -collname OSAUD_Collector
                        -srcname DBS1.REGRESS.RDBMS.DEV.US.ORACLE.COM
AVCTL started
```

```
Executing task start_collector
Starting Collector...
Collector started successfully.

avctl start_collector -collname DBAUD_Collector
                        -srcname DBS1.REGRESS.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Executing task start_collector
Starting Collector...
Collector started successfully.

avctl start_collector -collname REDO_Collector
                        -srcname DBS1.REGRESS.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Executing task start_collector
Starting Collector...
Collector started successfully.
```

To use the Audit Vault Console to start collectors, log in to the Audit Vault Console as the user with AV_ADMIN role granted. Click the **Management** tab, then the **Collectors** subtab to display the **Collectors** page (see Figure 4–9). On the **Collectors** page you can view the collectors and collector information and start and stop collectors. Locate the OSAUD_Collector, the DBAUD_Collector, and REDO_Collector collectors that you added. Note the status of each collector. A red down arrow should appear, indicating that the collector is not running. Select each collector and click **Start**. A green up arrow appears when the collector is successfully started and is in the RUNNING state.

Another way to check the collector status is to check for the process names. In the agent home shell, issue a ps command. If the DBAUD and OSAUD collectors are running, you will see that the avaudcoll and avoscoll processes are present. To see if audit records are being collected, inspect the contents of the log files in the Audit Vault Agent home $ORACLE_HOME/av/log directory. The log file has the format <collector_name>_<source-name_prefix><source_id>.log. For the DBAUD_Collector collector, the log file name is DBAUD_Collector_<source-name_prefix><source-id>.log. For the OSAUD_Collector collector, the log file name is OSAUD_Collector_<source-name_prefix>_<source-id>.log. Each log file keeps a running record of its audit record collection operations and will indicate when collection has occurred, or if a problem was encountered in the collection operation. See Chapter 6 for more information about troubleshooting collector setup and start collector operations.

3. Check the collector status from the Audit Vault Server shell using the AVCTL command-line utility.

   To check the status of the collectors, use the AVCTL show_collector_status command shown in Example 3–15.

Example 3–15 Checking the Status of the OSAUD, DBAUD, and REDO Collectors

```
avctl show_collector_status -collname OSAUD_Collector
                            -srcname DBS1.REGRES.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Getting collector metrics...
--------------------------------
Collector is running
--------------------------------

avctl show_collector_status -collname DBAUD_Collector
```

```
                            -srcname DBS1.REGRES.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Getting collector metrics...
--------------------------------
Collector is running
--------------------------------

avctl show_collector_status -collname REDO_Collector
                            -srcname DBS1.REGRES.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Getting collector metrics...
--------------------------------
Collector is running
--------------------------------
```

The status return message will indicate whether the collector is running or not; otherwise, it might display an error message indicating that there is a problem.

See Chapter 4 for additional configuration and management tasks that you may need to perform on your running Audit Vault system.

4 Configuring and Managing Audit Vault

Once you have configured and started agents and their collectors and set up the sources to be audited as described in Chapter 3, you may need to perform some additional configuration tasks and also begin to manage Audit Vault.

This chapter includes the following sections:

- Performing Additional Audit Vault Configuration Tasks
- Managing Audit Vault

4.1 Performing Additional Audit Vault Configuration Tasks

Some additional Audit Vault configuration tasks may include performing the following tasks as needed or as indicated previously in Chapter 3:

- Adding and Dropping Agents
- Adding, Altering, and Dropping Sources
- Adding, Altering, and Dropping Collectors
- Configuring the Data Warehouse Schedule
- Globally Disabling and Enabling Alert Settings
- Viewing Audit Event Categories

4.1.1 Adding and Dropping Agents

See *Oracle Audit Vault Agent Installation Guide* for information about installing an Audit Vault Agent.

Agents can only be added or dropped.

Agents can be dropped from Oracle Audit Vault. The AVCA drop_agent command does not delete the agent from Oracle Audit Vault. The AVCA drop_agent command disables the agent. Therefore, you can neither add an agent by the same name as the one that was dropped nor enable an agent that has been dropped.

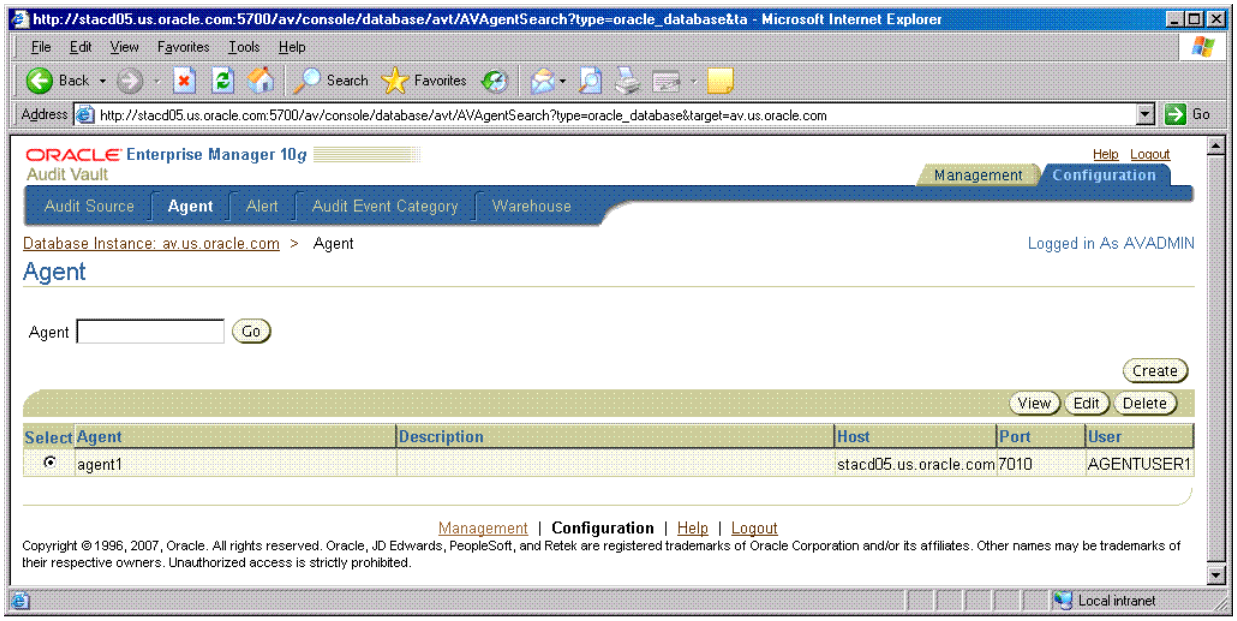
To drop an agent, use the AVCA drop_agent command. For example:

```
avca drop_agent -agentname OC4JAgent1
```

See Appendix A for reference information about each of these commands.

To use the Audit Vault Console to manage agents, log in to the Audit Vault Console as the user with `AV_ADMIN` role granted. Click the **Configuration** tab, then the **Agent** subtab to display the **Agent** page (see Figure 4–1).

Figure 4–1 Agent Configuration Management Page



http://stacd05.us.oracle.com:5700/av/console/database/avt/AVAgentSearch?type=oracle_database&ta - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://stacd05.us.oracle.com:5700/av/console/database/avt/AVAgentSearch?type=oracle_database&target=av.us.oracle.com Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management Configuration
Audit Source Agent Alert Audit Event Category Warehouse
Database Instance: av.us.oracle.com > Agent
Logged in As AVADMIN
Agent
Agent Go
Create
View Edit Delete
Local intranet

Select	Agent	Description	Host	Port	User
●	agent1		stacd05.us.oracle.com	7010	AGENTUSER1

Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

From the **Agent** page, you can:

- Enter an agent name in the Agent field and then click **Go** to view information about that agent.
- Select an agent, then click **View** to view the properties for the agent. After viewing the agent properties on the **View Agent** page, click **OK** to return to the **Agent** page.
- Select an agent, then click **Edit** to edit the properties for an agent. On the **Edit Agent** page, edit the desired properties for the agent. Click **OK** to save your changes and return to the **Agent** page.
- Select an agent, then click **Delete** to delete that agent. Once you delete that agent, its name cannot be used again to create another agent.
- Click **Create** to create an agent. An **Add Agent** page appears.

  At the **Add Agent** page, specify values for the following agent fields.

  – **Name**

  – **Host**

  – **Port**

  – **User**

  – **Description**

  Click **OK** to add the agent to Oracle Audit Vault and return to the **Agent** page, where you can view agent information including the agent just created.

Click **Help** on any of these agent pages for more information.

4.1.2 Adding, Altering, and Dropping Sources

Sources are databases in which the audit trail data is being managed by Oracle Audit Vault. Before adding a source, the Audit Vault Agent, which manages the collectors to extract the audit trail data, must exist or be installed.

This section describes configuring sources. After issuing the AVORCLDB setup command, a source is added and the specified collectors are added to Oracle Audit Vault (see Section 3.2).

The following information was provided to add the source to Audit Vault using the following arguments in the AVORCLDB add_source command:

- `-src <host:port:service>` – The source connection information consisting of the host name:port number:service ID (SID), separated by a colon.
- `-srcusr <usr>/<password>` – The source user name and password of the user granted AV_SOURCE role. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`usr/password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
- `-avsrcusr <usr>` – The Audit Vault source user name.
- `[-srcname <srcname>]` – Optional source name. If this argument is not specified, the global database name of the source will be used.
- `[-desc <desc>]` – Optional brief description of the source.
- `[-agentname <agentname>]` – Optional agent name to configure policy management.

The following source attribute information is modifiable after its creation by using the optional `<attrname>=<attrvalue>` argument and by separating multiple pairs by a space on the command line. The following attributes can be modified by entering one or more sets of attribute name and value pairs to be changed using the AVORCLDB alter_source command:

- `SOURCETYPE` – A new source type for this source
- `NAME` – A new name for this source
- `HOST` – A new source host name
- `HOSTIP` – A new source host IP address
- `VERSION` – A new source version
- `TIMEZONE` – A new time zone for this source
- `USERNAME` – A new user name used to connect to this audit data source
- `PASSWORD` – The password of the user name used to connect to the audit data source
- `AUTHENTICATION` – A new authentication method
- `DESCRIPTION` – A new description for this source
- `DB_SERVICE` – A new audit data source service name
- `PORT` – A new port number for the system where the audit data resides
- `GLOBAL_DATABASE_NAME` – The new global database name for this source
- `WALLET_LOC` – The wallet location, if used, for this audit data source

You can modify one or more attributes at a time using the AVORCLDB alter_source command. See the AVORCLDB alter_source command for more information.

To drop a source, specify its name in an AVORCLDB drop_source command. However, a source cannot be dropped or deleted if there are any active collectors for this source. All collectors must be inactive (dropped) to successfully drop or delete a source from Oracle Audit Vault. The drop_source command does not delete the source from Oracle Audit Vault. The drop_source command disables the source. Therefore, you can neither add a source by the same name as the one that was dropped nor enable a source that has been dropped. Audit data for a dropped source will no longer be collected once the source has been dropped, but information for a dropped source is maintained in Oracle Audit Vault with a status of dropped (inactive).

To alter a source, use the following AVORCLDB alter_source command:

```
avorcldb alter_source -srcname testSrc -srcdesc new desc
```

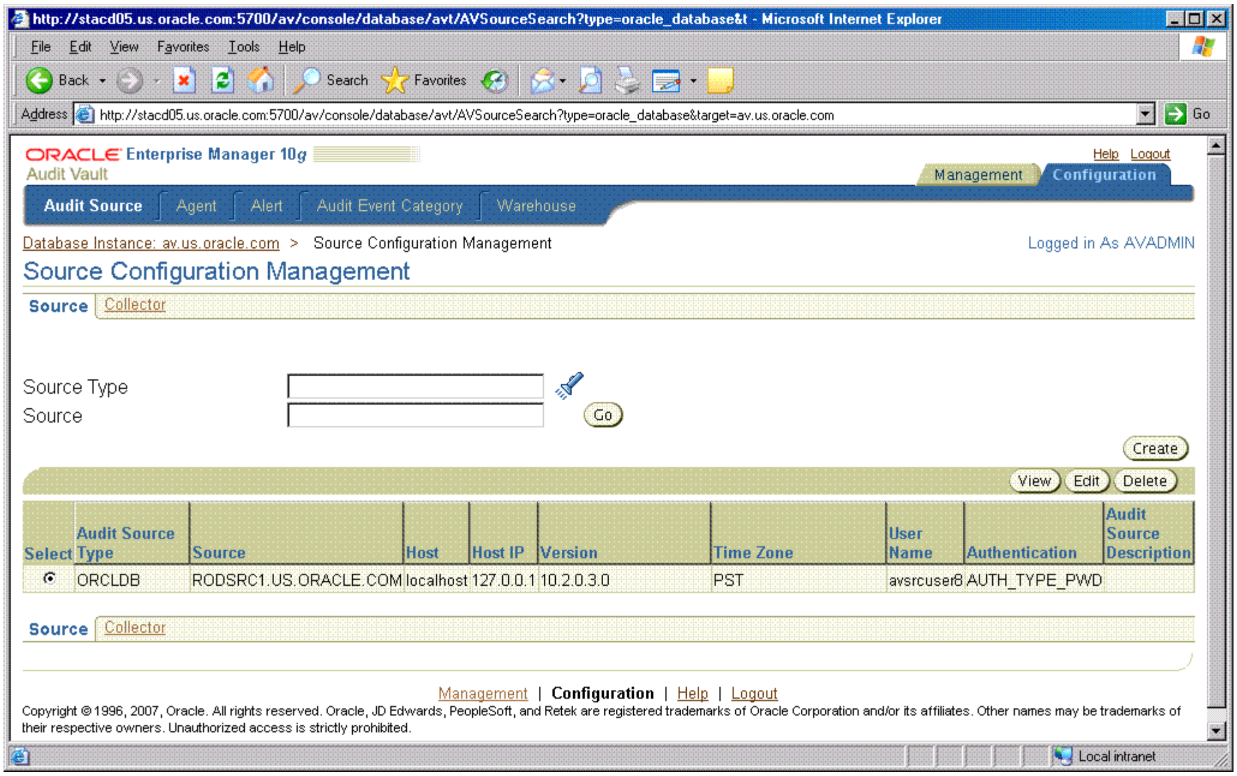
Use the AVORCLDB drop_source command to drop a source. For example:

```
avorcldb drop_source -srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
```

See Appendix C for reference information about each of these commands.

To use the Audit Vault Console to manage sources, log in to the Audit Vault Console as the user with AV_ADMIN role granted. Click the **Configuration** tab, then the **Audit Source** subtab to display the **Source Configuration Management** page (see Figure 4–2).

Figure 4–2 Source Configuration Management Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVSourceSearch?type=oracle_database&t - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://stacd05.us.oracle.com:5700/av/console/database/avt/AVSourceSearch?type=oracle_database&target=av.us.oracle.com
Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management
Configuration
Audit Source
Agent
Alert
Audit Event Category
Warehouse
Local intranet

Database Instance: av.us.oracle.com > Source Configuration Management

Logged in As AVADMIN

Source Configuration Management

Source | Collector

Source Type

Source

Go

Create

View Edit Delete

Select	Audit Source Type	Source	Host	Host IP	Version	Time Zone	User Name	Authentication	Audit Source Description
●	ORCLDB	RODSRC1.US.ORACLE.COM	localhost	127.0.0.1	10.2.0.3.0	PST	avsrcuser8	AUTH_TYPE_PWD	

Source | Collector

Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

From the **Source Configuration Management** page, you can:

- Enter a source type in the Source Type field and optionally enter a name of a source in the Source field, and then click **Go** to search for sources of that source type or a specific source of that source type.
- Select a source, then click **View** to view the properties and attributes for the source. After viewing the source properties and attributes on the **View Source Details** page, click **OK** to return to the **Source Configuration Management** page.

- Select a source, then click **Edit** to edit the properties and attributes for a source. On the **Edit Source Details** page, edit the desired properties and attributes for the source. Click **OK** to save your changes and return to the **Source Configuration Management** page.
- Select a source, then click **Delete** to delete that source. Once you delete that source, its name cannot be used again to create another source.
- Click **Create** to create a source. A series of three Add Source pages appears. On the **Add Source: Properties (Step 1 of 3)** page, enter the properties for the source, then click **Next**. On the **Add Source: Attributes (Step 2 of 3)** page, enter the attributes for the source, then click **Next**. On the **Add Source: Review (Step 3 of 3)** page, review the properties and attributes for the source that you are about to create. Click **Next** to create the source and return to the **Source Configuration Management** page, where you will see an entry for the source that you just created.

Click **Help** on any of the **Source Configuration Management** pages for more information.

4.1.3 Adding, Altering, and Dropping Collectors

This section describes configuring collectors using the AVCA utility. An Audit Vault collector is responsible for the collection of audit data for a source. The audit data is collected and sent to Oracle Audit Vault. A channel represents a session between a collector at the source and Oracle Audit Vault. A collector opens a channel to the audit service. After you issue the AVORCLDB setup command to set up the source at the agent (see Section 3.2).

The following information was provided to add each collector to Audit Vault using the following arguments in the AVORCLDB add_collector command:

- `-srcname <srcname>` – The source name from which this collector will collect audit data.
- `-srcusr <usr>/<password>` – The name and password of the source user granted the `AV_SOURCE` role to use this source. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`usr/password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
- `-agentname <agentname>` – The name of the agent to which this collector is associated.
- `-colltype [OSAUD,EVTLOG DBAUD,REDO]` – The type of collector this collector is OSAUD, EVTLOG, DBAUD, or REDO.
- `[-collname <collname>]` – Optional unique name of the collector.
- `[-desc <desc>]` – Optional brief description of the collector.
- `[-avsrcusr <usr>/<password>]` – Optional Audit Vault user and password associated with the given source. The argument is required if the `-colltype` argument value is REDO. The `-avsrcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_AVSRCUSR` is set to *`usr/password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
- `[-av <host:port:service>]` – Optional connection information for Audit Vault used for the database link from the source database to Audit Vault. This argument is required if the `-colltype` argument value is REDO.

- [-instname <instname>] – Optional instance name of Audit Vault Oracle Real Application Clusters (Oracle RAC) installation. This argument must be used to add multiple OSAUD collectors (one for each instance).

You can modify the following collector attribute information after its creation by using the optional <attrname>=<attrvalue> argument and by separating multiple pairs by a space on the command line. The following attributes can be modified by entering one or more sets of attribute name and value pairs to be changed in the AVORCLDB alter_collector command:

- COLLECTORTYPE – A new collector type for this collector
- NAME – A new name for this collector type
- COLLECTOR_NAME – A new name for this collector
- AGENT – A new name for the agent
- AUDIT_SERVICE_TYPE – A new type of audit service for this collector: default, filter, or batch
- SOURCE – A new source name for this collector
- DESCRIPTION – A new description for this collector

For the OSAUD collector, the following attributes can be modified (mutable) as noted:

- OSAUDIT_DEFAULT_FILE_DEST – The default directory for Oracle operating system audit files. The default value is $ORACLE_BASE/admin/DB_UNIQUE_NAME/adump. A valid value is a directory name on the host system. This attribute is mutable.
- OSAUDIT_FILE_DEST – The directory where Oracle operating system audit files can be found. The default value is $ORACLE_BASE/admin/DB_UNIQUE_NAME/adump. Another valid value is $ORACLE_HOME/rdbms/audit. This attribute is mutable.
- OSAUDIT_NLS_LANGUAGE – The NLS language of the data source. The default value is AMERICAN. This attribute is mutable.
- OSAUDIT_NLS_TERRITORY – The NLS territory of the data source. The default value is AMERICA. This attribute is mutable.
- OSAUDIT_NLS_CHARSET – The NLS character set of the data source. The default value is WE8ISO8859P1. This attribute is mutable.
- OSAUDIT_LOG_LEVEL – The log level: FATAL, ERROR, WARNING, INFO, and DEBUG. The default value is WARNING. This attribute is mutable.
- OSAUDIT_MAX_PROCESS_TIME – The maximum processing time for each call to process the collector (in centiseconds). A valid value is an integer value from 10 to 10000. The default value is 600. This attribute is mutable.
- OSAUDIT_MAX_PROCESS_RECORDS – The maximum number of records to be processed during each call to process the collector. A valid value is an integer value from 10 to 10000. The default value is 10000. This attribute is mutable.
- OSAUDIT_CHANNEL_TYPE – The channel type being used by the collector. The default value is NULL. This attribute is not mutable.
- OSAUDIT_AUDIT_VAULT_ALIAS – The alias name for the Audit Vault Server. The default value is NULL. This attribute is not mutable.
- OSAUD_NT_ORACLE_SID – The Oracle SID name on Windows systems. The default value is NULL. This attribute is mutable.

For the DBAUD collector, the following attributes can be modified (mutable) as noted:

- AUDAUDIT_DELAY_TIME – The amount of delay time (in seconds) for the DBAUD process. The default value is 20. This attribute is mutable.
- AUDAUDIT_SLEEP_TIME – The amount of sleep time (in seconds) for the DBAUD process. The default value is 5000. This attribute is mutable.
- AUDAUDIT_ACTIVE_SLEEP_TIME – The amount of active sleep time for the DBAUD process. The default value is 1000 (in seconds). This attribute is mutable.
- AUDAUDIT_MAX_PROCESS_RECORDS – The maximum processing time for each call to process the collector (in centiseconds). A valid value is an integer value from 10 to 10000. The default value is 1000. This attribute is mutable.
- AUDAUDIT_SORT_POLICY – The audit data sort policy. The default value is NULL. This attribute is mutable.
- AUDAUDIT_AUDIT_VAULT_ALIAS – The alias name for the Audit Vault Server. The default value is NULL. This attribute is not mutable.
- AUDAUDIT_SOURCE_ALIAS – The alias name for the audit data source. The default value is NULL. This attribute is not mutable.

For the REDO collector, the following attributes can be modified (mutable) as noted:

- STRCOLL_SRCADM_NAME – The name of the audit data source. The default value is NULL. This attribute is not mutable.
- STRCOLL_SRCADM_ALIAS – The alias name for the audit data source. The default value is NULL. This attribute is not mutable.
- STRCOLL_HEARTBEAT_TIME – The time, in seconds, between monitoring events for monitoring the status of the Audit Vault REDO collection system. The default value is 60. This attribute is mutable.
- STRCOLL_DBSERVICE – The service name of the audit data source Oracle database. The default value is NULL. This attribute is not mutable.
- STRCOLL_DBPORT – The port number of the audit data source Oracle database. The default value is NULL. This attribute is mutable.
- AV.DATABASE.NAME – The Audit Vault database name. The default value is NULL. This attribute is not mutable.

You can modify one or more attributes for a collector at a time using the AVORCLDB alter_collector command. See the AVORCLDB alter_collector command for more information.

To drop a collector, specify its name in an AVORCLDB drop_collector command.

The AVORCLDB drop_collector command does not delete the collector from Oracle Audit Vault. The drop_collector command disables the collector. Therefore, you can neither add a collector by the same name as the one that was dropped nor enable a collector that has been dropped.

To alter a collector, use the following AVORCLDB alter_collector command:

```
avorcldb alter_collector -collname testColl -srcname testSrc -colldesc "new desc"
```

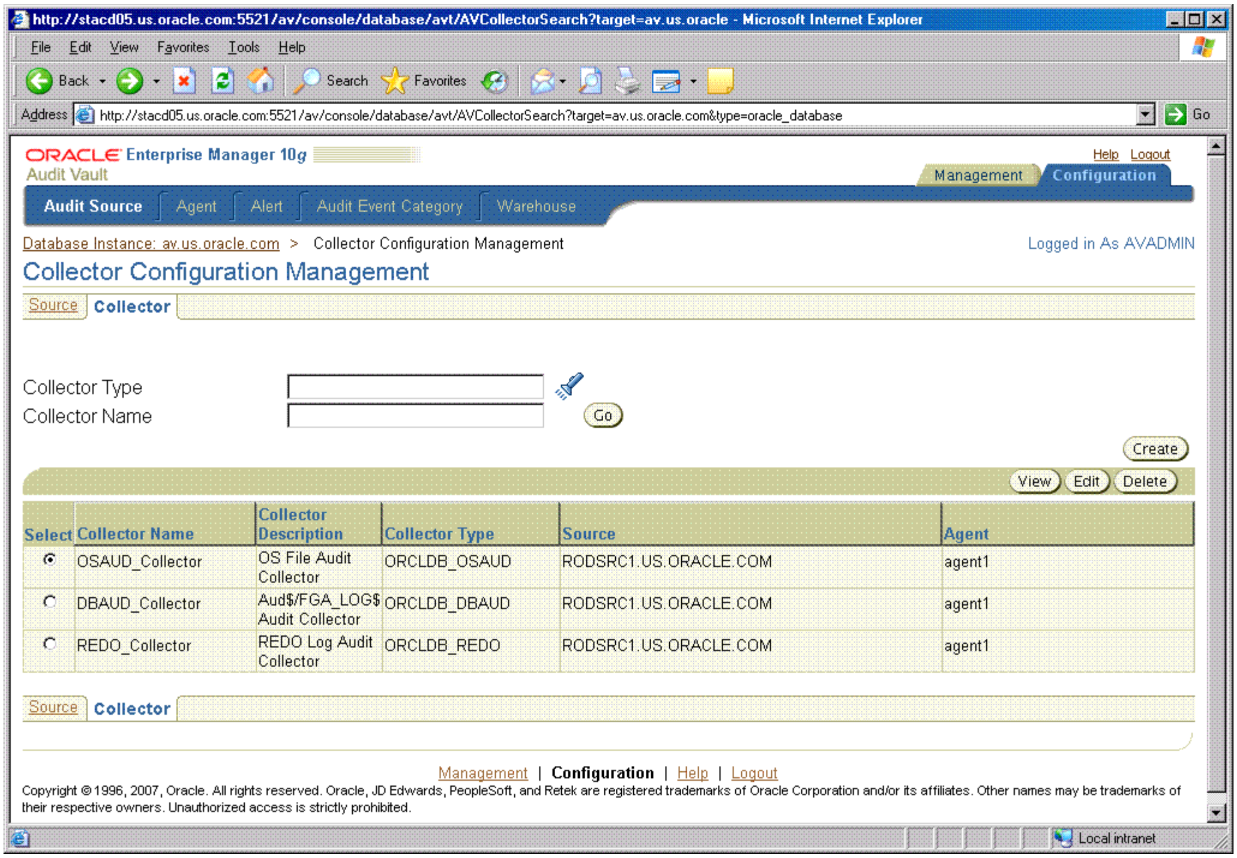
Use the AVORCLDB drop_collector command to drop a collector. For example:

```
avorcldb drop_collector -srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
-collname STREAMSCOLLECTOR
```

See Appendix C for reference information about each of these commands.

To use the Audit Vault Console to manage collectors, log in to the Audit Vault Console as the user with AV_ADMIN role granted. Click the **Configuration** tab, **Audit Source** tab, then the **Collector** subtab to display the **Collector Configuration Management** page (see Figure 4–3).

Figure 4–3 Collector Configuration Management Page


http://stacd05.us.oracle.com:5521/av/console/database/avt/AVCollectorSearch?target=av.us.oracle - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management
Configuration
Audit Source
Agent
Alert
Audit Event Category
Warehouse
Source
Collector
Go
Create
View
Edit
Delete
Source
Collector
Management | Configuration | Help | Logout
Local intranet

http://stacd05.us.oracle.com:5521/av/console/database/avt/AVCollectorSearch?target=av.us.oracle.com&type=oracle_database

Database Instance: av.us.oracle.com > Collector Configuration Management

Logged in As AVADMIN

Collector Configuration Management

Collector Type

Collector Name

Select	Collector Name	Collector Description	Collector Type	Source	Agent
●	OSAUD_Collector	OS File Audit Collector	ORCLDB_OSAUD	RODSRC1.US.ORACLE.COM	agent1
○	DBAUD_Collector	Aud$/FGA_LOG$ Audit Collector	ORCLDB_DBAUD	RODSRC1.US.ORACLE.COM	agent1
○	REDO_Collector	REDO Log Audit Collector	ORCLDB_REDO	RODSRC1.US.ORACLE.COM	agent1

Copyright © 1996, 2007, 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.

From the **Collector Configuration Management** page, you can:

- Enter a collector type in the Collector Type field and optionally enter a name of a collector in the Collector field, and then click **Go** to search for collectors of that collector type or a specific collector of that collector type.
- Select a collector, then click **View** to view the properties and attributes for the collector. After viewing the collector properties and attributes on the **View Collector Details** page, click **OK** to return to the **Collector Configuration Management** page.
- Select a collector, then click **Edit** to edit the properties and attributes for a collector. On the **Edit Collector Details** page, edit the desired properties and attributes for the collector. Click **OK** to save your changes and return to the **Collector Configuration Management** page.
- Select a collector, then click **Delete** to delete that collector. Once you delete that collector, its name cannot be used again to create another collector.
- Click **Create** to create a collector. A series of three Add Collector pages appears. On the **Add Collector: Properties (Step 1 of 3)** page, enter the properties for the collector, then click **Next**. On the **Add Collector: Attributes (Step 2 of 3)** page, enter the attributes for the collector, then click **Next**. On the **Add Collector:**

Review (Step 3 of 3) page, review the properties and attributes for the collector that you are about to create. Click **Next** to create the collector and return to the **Collector Configuration Management** page, where you will see an entry for the collector that you just created.

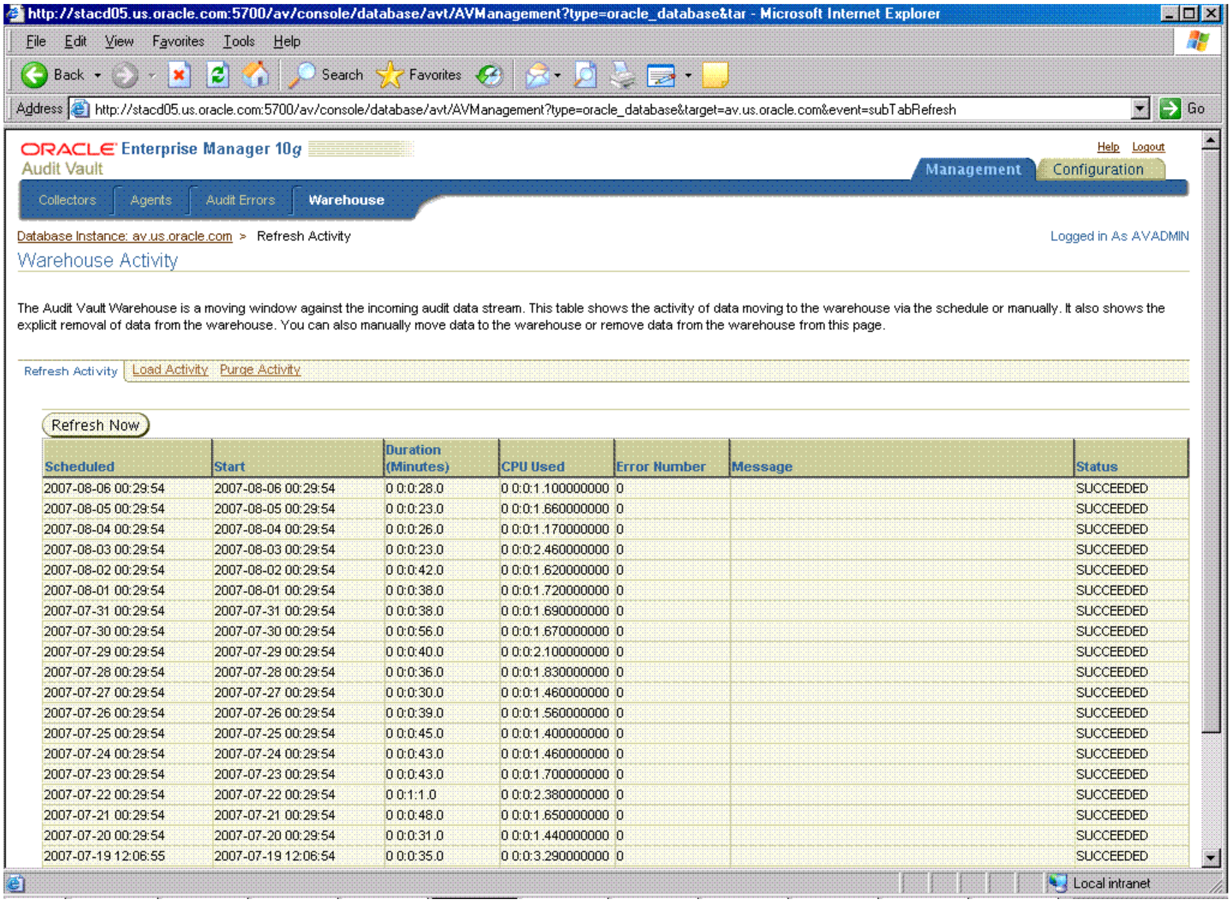
Click **Help** on any of the **Collector Configuration Management** pages for more information.

4.1.4 Configuring the Data Warehouse Schedule

Audit data moves to the data warehouse according to a specified schedule known as the warehouse schedule. After audit data is transferred from the source to the Audit Vault raw audit data store, an Oracle DBMS_SCHEDULER job runs an ETL (extract, transformation, load) process to normalize the raw audit data into the data warehouse. By default, the default DBMS_SCHEDULER job runs every 24 hours. Audit data is retained in the data warehouse for a specified period of time. Audit data can be refreshed in the data warehouse according to a schedule.

Audit Vault provides statistics of the ETL process to update the warehouse as shown in Figure 4–4. By utilizing the information provided in the `Duration in Minutes` and `CPU Used` columns, you can estimate how often the job may be run to update the data warehouse infrastructure.

Figure 4–4 History of Refreshing Page Showing Statistics of the ETL Process



Address: http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&target=av.us.oracle.com&event=subTabRefresh

Database Instance: av.us.oracle.com > Refresh Activity

Logged in As AVADMIN

Warehouse Activity

The Audit Vault Warehouse is a moving window against the incoming audit data stream. This table shows the activity of data moving to the warehouse via the schedule or manually. It also shows the explicit removal of data from the warehouse. You can also manually move data to the warehouse or remove data from the warehouse from this page.

Scheduled	Start	Duration (Minutes)	CPU Used	Error Number	Message	Status
2007-08-06 00:29:54	2007-08-06 00:29:54	0 0:0:28.0	0 0:0:1.100000000	0		SUCCEEDED
2007-08-05 00:29:54	2007-08-05 00:29:54	0 0:0:23.0	0 0:0:1.660000000	0		SUCCEEDED
2007-08-04 00:29:54	2007-08-04 00:29:54	0 0:0:26.0	0 0:0:1.170000000	0		SUCCEEDED
2007-08-03 00:29:54	2007-08-03 00:29:54	0 0:0:23.0	0 0:0:2.460000000	0		SUCCEEDED
2007-08-02 00:29:54	2007-08-02 00:29:54	0 0:0:42.0	0 0:0:1.620000000	0		SUCCEEDED
2007-08-01 00:29:54	2007-08-01 00:29:54	0 0:0:38.0	0 0:0:1.720000000	0		SUCCEEDED
2007-07-31 00:29:54	2007-07-31 00:29:54	0 0:0:38.0	0 0:0:1.690000000	0		SUCCEEDED
2007-07-30 00:29:54	2007-07-30 00:29:54	0 0:0:56.0	0 0:0:1.670000000	0		SUCCEEDED
2007-07-29 00:29:54	2007-07-29 00:29:54	0 0:0:40.0	0 0:0:2.100000000	0		SUCCEEDED
2007-07-28 00:29:54	2007-07-28 00:29:54	0 0:0:36.0	0 0:0:1.830000000	0		SUCCEEDED
2007-07-27 00:29:54	2007-07-27 00:29:54	0 0:0:30.0	0 0:0:1.460000000	0		SUCCEEDED
2007-07-26 00:29:54	2007-07-26 00:29:54	0 0:0:39.0	0 0:0:1.560000000	0		SUCCEEDED
2007-07-25 00:29:54	2007-07-25 00:29:54	0 0:0:45.0	0 0:0:1.400000000	0		SUCCEEDED
2007-07-24 00:29:54	2007-07-24 00:29:54	0 0:0:43.0	0 0:0:1.460000000	0		SUCCEEDED
2007-07-23 00:29:54	2007-07-23 00:29:54	0 0:0:43.0	0 0:0:1.700000000	0		SUCCEEDED
2007-07-22 00:29:54	2007-07-22 00:29:54	0 0:1:1.0	0 0:0:2.380000000	0		SUCCEEDED
2007-07-21 00:29:54	2007-07-21 00:29:54	0 0:0:48.0	0 0:0:1.650000000	0		SUCCEEDED
2007-07-20 00:29:54	2007-07-20 00:29:54	0 0:0:31.0	0 0:0:1.440000000	0		SUCCEEDED
2007-07-19 12:06:55	2007-07-19 12:06:54	0 0:0:35.0	0 0:0:3.290000000	0		SUCCEEDED

Use the AVCA set_warehouse_schedule command to refresh data from the raw audit data store by setting values for the following arguments:

- `-schedulename <schedule name>` – The schedule name
- `-startdate <start date>` – The start date
- `-rptintrv <repeat interval>` – The repeat interval
- `[-dateformat <date format>]` – Optional date format for the `-startdate` argument

The AVCA set_warehouse_schedule command is overloaded and can be used to either specify a schedule name created using `DBMS_SCHEDULER.create_schedule` procedure or specify a start date and repeat interval and optionally specify a particular date format. For example, the following AVCA set_warehouse_schedule command uses a start date and repeat interval argument to set the schedule for refreshing data from the raw audit data store to the star schema.

```
avca set_warehouse_schedule -startdate 01-JUL-06 -rptintrv 'FREQ=DAILY;BYHOUR=0'
```

Use the AVCA set_warehouse_retention command to control the amount of data kept online in the data warehouse fact table by setting values for the year month interval.

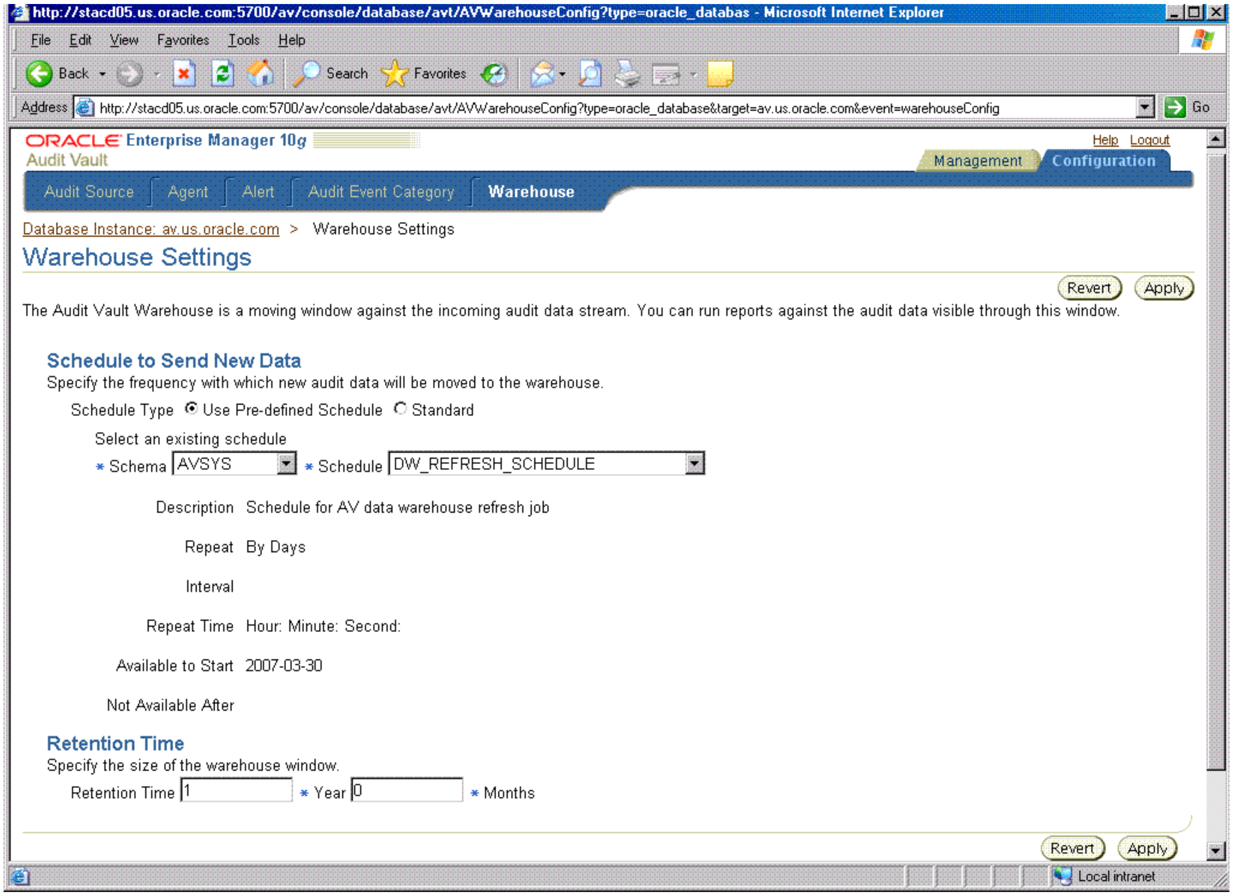
The following example controls the amount of data kept online in the data warehouse table for a time interval of one year.

```
avca set_warehouse_retention -intrv +01-00
```

See Appendix A for reference information about each of these commands.

To use the Audit Vault Console to set these warehouse settings, log in to the Audit Vault Console as the user with `AV_ADMIN` role granted. Click the **Configuration** tab, then the **Warehouse** subtab to display the **Warehouse Settings** page (see Figure 4–5).

Figure 4–5 Warehouse Settings Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVWarehouseConfig?type=oracle_databas - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://stacd05.us.oracle.com:5700/av/console/database/avt/AVWarehouseConfig?type=oracle_database&target=av.us.oracle.com&event=warehouseConfig Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management Configuration
Audit Source Agent Alert Audit Event Category Warehouse
Revert Apply
Local intranet

Database Instance: av.us.oracle.com > Warehouse Settings

Warehouse Settings

The Audit Vault Warehouse is a moving window against the incoming audit data stream. You can run reports against the audit data visible through this window.

Schedule to Send New Data

Specify the frequency with which new audit data will be moved to the warehouse.

Schedule Type ● Use Pre-defined Schedule ○ Standard

Select an existing schedule

* Schema AVSYS * Schedule DW_REFRESH_SCHEDULE

Description Schedule for AV data warehouse refresh job

Repeat By Days

Interval

Repeat Time Hour: Minute: Second:

Available to Start 2007-03-30

Not Available After

Retention Time

Specify the size of the warehouse window.

Retention Time 1 * Year 0 * Months

On the **Warehouse Settings** page, specify a standard schedule by selecting a **Schedule Type** of type **Standard**. Then specify the following frequency settings to move new audit data to the warehouse:

- **Frequency Type** by minutes, by hours, by days, weekly, monthly, or yearly
- **Interval (Days)** indicates the time between moving audit data to the warehouse
- **Time Zone** indicates the local time zone of the warehouse
- **Start Date** indicates the beginning day in which to move audit data to the warehouse
- **Start time** indicates the beginning time in which to move audit data to the warehouse

You can also specify a predefined schedule by selecting a **Schedule Type** of **Use Pre-defined Schedule** and then selecting the schema in the **Schema** field where the schedule is located and selecting the name of the schedule in the **Schedule** field.

Next, specify the retention time or length of time to retain the audit data in the warehouse in the **Retention Time** field.

Check your settings, then click **Apply** to save your warehouse settings.

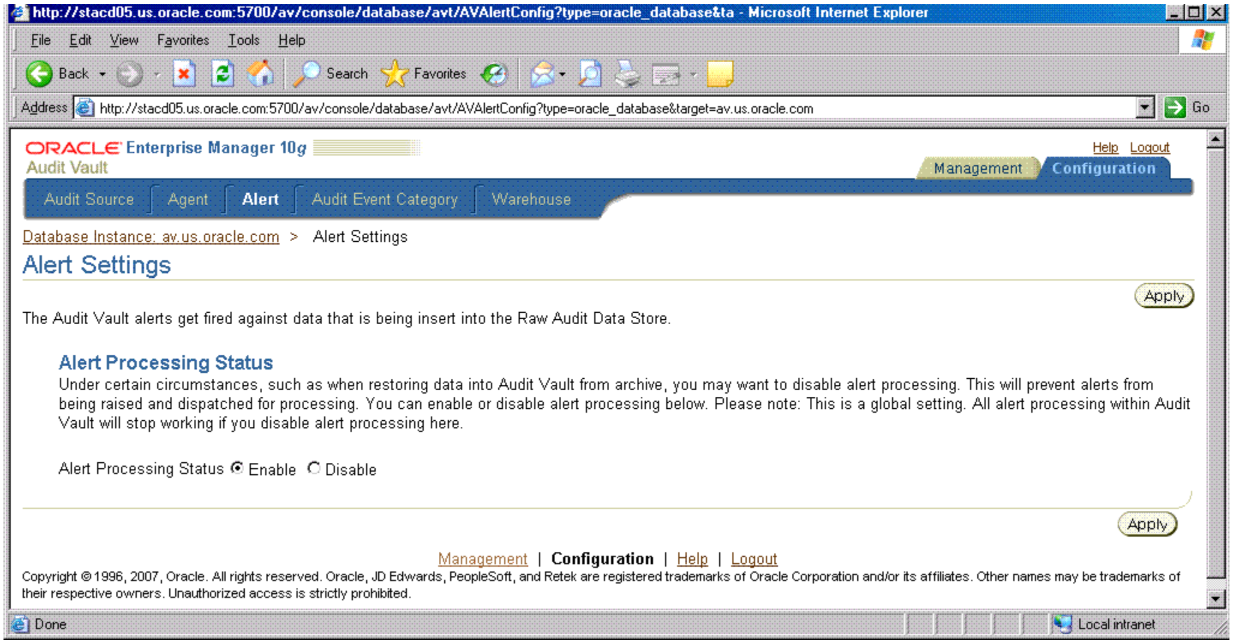
Click **Help** on the **Warehouse Settings** page for more information.

4.1.5 Globally Disabling and Enabling Alert Settings

Before loading audit data into the data warehouse that has been archived for long-term storage, you must disable alert processing so that alerts are not reissued again.

To use the Audit Vault Console to globally disable alert processing, log in to the Audit Vault Console as the user with `AV_ADMIN` role granted. Click the **Configuration** tab, then the **Alert** subtab to display the **Alert Settings** page (see Figure 4–6).

Figure 4–6 Alert Settings Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVAlertConfig?type=oracle_database&ta - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://stacd05.us.oracle.com:5700/av/console/database/avt/AVAlertConfig?type=oracle_database&target=av.us.oracle.com
Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management
Configuration
Audit Source
Agent
Alert
Audit Event Category
Warehouse
Database Instance: av.us.oracle.com > Alert Settings
Apply
Apply
Management | Configuration | Help | Logout
Done
Local intranet

Alert Settings

The Audit Vault alerts get fired against data that is being insert into the Raw Audit Data Store.

Alert Processing Status

Under certain circumstances, such as when restoring data into Audit Vault from archive, you may want to disable alert processing. This will prevent alerts from being raised and dispatched for processing. You can enable or disable alert processing below. Please note: This is a global setting. All alert processing within Audit Vault will stop working if you disable alert processing here.

Alert Processing Status ● Enable ○ Disable

Copyright © 1996, 2007, 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.

On the **Alert Settings** page, at the **Alert Processing Status** field, click the **Disable** option to globally disable alert processing, then click **Apply**.

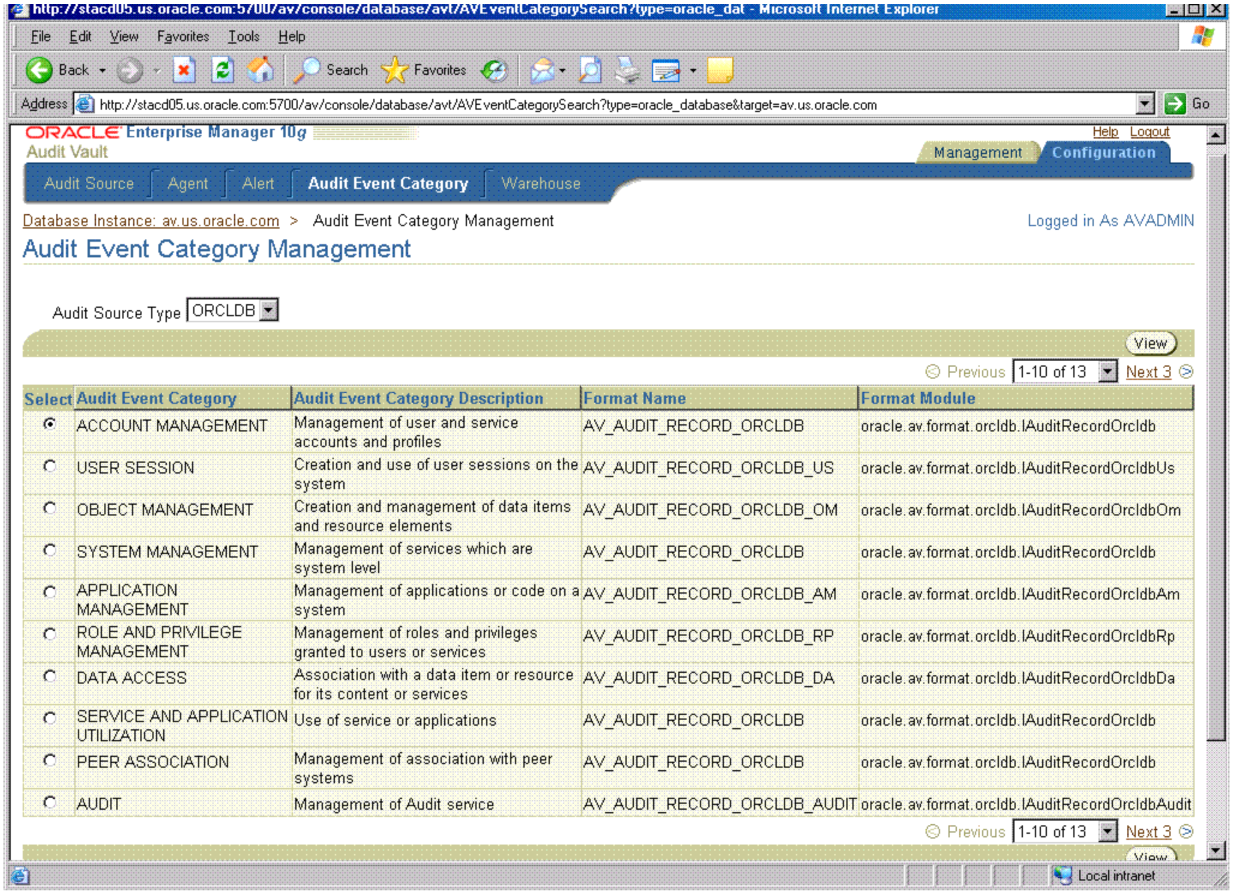
Click **Help** on the **Alert Settings** page for more information.

4.1.6 Viewing Audit Event Categories

Audit event category management consists of viewing the Audit Vault audit event categories, their attributes, and their audited events.

To use the Audit Vault Console to view the audit event categories, log in to the Audit Vault Console as the user with `AV_ADMIN` role granted. Click the **Configuration** tab, then the **Audit Event Category** subtab to display the **Audit Event Category Management** page (see Figure 4–7).

Figure 4–7 Audit Event Category Management Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVEventCategorySearch?type=oracle_dat - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://stacd05.us.oracle.com:5700/av/console/database/avt/AVEventCategorySearch?type=oracle_database&target=av.us.oracle.com Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management Configuration
Audit Source Agent Alert Audit Event Category Warehouse
Database Instance: av.us.oracle.com > Audit Event Category Management
Logged in As AVADMIN
View
Previous 1-10 of 13 Next 3
Local intranet

Audit Event Category Management

Audit Source Type ORCLDB

Select	Audit Event Category	Audit Event Category Description	Format Name	Format Module
●	ACCOUNT MANAGEMENT	Management of user and service accounts and profiles	AV_AUDIT_RECORD_ORCLDB	oracle.av.format.orcldb.IAuditRecordOrcldb
○	USER SESSION	Creation and use of user sessions on the system	AV_AUDIT_RECORD_ORCLDB_US	oracle.av.format.orcldb.IAuditRecordOrcldbUs
○	OBJECT MANAGEMENT	Creation and management of data items and resource elements	AV_AUDIT_RECORD_ORCLDB_OM	oracle.av.format.orcldb.IAuditRecordOrcldbOm
○	SYSTEM MANAGEMENT	Management of services which are system level	AV_AUDIT_RECORD_ORCLDB	oracle.av.format.orcldb.IAuditRecordOrcldb
○	APPLICATION MANAGEMENT	Management of applications or code on a system	AV_AUDIT_RECORD_ORCLDB_AM	oracle.av.format.orcldb.IAuditRecordOrcldbAm
○	ROLE AND PRIVILEGE MANAGEMENT	Management of roles and privileges granted to users or services	AV_AUDIT_RECORD_ORCLDB_RP	oracle.av.format.orcldb.IAuditRecordOrcldbRp
○	DATA ACCESS	Association with a data item or resource for its content or services	AV_AUDIT_RECORD_ORCLDB_DA	oracle.av.format.orcldb.IAuditRecordOrcldbDa
○	SERVICE AND APPLICATION UTILIZATION	Use of service or applications	AV_AUDIT_RECORD_ORCLDB	oracle.av.format.orcldb.IAuditRecordOrcldb
○	PEER ASSOCIATION	Management of association with peer systems	AV_AUDIT_RECORD_ORCLDB	oracle.av.format.orcldb.IAuditRecordOrcldb
○	AUDIT	Management of Audit service	AV_AUDIT_RECORD_ORCLDB_AUDIT	oracle.av.format.orcldb.IAuditRecordOrcldbAudit

On the Audit Event Category Management page, audit event categories appear in tabular format, showing the following columns:

- Audit Event Category
- Audit Event Category Description
- Format Name
- Format Module

From the **Audit Event Category Management** page, you can select an Audit Source Type and then view the audit event categories for that audit source type. The only audit source type available in this release is ORCLDB, the Oracle Database audit source type.

From the **Audit Event Category Management** page, you can select an audit event category, then click **View** to view its attributes and audit events on the **View Audit Event Category** page. From the **View Audit Event Category** page, the **Attributes** tab appears by default, showing the attributes for the selected audit event category. Click the **Audit Events** tab to display the audit events that are audited for the selected audit event category.

Click **Help** on any of the **Audit Event Category Management** pages for more information.

4.2 Managing Audit Vault

Managing Audit Vault consists of performing the following tasks as needed or as indicated in Chapter 3:

- Managing Audit Vault Server
- Managing the Agent OC4J
- Starting and Stopping Agents
- Starting and Stopping Collectors
- Refreshing, Loading, and Purging the Data Warehouse
- Viewing Audit Vault Errors

4.2.1 Managing Audit Vault Server

On occasion, you might need to shut down Audit Vault Console, for example, as part of the process of removing Audit Vault Console from the system.

To shut down Audit Vault Console, use the AVCTL stop_av command, which executes an `emctl stop dbconsole` command. For example:

```
avctl stop_av
```

To check the status of Audit Vault Console, use the AVCTL show_av_status command.

```
avctl show_av_status
```

To start the Audit Vault Console, use the AVCTL start_av command, which executes an `emctl start dbconsole` command. For example:

```
avctl start_av
```

4.2.2 Managing the Agent OC4J

The agent OC4J process might terminate abnormally, and you might need to restart it manually. However, first you might want to check its status.

To check the status of agent OC4,use the AVCTL show_oc4j_status command.

```
avctl show_oc4j_status
```

To start the agent OC4J, use the AVCTL start_oc4j command. For example:

```
avctl start_oc4j
```

If the agent OC4J process must be halted, for example, as one of steps for removing the Audit Vault Agent software from a system, use the AVCTL stop_oc4j command. For example:

```
avctl stop_oc4j
```

4.2.3 Starting and Stopping Agents

An agent is first installed on the system on which an audit source resides. Next, the agent is deployed as part of the installation process. This operation deploys the Audit Vault Agent into the standalone OC4J instance. Then the method of authentication is determined for the agent to communicate with the Audit Vault system. Finally, the network communication is established between the agent and its collectors and the

Audit Vault system. Once these tasks are completed as part of the postinstallation process, the agent is ready to be managed.

To manage an agent, use the AVCTL utility. When an AVCTL start_agent command is issued for an agent and that command is successful, the agent and its set of collectors are put into a RUNNING state. To check the agent status, issue the show_agent_status command. The AVCTL stop_agent command is issued to stop an agent so that you can perform maintenance on it.

The following AVCTL start_agent command starts the agent:

```
avctl start_agent -agentname OC4JAGENT1
```

The following AVCTL show_agent_status command checks the agent status.

```
avctl show_agent_status -agentname OC4JAGENT1
```

The following AVCTL stop_agent command stops the agent:

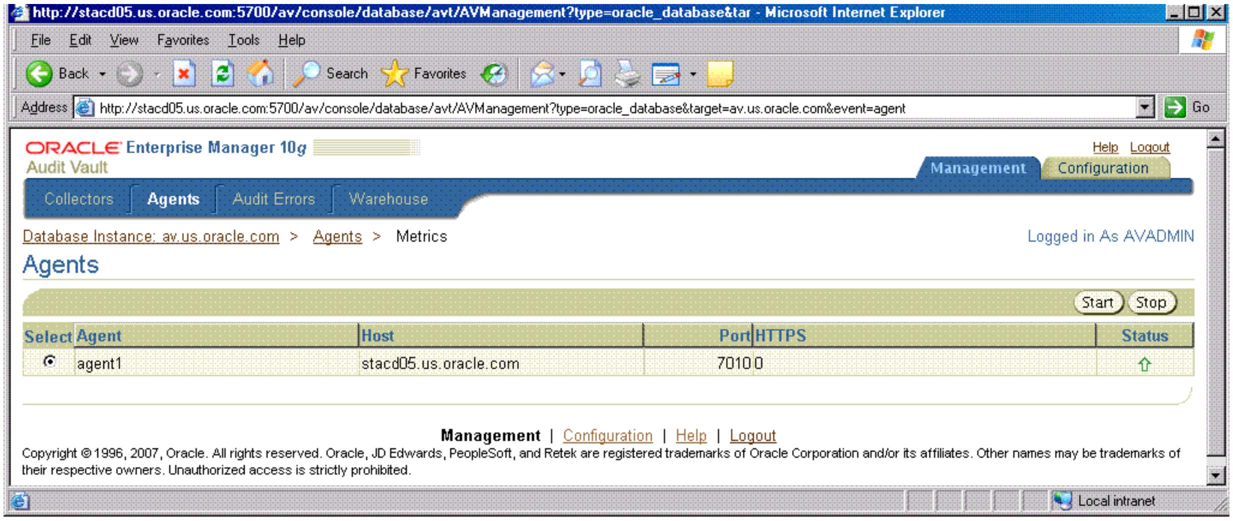
```
avctl stop_agent -agentname OC4JAGENT1
```

See Appendix B for reference information about each of these commands.

To manage agent metadata, use the AVCA utility. See Section 3.3 for tutorial information and see Appendix A for reference information.

To use the Audit Vault Console to manage agents, log in to the Audit Vault Console as the user with the AV_ADMIN role granted. Click the **Management** tab, then the **Agents** subtab to display the **Agents** page (see Figure 4–8).

Figure 4–8 Agents Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&tar - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management
Configuration
Collectors
Agents
Audit Errors
Warehouse
Start
Stop
Local intranet

Address: http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&target=av.us.oracle.com&event=agent

Database Instance: av.us.oracle.com > Agents > Metrics

Logged in As AVADMIN

Agents

Select	Agent	Host	Port	HTTPS	Status
●	agent1	stacd05.us.oracle.com	7010	0	⇧

Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

On the **Agents** page, you can view agent information and start and stop agents. Agent information includes:

- **Agent** – Name of the agent
- **Host** – The host name where the agent is installed
- **Port** – The port number of the host system where the agent is installed
- **HTTPS** – Whether or not the agent is communicating with the Audit Vault Server using a secure communication channel (HTTPS)

- **Status** – The current running status of the agent: an up green arrow indicates the agent is running; a down red arrow indicates the agent is not running, or error indicates the agent is in an error state

To start an agent, select the agent and click **Start**. To stop an agent, select the agent and click **Stop**.

Click **Help** for more information.

4.2.4 Starting and Stopping Collectors

Once an agent is installed, deployed, and started so that it is in a RUNNING state, you can set up collectors on the sources where the agent resides.

The following AVCTL start_collector command starts the collector named REDO_Collector in Oracle Audit Vault:

```
avctl start_collector -collname REDO_Collector
-srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
```

The following AVCTL show_collector_status command checks the collector status of the REDO_Collector collector.

```
avctl show_collector_status -collname REDO_Collector
                            -srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
```

The following AVCTL stop_collector command stops the collector named REDO_Collector in Oracle Audit Vault:

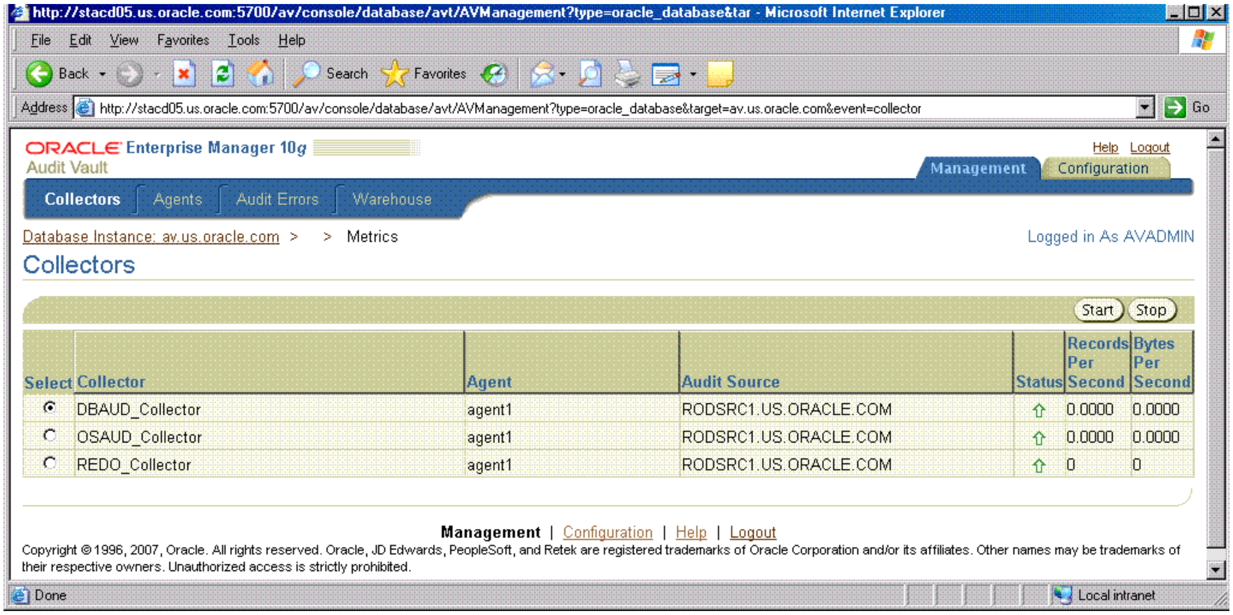
```
avctl stop_collector -collname REDO_Collector
-srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
```

See Appendix B for reference information about each of these commands.

To manage collector metadata, use the AVCA and AVORCLDB utilities. See Section 3.3 for tutorial information and see Appendix A and Appendix C for reference information.

To use the Audit Vault Console to manage collectors, log in to the Audit Vault Console as the user with AV_ADMIN role granted. Click the **Management** tab, then the **Collectors** subtab to display the **Collectors** page (see Figure 4–9).

Figure 4–9 Collectors Page



http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&tar - Microsoft Internet Explorer

Address: http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&target=av.us.oracle.com&event=collector

Database Instance: av.us.oracle.com > > Metrics

Logged in As AVADMIN

Collectors

Select	Collector	Agent	Audit Source	Status	Records Per Second	Bytes Per Second
●	DBAUD_Collector	agent1	RODSRC1.US.ORACLE.COM	↑	0.0000	0.0000
○	OSAUD_Collector	agent1	RODSRC1.US.ORACLE.COM	↑	0.0000	0.0000
○	REDO_Collector	agent1	RODSRC1.US.ORACLE.COM	↑	0	0

Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

On the **Collectors** page, you can view collector information and start and stop collectors. Collector information includes:

- **Collector** – Name of the collector
- **Agent** – The name of the agent for this collector
- **Audit Source** – The name of the audit data source
- **Status** – The current running status of the collector: an up green arrow indicates the collector is running, a down red arrow indicates the collector is not running, an error indicates that the collector is in an error state
- **Records Per Second** – The number of records per second being collected for the current time period
- **Bytes Per Second** – The number of bytes per second in audit records being collected for the current time period

To start a collector, select the collector and click **Start**. To stop a collector, select the collector and click **Stop**.

Click **Help** for more information.

4.2.5 Refreshing, Loading, and Purging the Data Warehouse

Use the Audit Vault Console to manage or view the history of refreshing, purging, and loading the data warehouse.

Use the AVCA command-line utility to populate the star schema with data from the raw audit data store, to refresh the data warehouse dimensions and fact tables with the data in the raw audit data store since the last refresh operation, and to remove audit data from the data warehouse. See the AVCTL load_warehouse, purge_warehouse, and refresh_warehouse commands for reference information.

For example, once audit records are collected and sent to the raw audit data store, refresh the warehouse to populate the warehouse with this fresh set of collected audit records for analysis. In the Audit Vault Server home shell, issue an AVCTL refresh_warehouse command specifying the `-wait` argument, as shown in Example 4–1.

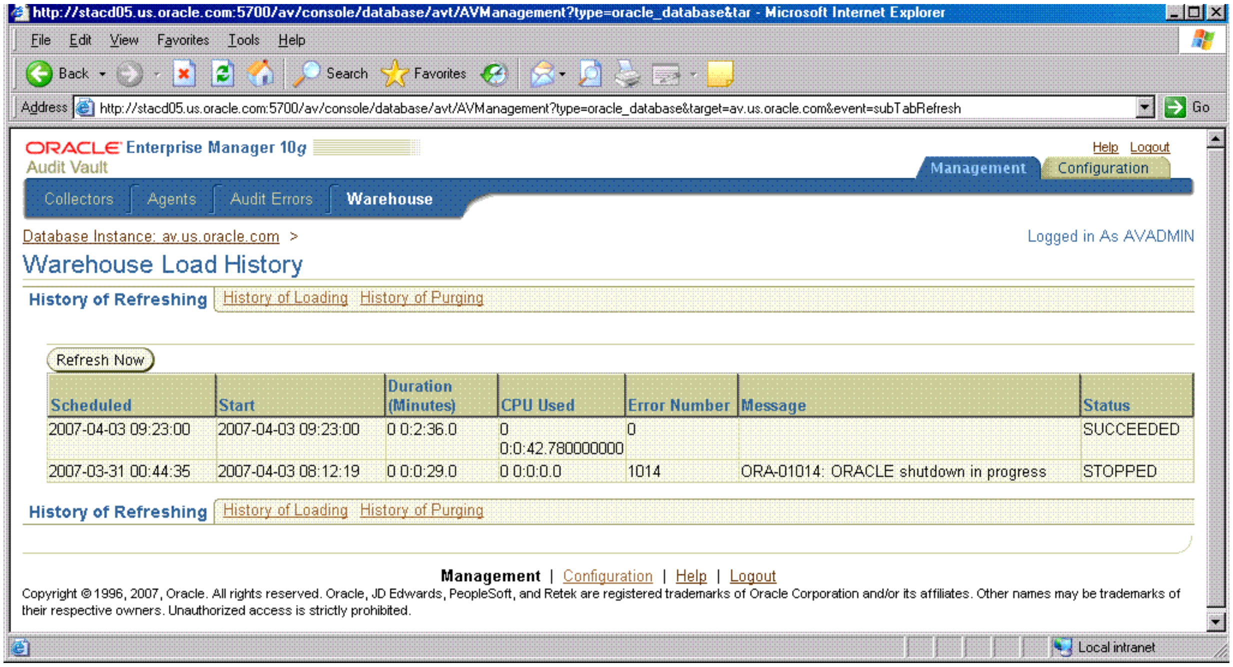
Example 4–1 Refreshing the Warehouse

```
avctl refresh_warehouse -wait
AVCTL started
Refreshing warehouse...
Waiting for refresh to complete...
done.
```

See Appendix B for reference information about each of these commands.

To use the Audit Vault Console to view warehouse history information, log in to the Audit Vault Console as the user with the AV_ADMIN role granted. Click the **Management** tab, then the **Warehouse** subtab to display the **Warehouse Load History** page. From this page, you can select the **History of Refreshing** page (see Figure 4–10), the **History of Loading** page, or the **History of Purging** page.

Figure 4–10 Warehouse Load History: History of Refreshing Page



http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&tar - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&target=av.us.oracle.com&event=subTabRefresh Go
ORACLE Enterprise Manager 10g
Audit Vault
Help Logout
Management Configuration
Collectors Agents Audit Errors Warehouse
Database Instance: av.us.oracle.com >
Logged in As AVADMIN

Warehouse Load History

History of Refreshing History of Loading History of Purging
Refresh Now

Scheduled	Start	Duration (Minutes)	CPU Used	Error Number	Message	Status
2007-04-03 09:23:00	2007-04-03 09:23:00	0 0:2:36.0	0 0:0:42.780000000	0		SUCCEEDED
2007-03-31 00:44:35	2007-04-03 08:12:19	0 0:0:29.0	0 0:0:0.0	1014	ORA-01014: ORACLE shutdown in progress	STOPPED

History of Refreshing History of Loading History of Purging
Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

On the **History of Refreshing** page, you can view warehouse refresh history information in tabular format that includes the following column headings:

- **Scheduled** – The scheduled time to perform a refresh operation
- **Start** – The start time when a refresh operation started
- **Duration (minutes)** – The total time required to complete a refresh operation
- **CPU Used** – The amount of time used to complete a refresh operation
- **Error Number** – The Oracle ORA- error number, if any, resulting from a refresh operation
- **Message** – Any error messages, if any, resulting from a refresh operation
- **Status** – The current status of a refresh operation: STOPPED or SUCCEEDED

Click **Refresh Now** to refresh the warehouse with audit data.

From the **Warehouse Load History** page, click **History of Loading** to display the **History of Loading** page. This page displays information about archived warehouse information that is reloaded into the warehouse. The column headings in tabular format that appear are identical to those in the **History of Refreshing** page described previously.

Click **Load Now** to load the warehouse with archived warehouse audit data.

From the **Warehouse Load History** page, click **History of Purging** to display the **History of Purging** page. This page displays information about warehouse audit data removed from the warehouse. The column headings in tabular format that appear are identical to those in the **History of Refreshing** page described previously.

Click **Purge Now** to purge the current warehouse audit data from the warehouse.

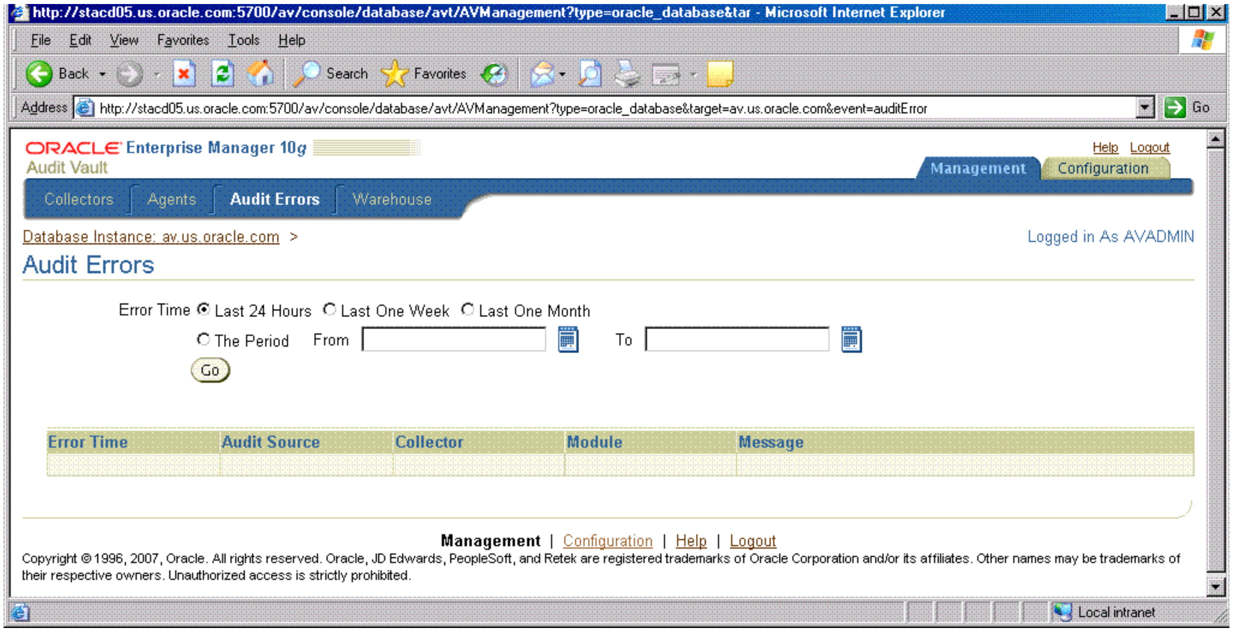
Click **Help** on any of the warehouse history pages for more information.

4.2.6 Viewing Audit Vault Errors

Audit Vault errors are logged in to an error table. You can view these errors using the Audit Vault Console.

To use the Audit Vault Console to view Audit Vault errors, log in to the Audit Vault Console as the user with AV_ADMIN role granted. Click the **Management** tab, then the **Audit Errors** subtab to display the **Audit Errors** page (see Figure 4–11).

Figure 4–11 Audit Errors Page


http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&tar - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://stacd05.us.oracle.com:5700/av/console/database/avt/AVManagement?type=oracle_database&target=av.us.oracle.com&event=auditError
Go
ORACLE Enterprise Manager 10g
Audit Vault
Help
Logout
Management
Configuration
Collectors
Agents
Audit Errors
Warehouse
Local intranet

Database Instance: av.us.oracle.com >

Logged in As AVADMIN

Audit Errors

Error Time ● Last 24 Hours ○ Last One Week ○ Last One Month

○ The Period From [ ] To [ ]

Go

Error Time	Audit Source	Collector	Module	Message

Management | Configuration | Help | Logout

Copyright © 1996, 2007, 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.

On the **Audit Errors** page, you can search for audit errors for a given time period. To do this, select one of the Error Time field options: **Last 24 Hours**, **Last One Week**, or **Last One Month**, and then click **Go**.

You can also search for audit errors for a given time period by selecting The Period field option and in the From field, enter a date and time or click the calendar icon to select a date and time, in the To field, enter a date and time or click the calendar icon to select a date and time, and then click **Go**.

On the **Audit Errors** page, you can view the error information in tabular format with the following column headings:

- **Error Time** – Local time when the audit error was generated

- **Audit Source** – The audit source on which the audit error originated
- **Collector** – The collector on which the audit error originated
- **Module** – The module name involved in the audit error
- **Message** – The content of the audit error message

Click **Help** for more information.

5 Administrative Tasks

This chapter describes important administrative tasks to perform on the Audit Vault system. These tasks are especially important if your audit data collectors are collecting high volumes of audit records and rapidly filling default tablespace and disk space settings.

The Audit Vault system Administrator should perform the following administrative tasks on a running Audit Vault system:

- Monitoring Space Usage on the SYSAUX Tablespace
- Monitoring Disk Space Usage Where Archive Logs Are Stored
- Setting Up an Agent Listener to Listen to Other Nodes in an Oracle RAC Environment
- Making Connectivity to the Source from the Audit Vault Agent More Highly Available in an Oracle RAC Environment
- Changing Audit Vault User Passwords on a Regular Basis
- Back Up and Recovery of Oracle Audit Vault

5.1 Monitoring Space Usage on the SYSAUX Tablespace

Following an Audit Vault Server installation and the creation of the Audit Vault database, the `SYSAUX` tablespace is created by default with one data file. The `SYSAUX` tablespace is a locally managed tablespace with automatic segment space management.

The Audit Vault administrator should monitor the space usage for the `SYSAUX` tablespace and set up additional datafiles for storage as needed. See *Oracle Database Administrator's Guide* for more information about the `SQL ALTER TABLESPACE` command.

5.2 Monitoring Disk Space Usage Where Archive Logs Are Stored

During an Audit Vault Server installation, ARCHIVELOG mode is turned on by default. For this reason, the Audit Vault administrator must monitor the disk space usage for these files to prevent a small disk from quickly filling to capacity. See *Oracle Database Administrator's Guide* for more information about changing the LOG_ARCHIVE_DEST_n location to relocate these archive log files to larger disks. For information about backing up the archive logs, see *Oracle Database Backup and Recovery Advanced User's Guide*.

5.3 Setting Up an Agent Listener to Listen to Other Nodes in an Oracle RAC Environment

In an Oracle Real Application Clusters (Oracle RAC) environment, after the Audit Vault Agent is set up, the node on which the agent was installed has its listener set up to listen to only that node. Thus, only that node can be specified to which to connect. However, the administrator can set up the listener to listen to the other nodes.

For the OSAUD and DBAUD collectors, the Administrator must update the `tnsnames.ora` file during installation of the Audit Vault Agents.

After the agent is set up, the `tnsnames.ora` file located in `$ORACLE_HOME/network/admin` might have the following alias:

```
AV = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = node01)
(PORT = 1521))(CONNECT_DATA = (SERVICE_NAME = av.us.oracle.com)))
```

For high availability, the administrator might need to edit the Audit Vault Agent home `tnsnames.ora` file after the agent is set up and add the host and port of the other listeners. For example:

```
AV =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = node01)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = node02)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = node03)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = node04)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
        (SERVICE_NAME = av.us.oracle.com)
    )
  )
```

For the REDO collector, the administrator must log in as the *`srcuser`* at the source database and re-create the database link for `av.us.oracle.com`. The new database link can either have a list of host and port numbers or point to a `tnsnames` entry with the list of host and port numbers.

5.4 Making Connectivity to the Source from the Audit Vault Agent More Highly Available in an Oracle RAC Environment

When a source is added to Oracle Audit Vault, the Audit Vault administrator must provide the `host:port:service` information for the source being added. This information is used for the following tasks from the agent:

- REDO collector: starting and stopping the capture process on the source
- DBAUD collector: retrieving rows from aud$ and fga_log$ tables
- Policy management: retrieving source dictionary information

Typically, when the Oracle Database instance on the host goes down or if the host machine goes down, the connectivity to the source from the Audit Vault Agent is broken and any attempt to perform these tasks is unsuccessful because this connection is not available:

The Audit Vault administrator can do any or all of the following operations to make the connection between the source and the Audit Vault Agent more highly available:

- Update in the Audit Vault Agent home, the `tnsnames.ora` file in the `/network/admin` directory on Linux or UNIX systems or in the \network\admin directory on Windows systems to add additional host or port information for the service. The user can also add options for load balancing and failure in the connect string. For additional information, see *Oracle Database Net Services Administrator's Guide* and specifically Chapter 13 "Enabling Advanced Features of Oracle Net Services".
- Configure a listener on the Oracle RAC nodes to support connecting to remote nodes and configuring the Oracle Database to communicate with remote listeners. This will help in the situation when the Oracle Database instance goes down, then the listener on the host can create connections on a different Oracle RAC node. For additional information, see *Oracle Database Net Services Administrator's Guide* and specifically Chapter 10 "Configuring and Administering the Listener".
- Provide host information using the virtual IP address of the node instead of the physical IP address. This will help when the host machine goes down, then all traffic to the host will get redirected to a different node.

5.5 Changing Audit Vault User Passwords on a Regular Basis

Most businesses and groups adhere to some internal policy for changing user name passwords. This is usually part of a password management policy. This policy often requires users to make password changes on a regular basis, such as every 120 days. Changing Audit Vault user name passwords should be considered part of the same password management policy. This section provides additional information about Audit Vault user names and source user names and how and where password changes are implemented.

Table 5–1 shows where the passwords for the Audit Vault user names and source user names are stored and where password changes must be made. Note that if a password for a source user name is updated in the source database, then the password, because it is also stored in the wallet in the Audit Vault Agent home, must also be updated.

Table 5–1 Where Passwords for the Audit Vault User Names and Source User Names Are Stored

Audit Vault Role	Audit Vault User Name	Is Password Stored in Wallet?	How Is Password Change Made?
`AV_ADMIN`	*`avadminusr`*	Yes	Use the `mkstore` command-line utility to change the password in the wallet in the Audit Vault Server home
`AV_AGENT`	*`avagentusr`*	Yes	Use the `mkstore` command-line utility to change the password in the wallet in the Audit Vault Agent home
Source user on source database	*`srcusr`*	Yes	Use the SQL `ALTER USER` command on the source databaseAudit Vault Server home. Use the `mkstore` command-line utility to change the password in the wallet in the Audit Vault Agent home
`AV_AUDITOR`	*`avauditorusr`*	No	Use the SQL `ALTER USER` command in the Audit Vault Server home
`AV_SOURCE`	*`avsrcusr`*	No	Use the SQL `ALTER USER` command in the Audit Vault Server home

Change the Passwords of the *avauditorusr* and *avsrcusr* User Names in the Audit Vault Server Home

To change the passwords of the avauditorusr and the avsrcusr user names, make the change in the Audit Vault Server home in the Audit Vault database using the SQL ALTER_USER command. Log in as the user with the role of Database Vault Account Manager.

For example, to change passwords of the avauditorusr and avsrcusr user names, perform the following steps:

1. Log in to SQL*Plus as the Database Vault Account Manager.

   For the Basic installation, log in as follows:

   ```
   sqlplus /nolog
   SQL> connect <avadmin>dva
   Enter password: <avadmin user password>
   Connected.
   SQL>
   ```

   For the Advanced installation, log in as follows:

   ```
   sqlplus /nolog
   SQL> connect <dv_acctmgr user name>
   Enter password: <dv_acctmgr user password>
   Connected.
   SQL>
   ```

2. To change the *avauditorusr name* password, use the SQL ALTER USER command.

   ```
   SQL> alter user <avauditorusr name> identified by <avauditorusr password>;
   ```

3. To change the *avsrcusr name* password, use the SQL ALTER USER command.

   ```
   SQL> alter user <avsrcusr name> identified by <avsrcusr password>;
   SQL> exit
   ```

Change the Password of the *avadminusr* User Name in the Audit Vault Server Home

To change the password of the *avadminusr* user name in the wallet location, use the mkstore command-line utility found in the $ORACLE_HOME/bin directory on LINUX and UNIX systems or found in the ORACLE_HOME\bin directory on Windows systems of the Audit Vault Server home.

For example, to change password of the *avadminusr* user name, perform the following steps in the Audit Vault Server home:

1. To list all entries (all database service names (aliases) and the corresponding user name (schema) for that database) in the wallet, use the following mkstore command. The password that you enter is the current *avadminusr* user name password. For example:

   ```
   mkstore -wrl ORACLE_HOME/network/admin/avwallet -listCredential
   Enter password: <current avadminusr password>

   List credential (index: connect_string username)
   1: av avadminusr
   ```

2. To update the password for the credential, use the following mkstore command. The password that you enter is the new avadminusr user name password. At the

`Enter password:` prompt, enter the new password for the `avadminusr` user name. For example:

```
mkstore -wrl ORACLE_HOME/network/admin/avwallet -modifyCredential av avadmin
<new avadminusr password>
Enter password: <new avadminusr password>
```

Change the Passwords of the *avagentusr* and *srcusr* User Name in the Audit Vault Agent Home

To change the passwords of the *`avagentusr`* and *`srcusr`* user names in the wallet location, use the `mkstore` command-line utility found in the `$ORACLE_HOME/bin` directory on LINUX and UNIX systems or found in the `ORACLE_HOME\bin` directory on Windows systems of the Audit Vault Agent home.

For example, to change the passwords of the *`avagentusr`* and *`srcusr`* user names, perform the following steps in the Audit Vault Agent home:

1. To list all entries (all database service names (aliases) and the corresponding user name (schema) for that database) in the wallet, use the following `mkstore` command. The password that you enter is the current *`avagentusr`* user name password. For example:

   ```
   mkstore -wrl ORACLE_HOME/network/admin/avwallet -listCredential
   Enter password: <current avagentusr password>
   List credential (index: connect_string username)
   1: AV avagentusr
   2: SRCDB1 srcusr
   ```

2. To update the passwords, use the following `mkstore` command. The passwords that you enter are the new *`avagentusr`* user name password or the new *`srcusr`* user name password. At the `Enter password:` prompt, enter the new password for each user name. For example:

   ```
   mkstore -wrl $ORACLE_HOME/network/admin/avwallet -modifyCredential AV
   agentuser1 <new avagntusr password>
   Enter password: <new avagntusr password>

   mkstore -wrl ORACLE_HOME/network/admin/avwallet -modifyCredential SRCDB1 srcusr
   <new srcusr password>
   Enter password: <new srcusr password>
   ```

Check To Ensure All Changed User Name Passwords Work Correctly

Always check to make sure all changed passwords for Audit Vault user names and source user names are working correctly. To check the passwords of the *`avadminusr`* and *`avauditorusr`* user name, open a Web browser and log in to the Audit Vault Console as the Audit Vault administrator. Then log out and log in to the Audit Vault Console as the Audit Vault auditor. A successful log in indicates that the new *`avadminusr`* and *`avauditor`* user name passwords are working fine. If your login is not successful after several attempts, repeat the steps previously mentioned in this section to change the password again for that particular Audit Vault user name and retry the login.

Next, stop the agent and collectors and start the agent and each collector. If the agent and the collectors each start up and collectors are collecting audit records again, the new *`avagntusr`*, *`avsrcusr`*, and *`srcusr`* user name passwords are all working.

If you experience problems, check the log files (see Chapter 6 for more information) to determine which user name password might be the source of the problem. Then, if needed, repeat the steps previously mentioned to change the password for that user name and try to start up the agent and the collectors again.

5.6 Back Up and Recovery of Oracle Audit Vault

Oracle Audit Vault patches do not have the ability to be rolled back, therefore you should take precautions to backup the files before any Oracle Audit Vault patch is applied until you have tested the patchset apply.

Back Up the Database

Out of the box, Audit Vault does not enable the `SYSDBA` privilege. Therefore, if you will be using `RMAN` to backup the database, you will need to follow the directions in Section 3.7.2 "Enabling or Disabling Connections with the SYSDBA Privilege" in the Audit Vault Server installation guide for the respective platform install documentation. After cleanly shutting down the instance following the analysis of the database, you should perform a full backup of the database. Complete the following steps:

1. Sign on to RMAN:

   ```
   rman "target / nocatalog"
   ```

2. Issue the following RMAN commands:

   ```
   RUN
   {
       ALLOCATE CHANNEL chan_name TYPE DISK;
       BACKUP DATABASE FORMAT 'some_backup_directory%U' TAG before_upgrade;
       BACKUP CURRENT CONTROLFILE TO 'save_controlfile_location';
   }
   ```

Caution: If you encounter problems with the upgrade and wish to abandon the upgrade completely, then you will need to restore the database from this backup. Therefore, make sure you back up your database now as a precaution.

See Also: *Oracle Database Backup and Recovery Basics* for more information about backing up a database.

Back Up Audit Vault Server Home

Because the patchset will update files in the Audit Vault Server Home, these files should all be backed up or copied to another directory until the patchset has been tested.

Back Up Audit Vault Collection Agent Home

Because the patchset will update files in the Audit Vault Collection Agent Home, these files should be backed up or copied to another directory until the patchset has been tested.

Abandon the Upgrade

If the patchset apply is not successful, to abandon the upgrade, perform the following steps:

1. Copy (Restore) the Audit Vault Server Home files back.

2. Copy (Restore) the Audit Vault Agent Home files back.
3. If you completed the steps in Back Up the Database to back up your database, then restore that backup. Complete the following steps:
   a. Log in to the system as the owner of the Oracle home directory of the previous release.
   b. Sign on to RMAN:

      ```
      rman "target / nocatalog"
      ```

   c. Issue the following RMAN commands:

      ```
      STARTUP NOMOUNT
      RUN
      {
          REPLICATE CONTROLFILE FROM 'save_controlfile_location';
          ALTER DATABASE MOUNT;
          RESTORE DATABASE FROM TAG before_upgrade
          ALTER DATABASE OPEN RESETLOGS;
      }
      ```

6

Troubleshooting an Audit Vault System

This chapter provides troubleshooting information for administering an Audit Vault system. This chapter includes the following sections:

- Location of Audit Vault Server Log and Error Files
- Location of Audit Vault Agent Log and Error Files
- Troubleshooting Tips

6.1 Location of Audit Vault Server Log and Error Files

Table 6–1 shows the names and a description of the Audit Vault Server log and error files located in the Audit Vault Server `$ORACLE_HOME/av/log` directory. These files contain important information regarding the return status of commands and operations that will be useful in diagnosing problems should they occur. Log files can be deleted at any time, except for the `avca.log` file, which can only be deleted when the Audit Vault Server is shut down.

Table 6–1 Name and Description of Audit Vault Server Log and Error Files

File Name	Description
`agent.err`	Contains a log of errors encountered in agent initialization. This file can be deleted at any time.
`agent.out`	Contains a log of all primary agent-related operations and activity. This file can be deleted at any time.
`avca.log`	Contains a log of all AVCA commands that have been run and the results of running each command. This file can only be deleted after Audit Vault Server is shut down.
`av_client-%g.log.n`	Contains a log of the agent operations and any errors returned from those operations. The `%g` is a generation number that starts from 0 (zero) and increases once the file size reaches the 10 MB limit. A concurrent existence of this file is indicated by a `.n` suffix appended to the file type name, such as `av_client-%g.log.n`, where *n* is an integer issued in sequence, for example, `av_client-0.log.1`. This file can be deleted at any time.
`avorcldb.log`	Contains a log of all AVORCLDB commands that have been run and the results of running each command. This file can be deleted at any time.

Oracle Enterprise Manager stores its logs in the directory *`Audit Vault_Server_Home`*`/`*`Host_Name_SID`*`/sysman/log`. The file `emdb.nohup` in this directory contains a log of activity for the Audit Vault Console, including graphical user interface (GUI) conversations, requests from the AVCTL utility and communication with the various Audit Vault agents. This information can be used to debug communication issues between the server and the agents.

6.2 Location of Audit Vault Agent Log and Error Files

Table 6–2 shows the names and a description of the Audit Vault Agent log and error files located in the Audit Vault Agent `$ORACLE_HOME/av/log` directory. These files contain important information regarding the return status of commands and operations that will be useful in diagnosing problems should they occur.

Table 6–2 Name and Description of Audit Vault Agent Log and Error Files

File Name	Description
`agent.err`	Contains a log of all errors encountered in agent initialization and operation. This file can be deleted at any time.
`agent.out`	Contains a log of all primary agent-related operations and activity. This file can be deleted at any time.
`avca.log`	Contains a log of all AVCA commands that have been run and the results of running each command. This file can be deleted at any time.
`avorcldb.log`	Contains a log of all AVORCLDB commands that have been run and the results of running each command. This file can be deleted at any time.
`DBAUD_Collector_<source-name_prefix><source-id>.log`	Contains a log of collection operations for the DBAUD_Collector collector. This file can only be deleted after Audit Vault Agent is shut down.
`orcldb_osaud_<source name>.log`	Contains a log of all collection operations for the OSAUD_Collector collector. This file can only be deleted after Audit Vault Agent is shut down.
`av_client-`*`%g`*`.log.`*`n`*	Contains a log of the agent operations and any errors returned from those operations. The *`%g`* is a generation number that starts from 0 (zero) and increases once the file size reaches the 10 MB limit. A concurrent existence of this file is indicated by a `.`*`n`* suffix appended to the file type name, such as `av_client-`*`%g`*`.log.`*`n`*, where *`n`* is an integer issued in sequence, for example, `av_client-0.log.1`. This file can be deleted at any time.
`sqlnet.log`	Contains a log of SQL*Net information.

The directory *`Audit_Vault_Agent_Home`*`/oc4j/j2ee/home/log` contains the logs generated by the agent OC4J. In this directory, the file `AVAgent-access.log` contains a log of requests the agent receives from the Audit Vault Server. This information can be used to debug communication issues between the server and the agent.

Failed configuration commands are located in the Audit Vault Agent `$ORACLE_HOME/cfgtoollogs` directory, which includes the file, `configToolFailedCommands`. This file contains just the name of the failed command. See the `avca.log` or `avorcldb.log` file for additional information, including any associated errors and error messages.

6.3 Troubleshooting Tips

This section describes a number of troubleshooting scenarios that you might encounter with some of the Audit Vault components and how try to resolve each one. The scenarios are placed in the following groupings:

- Audit Vault Server
- Audit Vault Agent
- Audit Vault Collector
- Audit Vault Console
- Audit Vault in an Oracle Real Application Clusters (Oracle RAC) Environment

6.3.1 Audit Vault Server

This section describes Audit Vault Server problems that you might encounter.

Problem: Best way to tune Audit Vault Server performance when using the REDO collector.

Following an Audit Vault Server installation, the `streams_pool_size` initialization parameter is set to 150 MB. This parameter must be tuned to maximize REDO collector performance if you are going to be using this collector. In an Oracle Real Application Clusters (Oracle RAC) environment, this parameter must be tuned on all nodes because it is uncertain where the queue will be particularly after an instance startup.

Solution:

Typically, once a REDO collector is configured and started, let it run for a while. This will allow the autotuning feature of Oracle Database to allocate memory for the best database performance for the `streams_pool_size` parameter. Using AWR, check to see if STREAMS AQ has a flow control issue – enqueue being blocked. In the event that you notice that the performance, for example, is only 500 records being applied per second, it may become necessary to manually tune this parameter.

Assuming that you have at least 1 GB of physical memory in your Audit Vault Server system, set this parameter to 200 MB using the SQL command `ALTER SYSTEM SET STREAMS_POOL_SIZE=200;`. Monitor the performance again using AWR. You should achieve a record apply rate of 2000 records per second, which is a typical maximum rate for the REDO collector. Usually, setting the value to 200 MB should be sufficient. If you using Oracle Audit Vault in an Oracle RAC environment, set this parameter value accordingly on all nodes in the cluster. Use the SQL command `ALTER SYSTEM SET STREAMS_POOL_SIZE=200 SID=av`*`n`*`;`, where *`n`* is the number portion of the SID for each node in the cluster, for example, `av2`, `av3`, `av4`, and so forth, if that is your naming convention.

6.3.2 Audit Vault Agent

This section describes Audit Vault Agent problems that you might encounter.

Problem: While issuing an AVORCLDB setup command in the agent shell, you misenter the srcusr password in setting up the source on the agent. How do you recover from this problem?

In the agent shell, one of the last setup steps involves setting up the source with the agent using the AVORCLDB setup command. When entering the `-srcusr` argument, if you enter an incorrect password and invoke the command, an error message is returned indicating that the password is not recognized. Suddenly, you realize the source of the error as being a mistyped password.

Efforts to reenter the command using the correct password for the source user indicates that the credential already exists, so it cannot be entered again. How do you work around this problem so that you can use the setup command and the correct source user password?

Solution:

The incorrect credential that was added populates the avwallet in the Audit Vault Agent home. One workaround is to rename the avwallet file and create a new avwallet file. Next, you must add the agentuser credential. Finally, invoke the AVORCLDB setup command using the correct source user password. These steps follow:

1. In the Audit Vault Agent home, change directory to the `avwallet` directory.

   ```
   cd ../../network/admin/avwallet
   ```

2. Rename the `avwallet` file.

   ```
   mv avwallet/ avwallet.1
   ```

3. Create the `avwallet` file. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVCA_WPWD` is set to *`wallet password`*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable. In this example, the environment variable is set and the `-wpwd` argument is omitted.

   ```
   avca create_wallet -wrl $ORACLE_HOME/network/admin/avwallet
   ```

4. Check to see that the `avwallet` file was created.

   ```
   ls -l avwallet
   ```

5. Check to see that no credentials exist that allow you to connect to the Audit Vault database.

   ```
   sqlplus /@av
   ```

   Note that the connection fails because the agent user credential does not exist.

6. Create the credential for the agent user. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVCA_WPWD` is set to *`wallet password`*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable. The `-usr` argument can be omitted if the corresponding environment variable, `AVCA_USR` is set to *`usr/password`*. If the command-line argument `-usr` is specified, then the command-line argument overrides the environment variable. In this example, the environment variable is set and the `-wpwd` argument is omitted.

   ```
   avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -wpwd <passwd>
                          -dbalias <dbalias>
   ```

7. Check to see that the agent user credential exists, allowing you to connect to the Audit Vault database.

   ```
   sqlplus /@av
   ```

   The connection succeeds.

8. Invoke the AVORCLDB `setup` command in the Audit Vault Agent shell. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVORCLDB_WPWD` is set to *`wallet password`*. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`source username/password`*. If the command-line arguments `-wpwd` and -usr are specified, then the command-line arguments override the environment

variable. In this example, these environment variables are set and the -srcusr and -wpwd arguments are omitted.

```
avorcldb setup -srcname DBS1.US.ORACLE.COM
```

9. Check the tnsnames.ora file in the Audit Vault Agent home to see that it contains a SRCDBA1 alias.

```
vi tnsnames.ora

SRCDB1   = (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=localhost)
(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=src1.DBS1.US.ORACLE.COM)))
```

10. Check to see that the source user alias for the source database can connect to the Audit Vault database.

```
sqlplus /@srcdba1
```

Note that the connection succeeds. The avwallet file is current and working.

6.3.3 Audit Vault Collector

This section describes Audit Vault collector problems that you might encounter.

Problem: Starting any collector fails, Returning Errors

After you add the source, add the collectors, then set up the source at the agent as part of the configuration steps described in Section 3.2, you are ready to start each collector. However, when you attempt to start any of the collectors through the Audit Vault Console, the operation fails with an HTTP error. When this same operation is attempted through the AVCTL start_collector command, it again fails, but with the following error message:

```
Starting collector...
Error executing task start_collector: Cannot find Agent for Collector
<source-name>:OSAUD
```

A quick search of the agent.err log file in the Audit Vault Agent home shows the following error:

```
SEVERE: java.sql.SQLException: ORA-28150: proxy not authorized to connect as
client
```

The cause stated for an ORA-28150 error is stated as follows: A proxy user attempted to connect as an agent, but the proxy was not authorized to act on behalf of the agent.

Solution:

The solution stated for an ORA-28150 error is as follows: Grant the proxy user permission to perform actions on behalf of the agent by using the SQL ALTER USER...GRANT CONNECT command.

One of the configuration steps is to create the Audit Vault source user. Next, you grant proxy connect privilege to the Audit Vault source user through the Agent user. Overlooking this step results in these error messages. This means that the Audit Vault source user has not been granted proxy connect privilege to the Audit Vault source user <avsrcusr> through the agent user <agentusr> to connect to the source database.

See Section 3.2, the second part of Step 2b, about granting proxy connect privilege to the Audit Vault source user <avsrcusr> through the agent user <agentusr>.

Performing this step solves the problem. See Example 3–3 for the detailed syntax to perform this step. After the Audit Vault source user is granted this proxy connect privilege, attempts to start any of the collectors should be successful.

Problem: Not sure if the DBAUD_Collector or OSAUD_Collector collectors are collecting from the AUD$ table and the OS file, respectively

After you set up both the DBAUD_Collector and OSAUD_Collector collectors, you want to check to see that they are collecting from the AUD$ table and OS file, respectively.

Solution:

To see if DBAUD_Collector is collecting from the AUD$ table, check the contents of the `DBAUD_Collector_<source-name_prefix><source-id>.log` file in the Audit Vault Agent home `/av/log` directory.

To see if OSAUD_Collector is collecting from the OS File, check the contents of the `orcldb_osaud_<source name>.log` file in the Audit Vault Agent home `/av/log` directory.

Bring each file into an editor and search for entries that indicate that the collector is collecting audit records.

For example, entries like these would be found in the DBAUD_Collector log file:

```
     ***** Started logging for 'AUD$ Audit Collector' *****
.
.
.
INFO @ '25/01/2007 19:08:42 -8:00':
     ***** SRC connected OK

INFO @ '25/01/2007 19:08:53 -8:00':
     ***** SRC data retireved OK
.
.
.
```

For example, an entry like this would be found in the OSAUD_Collector log file:

```
File opened for logging source "DBS1.REGRESS.RDBMS.DEV.US.ORACLE.COM"
INFO @ '24/01/2007 18:16:18 -8:00':
***** Started logging for 'OS Audit Collector' *****
```

If everything looks OK, close the editor, then refresh the warehouse using the AVCTL refresh_warehouse command in the Audit Vault Server shell. When this operation completes, log in to the Audit Vault Console as the Audit Vault auditor and examine the graphical summary named **Activity by Audit Event Category** on the **Overview** page for the appearance of additional audit records in the various event categories. Increased counts for the various event categories indicate that these collectors are collecting audit records.

Problem: ORA-01017:invalid username/password; logon denied error when starting up the DBAUD_Collector or setting up the REDO_Collector

When you try to start up the DBAUD_Collector or set up the REDO_Collector, you get an ORA-01017: invalid username/password; logon denied error.

Solution:

This error is likely due to a problem with your user name or your password or both in the password file. Try re-creating the user name and password. If the problem persists, re-create the password file.

6.3.4 Audit Vault Console

This section describes Audit Vault Console problems that you might encounter.

Problem: Audit Vault Console does not come up in the Web browser

When you try to bring up the Audit Vault Console in a Web browser, it appears to hang, or after a while it times out.

Solution:

This may be happening because Audit Vault Console is down. To check the status of Audit Vault Console, issue an AVCTL show_av_status command in the Audit Vault Server shell. If the status indicates that the Audit Vault Console is down, issue an AVCTL start_av command in the Audit Vault Server shell to get it started again. Then start up the Audit Vault Console in the Web browser. The Audit Vault Console should appear and let you log in to the Audit Vault auditor's or administrator's management system.

6.3.5 Audit Vault in an Oracle Real Application Clusters (Oracle RAC) Environment

This section describes some problems that you might encounter when you run Audit Vault in an Oracle Real Application Clusters (Oracle RAC) environment.

Problem: In an Oracle RAC environment, the AVCA drop_agent operation fails with an error when this command is issued from one of the Oracle RAC nodes

When you try to issue an AVCA `add_agent` command from one of the Oracle RAC nodes, the command fails.

Solution:

In an Oracle RAC environment, AVCA commands must be issued from the node on which Oracle Enterprise Manager resides. This is the same node on which the `av.ear` file is deployed.

In an Oracle RAC environment, AVCA and AVCTL commands can be issued only from the node where the `av.ear` file is deployed.

To see where the `av.ear` file is deployed, check to see where the following file is located: `$ORACLE_HOME/oc4j/j2ee/oc4j_applications/applications/av/av/WEB-INF/classes/av.properties`

Once you locate the node, run all AVCA and AVCTL commands from that node.

If the node on which the `av.ear` file is deployed is down, deploy the `av.ear` file to another node using the AVCA `deploy_av` command. The command syntax is as follows:

```
deploy_av -avadm <usr>/<pwd> -jdbc_str <jdbc connect string>
          -sid <sid> -dbalias <db alias>
          -avconsoleport <av console port>
```

In this example:

- `-avadm <usr>/<pwd>` is the user name and password of the Audit Vault administrator (user granted AV_ADMIN role). Use a slash (/) to separate the user name and password. The `-avadm` argument can be omitted if the corresponding environment variable, `AVCA_AVADM` is set to *`usr/pwd`*. If the command-line argument `-usr` is specified, then the command-line argument overrides the environment variable.
- `-jdbc_str <jdbc connect string>` is the JDBC connect string to connect to Audit Vault, which uses the format `jdbc:oracle:<driver type>:@//<host>:<port>/<service name>`.
- `-sid <sid>` is the Oracle system identifier (SID) for the instance.
- `-dbalias <db alias>` is the database alias.
- `-avconsoleport <av console port>` is the port number for the Audit Vault Console.

A

Audit Vault Configuration Assistant (AVCA) Reference

Audit Vault Configuration Assistant (AVCA) is a command-line utility that provides the Audit Vault administrator with the ability to manage various Audit Vault components.

The user running the AVCA commands must be granted the `AV_ADMIN` role.

Table A–1 describes the Audit Vault Configuration Assistant commands and where each is used, whether on the Audit Vault Server, on the Audit Vault Agent, or in both places.

Table A–1 Audit Vault Configuration Assistant Commands

Command	Used Where?	Description
add_agent	Server	Adds an agent to Oracle Audit Vault
create_credential	Both	Creates a credential to be stored in the wallet
create_wallet	Both	Creates a wallet to hold credentials
deploy_av	Server	Deploys the `av.ear` file to another node in an Oracle RAC environment
drop_agent	Server	Drops an agent from Oracle Audit Vault
help	Both	Displays Help for the AVCA commands
redeploy	Both	Redeploys the `av.ear` file on the Audit Vault Server system or the `AVAgent.ear` file on the Audit Vault Agent system
secure_agent	Agent	Secures the Audit Vault Agent by enabling mutual authentication with Audit Vault
secure_av	Server	Secures Audit Vault Server by enabling mutual authentication with the Audit Vault Agent
set_warehouse_retention	Server	Controls the amount of data kept online in the data warehouse fact table
set_warehouse_schedule	Server	Sets the schedule for refreshing data from the raw audit data store to the star schema
upgrade	Both	Upgrades the current Audit Vault Server and Audit Vault Agent installation to the next revision

Note: In an Oracle RAC environment, AVCA commands must be issued from the node on which Oracle Enterprise Manager resides. This is the same node on which the `av.ear` file is deployed.

If the node on which the `av.ear` file is deployed is down, deploy the `av.ear` file to another node using the AVCA deploy_av command.

add_agent

Adds or registers an agent to Audit Vault. This command is run on the Audit Vault Server.

Syntax

```
avca add_agent -agentname <agent name>
[-agentdesc <desc>] -agenthost <host> -agentusr <usr>
```

Arguments

Argument	Description
`-agentname <agent name>`	Specify the agent (by agent name) to be modified.
`[-agentdesc <desc>]`	Optionally, specify a description of the agent.
`-agenthost <host>`	Specify a new host value for this agent.
`-agentusr <usr>`	Specify the existing user name to represent the agent and for whom the `AV_AGENT` role has been granted.

Usage Notes

To install an Audit Vault Agent, perform the following steps:

1. Using the Database Vault Owner role, create an agent user at the Audit Vault Server.
2. Add the agent to Audit Vault using the AVCA `add_agent` command (as the Audit Vault administrator user with the `AV_ADMIN` role granted. This registers the Audit Vault Agent at the Audit Vault Server.
3. Install the Audit Vault Agent at the corresponding host system where the agent is to be installed.

Example

The following example shows how to add an agent to Audit Vault:

```
avca add_agent -agentname TTAgent2 -agenthost stapj40 -agentusr avagentt
AVCA started
Adding agent...
Agent added successfully.
```

create_credential

Creates a credential to be stored in the wallet. This command is run on both the Audit Vault Server and Audit Vault Agent.

Syntax

```
avca create_credential -wrl <wallet_location> -wpwd <wallet_pwd>
-dbalias <db_alias> -usr <usr>/<pwd>
```

Arguments

Argument	Description
`-wrl <wallet_location>`	The wallet location
`-wpwd <wallet_pwd>`	The wallet password (the password needed to open the wallet). This is the password of the agent user granted the `AV_AGENT` role. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVCA_WPWD` is set to *`wallet_pwd`*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable.
`-dbalias <db_alias>`	The database alias
`-usr <usr>/<pwd>`	The target user name and password to be secured and stored in the wallet. Use a slash (/) to separate the user name and password. The `-usr` argument can be omitted if the corresponding environment variable, `AVCA_USR` is set to *`usr/pwd`*. If the command-line argument `-usr` is specified, then the command-line argument overrides the environment variable.

Usage Notes

Use this command to create a new certificate if someone changes the source user password on the source, thus eventually breaking the connection between the collector and the source.

You must modify the `sqlnet.ora` file as follows after executing this command:

- Add one line "`sqlnet.wallet_override=true`" in the `sqlnet.ora` file.
- Modify the wallet location correspondingly.
- Set the environment variable (`setenv $TNS_ADMIN`) if needed.

Example

The following example shows how to create a credential to be stored in a wallet located at $T_WORK/tt_1. In this example, the `AVCA_WPWD` environment variable is set to `welcome1`, the wallet password; the `AVCA_USR` environment variable is set to `scott/tiger`, and both the `-wpwd` and `-usr` arguments are omitted.

```
avca create_credential -wrl $T_WORK/tt_1 -dbalias inst1
AVCA started
Storing user credentials in wallet...
Create credential oracle.security.client.connect_string1
done.
```

create_wallet

Creates a wallet to hold credentials. This command is run on both the Audit Vault Server and Audit Vault Agent.

Syntax

```
avca create_wallet -wrl <wallet_location> -wpwd <wallet_pwd>
```

Arguments

Argument	Description
-wrl <wallet_location>	The wallet location
-wpwd <wallet_pwd>	The wallet password (the password needed to open the wallet). This is the password of the agent user granted AV_AGENT role. The -wpwd argument can be omitted if the corresponding environment variable, AVCA_WPWD is set to *wallet_pwd*. If the command-line argument -wpwd is specified, then the command-line argument overrides the environment variable.

Usage Notes

After you execute this command, .sso and .p12 files are generated in the wallet location.

Example

The following example shows how to create a wallet in the location specified as $T_WORK/tt_1. In this example, the AVCA_WPWD environment variable is set to welcome1, the wallet password, and the -wpwd argument is omitted.

```
avca create_wallet -wrl $T_WORK/tt_1
AVCA started
Creating wallet...
Wallet created successfully.
```

deploy_av

Deploys the av.ear file to another node in an Oracle Real Application Clusters (Oracle RAC) environment. This command is run on the Audit Vault Server.

Syntax

```
deploy_av -avadm <usr>/<pwd> -jdbc_str <jdbc connect string>
          -sid <sid> -dbalias <db_alias>
          -avconsoleport <av_console_port>
```

Arguments

Argument	Description
-avadm <usr>/<pwd>	The user name and password of the Audit Vault administrator (user granted AV_ADMIN role). Use a slash (/) to separate the user name and password. The -avadm argument can be omitted if the corresponding environment variable, AVCA_AVADM is set to *usr/pwd*. If the command-line argument -usr is specified, then the command-line argument overrides the environment variable.
-jdbc_str <jdbc connect string>	The JDBC connect string to connect to Audit Vault, which uses the format jdbc:oracle:<driver type>:@//<host>:<port>/<service name>
-sid <sid>	The Oracle system identifier (SID) for the instance
-dbalias <db_alias>	The database alias
-avconsoleport <av_console_port>	The port number for the Audit Vault Console

Options

None

Usage Notes

In an Oracle RAC environment, AVCA commands must be issued from the node on which Oracle Enterprise Manager resides. This is the same node on which the av.ear file is deployed.

If the node on which the av.ear file is deployed is down, deploy the av.ear file to another node using the AVCA deploy_av command.

Example

The following example shows how to deploy the av.ear file to another node in an Oracle RAC environment. In this example, the AVCA_AVADM environment variable is set to *usr/pwd* and the -avadm argument is omitted.

```
avca deploy_av -jdbc_str jdbc:oracle:<driver type>:@//system14:<port>/<service
name> -sid av -dbalias av -avconsoleport 5700
```

drop_agent

Drops an agent from Audit Vault. This command is run on the Audit Vault Server.

Syntax

```
avca drop_agent -agentname <agent name>
```

Arguments

Argument	Description
`-agentname <agent name>`	Specify the agent (by agent name) to be dropped from Audit Vault.

Usage Notes

- The `drop_agent` command does not delete the agent from Audit Vault; it disables the agent. The user can neither add the same agent name again nor enable the dropped agent.
- An error will be raised if active collectors are still running in the agent.

Example

The following example shows how to drop an agent named 'OC4JAgent1' from Audit Vault:

```
avca drop_agent -agentname OC4JAgent1
AVCA started
Dropping agent...
Agent dropped successfully.
```

help

Displays Help for the AVCA commands. This command is run on both the Audit Vault Server and Audit Vault Agent.

Syntax

```
avca -help

avca <command> -help
```

Arguments

Argument	Description
`<command>`	The name of an AVCA command for which you want Help to appear

Options

None

Usage Notes

None

Example

The following example shows how to display general AVCA utility Help in the Audit Vault Server home.

```
avca -help
  -------------------------------------------
  AVCA Usage
  -------------------------------------------
  Oracle Audit Vault Server Installation commands
      avca secure_av -avkeystore <keystore location> -avkeystorepwd <keystore pwd> -avtruststore
<truststore location>
      avca secure_av -remove
      avca upgrade -avsysdba <usr>/<pwd> -dvowner <usr>/<pwd>

  Oracle Audit Vault Configuration commands - Agent:
      avca add_agent -agentname <agent name> [-agentdesc <desc>] -agenthost <host> -agentusr <usr>
      avca drop_agent -agentname <agent name>

  Oracle Audit Vault Configuration commands - Warehouse:
      avca set_warehouse_schedule -schedulename <schedule name>
      avca set_warehouse_schedule -startdate <start date> -rptintrv <repeat interval> [-dateformat
<date format>]
      avca set_warehouse_retention -intrv <year-month interval>

  Oracle Audit Vault Configuration commands - Authentication:
      avca create_wallet -wrl <wallet_location> -wpwd <wallet_pwd>
      avca create_credential -wrl <wallet_location> -wpwd <wallet_pwd> -dbalias<db alias> -usr
<usr>/<pwd>

  avca -help
```

The following example shows how to display specific AVCA Help for the `add_agent` command in Audit Vault.

```
avca add_agent -help

  avca add_agent -agentname <agent name> [-agentdesc <desc>] -agenthost <host>
-agentusr <usr>
  ------------------------------------------------
  -agentname <agent name>
  [-agentdesc <agent description>]
  -agenthost <agent host>
  -agentusr <the user which represents agent>
  ------------------------------------------------
```

The following example shows how to display general AVCA utility Help in the Audit Vault Agent home.

```
avca -help
  --------------------------------------------
  AVCA Usage
  --------------------------------------------
  Oracle Audit Vault Agent Installation commands
      avca secure_agent -agentkeystore <keystore location> -agentkeystorepwd
<keystore pwd> -avdn <DN of Audit Vault> -agentdn <DN of agent>
      avca secure_agent -remove
      avca upgrade

  Oracle Audit Vault Configuration commands - Authentication:
      avca create_wallet -wrl <wallet_location> -wpwd <wallet_pwd>
      avca create_credential -wrl <wallet_location> -wpwd <wallet_pwd> -dbalias<db
alias> -usr <usr>/<pwd>

  avca -help
```

redeploy

Redeploys the `av.ear file` on the Audit Vault Server system or the `AVAgent.ear` file on the Audit Vault Agent system.

Syntax

```
avca redeploy
```

Arguments

None

Options

None

Usage Notes

None

Example

The following example shows how to redeploy either the `av.ear` file on the Audit Vault Server system or the `AVAgent.ear` file on the Audit Vault Agent system.

```
avca redeploy
```

secure_agent

Secures the Audit Vault Agent by enabling mutual authentication with the Audit Vault Server. This command is run on the Audit Vault Agent. This command also removes mutual authentication with Audit Vault Server.

Syntax

```
avca secure_agent -agentkeystore <keystore location>
-agentkeystorepwd <keystore pwd> -avdn <DN of Audit Vault Server>
-agentdn <DN of agent>

avca secure_agent -remove
```

Arguments

Argument	Description
`-agentkeystore <keystore location>`	Specify the key store location for this agent.
`-agentkeystorepwd <keystore pwd>`	Specify the key store password for this agent.The `-agentkeystorepwd` argument can be omitted if the corresponding environment variable, `AVCA_AGENTKEYSTOREPWD` is set to *`keystore password`*. If the command-line argument `-agentkeystorepwd` is specified, then the command-line argument overrides the environment variable.
`-avdn <DN of Audit Vault Server>`	Distinguished name (DN) of the Audit Vault Server
`-agentdn <DN of agent>`	DN of this Audit Vault Agent
`-remove`	Keyword to indicate removing mutual authentication with Audit Vault Server

Usage Notes

- The key store and certificate must be in place at the agent side before you execute this command.
- Use the following command to generate a key store:

  ```
  $ORACLE_HOME/jdk/bin/keytool
  ```

- When you issue the `secure_agent` command for the specified agent with both the agent and its collectors in a running state, the agent and all its collectors will shut down when the agent OC4J shuts down and starts up again. The specified agent and its collectors must all be manually started again.

Example

The following example shows how to secure the Audit Vault Agent by enabling mutual authentication with the Audit Vault Server. In this example, the `AVCA_AGENTKEYSTOREPWD` environment variable is set to `welcome1` and the `-agentkeystorepwd` argument is omitted.

```
avca secure_agent -agentkeystore /tmp/agentkeystore
```

```
-agentdn "CN=agent1, OU=development, O=oracle,
L=redwoodshores, ST=ca, C=us" -avdn "CN=av1, OU=development, O=oracle,
L=redwoodshores, ST=ca, C=us"
```

The following example shows how to unsecure the Audit Vault Agent by disabling mutual authentication with the Audit Vault Server.

```
avca secure_agent -remove
AVCA started
Restarting agent OC4J...
OC4J restarted successfully.
```

secure_av

Secures Audit Vault Server by enabling mutual authentication with the Audit Vault Agent. This command is run on the Audit Vault Server. This command also removes mutual authentication with Audit Vault Agent.

Syntax

```
avca secure_av -avkeystore <keystore location> -avkeystorepwd <keystore pwd>
-avtruststore <truststore location>

avca secure_av -remove
```

Arguments

Argument	Description
`-avkeystore <keystore location>`	Specify the key store location for Audit Vault Server.
`-avkeystorepwd <keystore pwd>`	Specify the key store password for Audit Vault Server. The `-avkeystorepwd` argument can be omitted if the corresponding environment variable, `AVCA_AVKEYSTOREPWD` is set to *`keystore password`*. If the command-line argument `-avkeystorepwd` is specified, then the command-line argument overrides the environment variable.
`-avtruststore <truststore location>`	Specify the trust store location for Audit Vault Server.
`-remove`	Keyword to indicate removing mutual authentication with the Audit Vault Agent.

Usage Notes

- The key store and certificate must be in place at Audit Vault Server before you execute this command.
- Use the following command to generate a key store:

  ```
  $ORACLE_HOME/jdk/bin/keytool
  ```

- When you issue the `secure_av` command, the Audit Vault Console OC4J will shut down and start up again, requiring you to log in to Audit Vault Console again.

Example

The following example shows how to secure Audit Vault Server by enabling mutual authentication with the Audit Vault Agent. In this example, the `AVCA_AVKEYSTOREPWD` environment variable is set to `welcome1` and the `-avkeystorepwd` argument is omitted.

```
avca secure_av -avkeystore /tmp/avkeystore
-avtruststore /tmp/avkeystore
```

The following example shows how to unsecure Audit Vault Server by disabling mutual authentication with the Audit Vault Agent.

```
avca secure_av -remove
AVCA started
Stopping OC4J...
OC4J stopped successfully.
Starting OC4J...
OC4J started successfully.
Oracle Audit Vault 10g Database Control Release 10.2.2.0.0  Copyright (c)
1996,2005 Oracle Corporation.  All rights reserved.
http://stacd05.us.oracle.com:5700/av
Oracle Audit Vault 10g is running.
------------------------------------

Logs are generated in directory /scratch/10.2.2/av_1/av/log
```

set_warehouse_retention

Controls the amount of data kept online in the data warehouse fact table. This command is run on the Audit Vault Server.

Syntax

```
avca set_warehouse_retention -intrv <year-month interval>
```

Arguments

Argument	Description
`-intrv <year-month interval>`	Specify the year month interval in the form [+]YY-MM.

Usage Notes

- The interval set defines the lifetime of the partitions in the fact table.
- Partitions that are older than the lifetime are removed during the next refresh of the fact table.
- The interval must be positive.
- Only data loaded using the AVCTL load_warehouse command can be purged using the AVCTL purge_warehouse command. The data loaded using the AVCTL refresh_warehouse command is removed automatically based on the warehouse retention specified using the AVCA `set_warehouse_retention` command.

Example

The following example shows how to control the amount of data kept online in the data warehouse table. In this case, a time interval of one year is specified.

```
avca set_warehouse_retention -intrv +01-00
AVCA started
Setting warehouse retention period...
done.
```

set_warehouse_schedule

Sets the schedule for refreshing data from the raw audit data store to the star schema. This command is run on the Audit Vault Server.

Syntax

```
avca set_warehouse_schedule -schedulename <schedule name>

avca set_warehouse_schedule -startdate <start date>
     -rptintrv <repeat interval> [-dateformat <date format>]
```

Arguments

Argument	Description
-schedulename <schedule name>	Specify the schedule name created using the DBMS_SCHEDULER.create_schedule procedure.
-startdate <start date>	Specify the start date for a warehouse refresh job using the default format DD-MON-YY. To use a different format, specify the -dateformat argument.
-rptintrv <repeat interval>	Specify the repeat interval for the schedule using the syntax used in the DBMS_SCHEDULER.create_schedule procedure.
[-dateformat <date format>]	Optionally, specify the date format for the -startdate argument.

Usage Notes

- The schedule can be set using a named schedule created using the DBMS_SCHEDULER.create_schedule procedure, or the schedule can be set by providing the start date and repeat interval.
- The following are error conditions:
  - The schedule name argument must be a valid schedule created using the DBMS_SCHEDULER.create_schedule procedure.
  - The repeat interval argument must be a valid interval specification consistent with the DBMS_SCHEDULER package.

Example

The following examples show how to set the schedule for refreshing data from the raw audit data store to the star schema by schedule name and by start date using the AVCA set_warehouse_schedule command.

The following example uses a schedule name argument based on a valid schedule created using the DBMS_SCHEDULER.create_schedule procedure.

```
avca set_warehouse_schedule -schedulename daily_refresh
AVCA started
Set warehouse schedule...
done.
```

The following example uses a start date and repeat interval argument.

```
avca set_warehouse_schedule -startdate 01-JUL-06 -rptintrv 'FREQ=DAILY;BYHOUR=0'
AVCA started
Set warehouse schedule...
done.
```

The following example uses a start date with a specified date format and a repeat interval argument.

```
avca set_warehouse_schedule -startdate 01-07-2006 -dateformat 'DD-MM-YYYY'
-rptintrv 'FREQ=DAILY;BYHOUR=0'
AVCA started
Set warehouse schedule...
done.
```

upgrade

Upgrades an Audit Vault Server or an Audit Vault Agent to the current release from the previous release. This command is run on both the Audit Vault Server and on the Audit Vault Agent.

Syntax

For upgrading the Audit Vault Server:

```
avca upgrade -avsysdba <usr>/<pwd> -dvowner <ysr>/<pwd>
```

For upgrading the Audit Vault Agent.

```
avca upgrade
```

Arguments

Argument	Description
`-avsysdba <usr>/<pwd>`	Specify the Audit Vault sysdba user name and password.
`-dvowner <sys>/<pwd>`	Specify the Oracle Database Vault Owner user name and password.

Usage Notes

None

Example

The following example shows how to upgrade an Audit Vault Agent:

```
avca upgrade
```

B

Audit Vault Control (AVCTL) Reference

Audit Vault Control (AVCTL) is a command-line utility that provides the Audit Vault administrator with the ability to control various Audit Vault components.

Table B–1 describes the Audit Vault Control commands and where each is used, whether on the Audit Vault Server, on the Audit Vault Agent, or in both places.

Table B–1 Audit Vault Control Commands

Command	Where Used	Description
-help	Both	Displays Help for the AVCTL commands
load_warehouse	Server	Loads older data from the raw audit data store into the data warehouse tables for analysis
purge_warehouse	Server	Purges older data from the data warehouse tables
refresh_warehouse	Server	Refreshes the data warehouse dimensions and fact table with the data in the raw audit data store since the last refresh operation.
show_agent_status	Server	Shows the status (metric) of an agent
show_av_status	Server	Shows the status (metric) of the Audit Vault Console
show_collector_status	Server	Shows the status (metric) of a collector
show_oc4j_status	Agent	Shows the status (metric) of the agent OC4J
start_agent	Server	Starts the agent
start_av	Server	Starts the Audit Vault Console
start_collector	Server	Starts the collector
start_oc4j	Agent	Starts the agent OC4J
stop_agent	Server	Stops the agent
stop_av	Server	Stops the Audit Vault Console
stop_collector	Server	Stops the collector
stop_oc4j	Agent	Stops the agent OC4J

Note: In an Oracle RAC environment, AVCTL commands must be issued from the node on which Oracle Enterprise Manager resides. This is the same node on which the `av.ear` file is deployed.

If the node on which the `av.ear` file is deployed is down, deploy the `av.ear` file to another node using the AVCA deploy_av command.

-help

Displays Help for the AVCTL commands. This command is run on both the Audit Vault Server and the Audit Vault Agent.

Syntax

```
avctl -help

avctl <command> -help
```

Arguments

Argument	Description
<command>	The name of an AVCTL command for which you want Help to appear

Usage Notes

None

Example

The following example shows how to display general AVCTL utility Help in the Audit Vault Server home.

```
avctl -help
  -------------------------------------------
  AVCTL Usage
  -------------------------------------------
  Oracle Audit Vault Control commands - AV Server:
      avctl start_av [-loglevel error|warning|info|debug]
      avctl stop_av
      avctl show_av_status

  Oracle Audit Vault Control commands - Agent:
      avctl start_agent -agentname <agent name>
      avctl stop_agent -agentname <agent name>
      avctl show_agent_status -agentname <agent name>

  Oracle Audit Vault Control commands - Collector:
      avctl start_collector -collname <collector name> -srcname <source name>
      avctl stop_collector -collname <collector name> -srcname <source name>
      avctl show_collector_status -collname <collector name> -srcname <source 
name>

  Oracle Audit Vault Control commands - Warehouse:
      avctl refresh_warehouse [-wait]
      avctl load_warehouse -startdate <start date> -numofdays <num of days> 
[-dateformat <date format>] [-wait]
      avctl purge_warehouse -startdate <start date> -numofdays <num of days> 
[-dateformat <date format>] [-wait]

  avctl -help
```

The following example shows how to display specific AVCTL Help for the start_agent command in Audit Vault.

```
avctl start_agent -help
  avctl start_agent -agentname <agent name>
  ------------------------------------------------
  -agentname <agent name>
  ------------------------------------------------
```

The following example shows how to display general AVCTL utility Help in the Audit Vault Agent home.

```
  --------------------------------------------
  AVCTL Usage
  --------------------------------------------
  Oracle Audit Vault Control commands - Agent OC4J:
      avctl start_oc4j [-loglevel error|warning|info|debug]
      avctl stop_oc4j
      avctl show_oc4j_status

  avctl -help
```

load_warehouse

Loads older data from the raw audit data store into the data warehouse tables for analysis. This command is run on the Audit Vault Server.

Syntax

```
avctl load_warehouse -startdate <start date> -numofdays <num of days>
                    [-dateformat <date format>] [-wait]
```

Arguments

Argument	Description
`-startdate` <startdate>	Specify the start date for the events to be loaded into the data warehouse tables using the default format DD-MON-YY. To use a different format, specify the `-dateformat` argument.
`-numofdays` <num of days>	Specify the number of days' worth of data to be loaded.
`[-dateformat <date format>]`	Optionally, specify the date format for the `-startdate` argument.
`[-wait]`	Optionally, specify that the command wait for the load job to complete. If this argument is not specified, a DBMS job is started, and the command returns immediately.

Usage Notes

The audit records received from the value of the `-startdate` argument for the given number of days specified by the `-numofdays` argument will be loaded into the data warehouse.

Example

The following example shows how to load the data warehouse with 10 days' worth of audit data beginning with January 1, 2004:

```
avctl load_warehouse -startdate 01-JAN-04 -numofdays 10
AVCTL started
Loading older audit records into warehouse...
done.
```

The following example shows how to load the data warehouse with 10 days' worth of audit data beginning with January 1, 2004 and to specify that the operation wait until the previous load job completes.

```
avctl load_warehouse -startdate 01-JAN-04 -numofdays 10 -wait
AVCTL started
Loading older audit records into warehouse...
Waiting for load to complete...
done.
```

The following example shows how to load the data warehouse with 10 days' worth of audit data beginning with January 1, 2004 using the DD/MM/YYYY date format.

```
avctl load_warehouse -startdate 01/01/2004 -numofdays 10 -dateformat DD/MM/YYYY
AVCTL started
Loading older audit records into warehouse...
done.
```

purge_warehouse

Purges older data from the data warehouse tables. This command is run on the Audit Vault Server.

Syntax

```
avctl purge_warehouse -startdate <start date> -numofdays <num of days>
                    [-dateformat <date format>] [-wait]
```

Arguments

Argument	Description
`-startdate`	Specify the start date for the events to be removed from the data warehouse tables using the default format DD-MON-YY. To use a different format, specify the `-dateformat` argument.
`-numofdays`	Specify the number of days' worth of data to be removed.
`[-dateformat]`	Optionally, specify the date format for the `-startdate` argument.
`[-wait]`	Optionally, specify that the command wait for the purge job to complete. If this argument is not specified, a DBMS job is started, and the command returns immediately.

Usage Notes

- The audit records received from the `-startdate` argument for the given number of days specified by the `-numofdays` argument will be removed from the data warehouse tables.
- Only data loaded using the AVCTL load_warehouse command can be purged using the `purge_warehouse` command. The data loaded using the AVCTL refresh_warehouse command is removed automatically based on the warehouse duration specified using the AVCA set_warehouse_retention command.

Example

The following example shows how to purge 10 days' worth of data from the data warehouse beginning with January 1, 2004:

```
avctl purge_warehouse -startdate 01-JAN-04 -numofdays 10
AVCTL started
Purging older audit records from warehouse...
done.
```

The following example shows how to purge 10 days' worth of data from the data warehouse beginning with January 1, 2004 and to specify that the operation wait until the previous purge job completes:

```
avctl purge_warehouse -startdate 01-JAN-04 -numofdays 10 -wait
AVCTL started
Purging older audit records from warehouse...
Waiting for purge to complete...
done.
```

The following example shows how to purge 10 days' worth of data from the data warehouse beginning with January 1, 2004 using the date format of DD/MM/YYYY.

```
avctl purge_warehouse -startdate 01/01/2004 -numofdays 10 -dateformat DD/MM/YYYY
AVCTL started
Purging older audit records from warehouse...
done.
```

refresh_warehouse

Refreshes the data warehouse dimensions and fact table with the data from the raw audit data store since the last refresh operation. This command is run on the Audit Vault Server.

Syntax

```
avctl refresh_warehouse [-wait]
```

Arguments

Argument	Description
`[-wait]`	Optionally, specify that the command wait for the refresh job to complete. If this argument is not specified, a DBMS job is started, and the command returns immediately.

Usage Notes

The last refresh operation could have been an explicit refresh using this command or a scheduled refresh based on the schedule set using the AVCA set_warehouse_schedule command.

Example

The following example shows how to refresh the data warehouse:

```
avctl refresh_warehouse
AVCTL started
Refreshing warehouse...
done.
```

The following example shows how to specify that the refresh operation wait until the previous refresh job completes before refreshing the data warehouse:

```
avctl refresh_warehouse -wait
AVCTL started
Refreshing warehouse...
Waiting for refresh to complete...
done.
```

show_agent_status

Shows the status (metric) of an agent. This command is run on the Audit Vault Server.

Syntax

```
avctl show_agent_status -agentname <agent name>
```

Arguments

Argument	Description
`-agentname`	Specify the agent (by agent name).

Usage Notes

None

Example

The following example shows the agent status for the OC4JAGENT1 agent:

```
avctl show_agent_status -agentname OC4JAGENT1
AVCTL started
Getting agent metrics...
--------------------------------
Agent is running
--------------------------------
Metrics retrieved successfully.
```

show_av_status

Shows the Audit Vault Console status or the metric of the Audit Vault Server. This command is run on the Audit Vault Server.

Syntax

```
avctl show_av_status
```

Arguments

None

Usage Notes

When the Audit Vault Console becomes inaccessible, issue this command to determine its status.

Example

The following example shows the Audit Vault Console status:

```
avctl show_av_status
AVCTL started
Oracle Audit Vault 10g Database Control Release 10.2.2.0.0  Copyright (c) 1996,
 2005 Oracle Corporation.  All rights reserved.
http://atacw05.us.oracle.com:5521/av
Oracle Audit Vault 10g is running.
------------------------------------
Logs are generated in directory /oracle/product/10.2.2/av_1/av/log
```

show_collector_status

Shows the status (metric) of a collector. This command is run on the Audit Vault Server.

Syntax

```
avctl show_collector_status -collname <collector name> -srcname <source name>
```

Arguments

Argument	Description
-collname	Specify the target collector (by collector name).
-srcname	Specify the source (by source name) to which this collector belongs.

Usage Notes

None

Example

The following example shows the collector status for the DBAUD_Collector collector:

```
avctl show_collector_status -collname DBAUD_Collector
                              -srcname RODSRC1.US.ORACLE.COM
AVCTL started
Getting collector metrics...
--------------------------------
Collector is running.
--------------------------------
```

show_oc4j_status

Shows the agent OC4J status (metric). This command is run on the Audit Vault Agent.

Syntax

```
avctl show_oc4j_status
```

Arguments

None

Usage Notes

None

Example

The following example shows the agent OC4J status for when it is running and when it is not running:

```
avctl show_oc4j_status
AVCTL started
------------------------------------
OC4J is running
------------------------------------

avctl stop_oc4j
AVCTL started
Stopping OC4J...
OC4J stopped successfully.

avctl show_oc4j_status
AVCTL started
------------------------------------
OC4J is not running
------------------------------------
```

start_agent

Starts the agent. This command is run on the Audit Vault Server.

Syntax

```
avctl start_agent -agentname <agent name>
```

Arguments

Argument	Description
`-agentname`	Specify the agent (by agent name) to be started.

Usage Notes

- On successful completion of this command, the agent is moved to a RUNNING state. If an error is encountered, the agent is moved to an ERROR state.
- Audit Vault accepts audit records only from agents in the RUNNING state.

Example

The following example shows how to start the agent in Oracle Audit Vault:

```
avctl start_agent -agentname OC4JAGENT1
AVCTL started
Starting Agent...
Agent started successfully.
```

start_av

Starts the Audit Vault Console. This command is run on the Audit Vault Server.

Syntax

```
avctl start_av [-loglevel error|warning|info|debug]
```

Arguments

Argument	Description
`[-loglevel error|warning|info|debug]`	Optionally, specify the desired level of logging.

Usage Notes

This command executes an `emctl start dbconsole` command.

Example

The following example shows how to start the Audit Vault Console:

```
avctl start_av
AVCTL started
Starting agent OC4J...
OC4J started successfully.
Oracle Audit Vault 10g Database Control Release 10.2.2.0.0  Copyright (c)
1996,2005 Oracle Corporation.  All rights reserved.
http://atacw05.us.oracle.com:5521/av
Oracle Audit Vault 10g is running.
------------------------------------
Logs are generated in directory /oracle/product/10.2.2/av_1/av/log
```

start_collector

Starts the collector. This command is run on the Audit Vault Server.

Syntax

```
avctl start_collector -collname <collector name> -srcname <source name>
```

Arguments

Argument	Description
-collname	Specify the collector (by collector name) to be started.
-srcname	Specify the name of the source to which the collector (specified in the -collname argument) belongs.

Usage Notes

- On successful completion of this command, the collector is moved to a RUNNING state. If an error is encountered, the collector is moved to an ERROR state.
- Audit Vault accepts audit records only from collectors in the RUNNING state.

Example

The following example shows how to start the collector in Audit Vault:

```
avctl start_collector -collname REDO_Collector
-srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Starting Collector...
Collector started successfully.
```

start_oc4j

Starts the agent OC4J. This command is run on the Audit Vault Agent.

Syntax

```
avctl start_oc4j [-loglevel error|warning|info|debug]
```

Arguments

Argument	Description
`[-loglevel error|warning|info|debug]`	Optionally, specify the desired level of logging.

Usage Notes

It is possible for the Agent OC4J process to terminate abnormally. Use this command on the command line to manually start the agent OC4J.

Example

The following example shows how to start OC4J:

```
avctl start_oc4j
AVCTL started
Starting agent OC4J...
OC4J started successfully.
```

stop_agent

Stops the agent. This command is run on the Audit Vault Server.

Syntax

```
avctl stop_agent -agentname <agent name>
```

Arguments

Argument	Description
`-agentname`	Specify the agent (by agent name) to be stopped.

Usage Notes

- This command will first stop all collectors running at this agent, and then stop the agent itself.
- On successful completion of this command, the agent and its collectors are moved to a STOPPED state.
- If an error is encountered, the agent is moved to an ERROR state. Audit Vault accepts audit records only from agents in the RUNNING state.
- This is usually a maintenance operation.

Example

The following example shows how to stop the agent in Audit Vault:

```
avctl stop_agent -agentname OC4JAGENT1
AVCTL started
Stopping Agent...
Agent stopped successfully.
```

stop_av

Stops the Audit Vault Console. This command is run on the Audit Vault Server.

Syntax

```
avctl stop_av
```

Arguments

None

Usage Notes

This command executes an `emctl stop dbconsole` command.

Example

The following example shows how to stop the Audit Vault Console:

```
avctl stop_av
AVCTL started
Stopping OC4J...
OC4J stopped successfully.
```

stop_collector

Stops the collector. This command is run on the Audit Vault Server.

Syntax

```
avctl stop_collector -collname <collector name> -srcname <source name>
```

Arguments

Argument	Description
`-collname`	Specify the collector (by collector name) to be stopped.
`-srcname`	Specify the name of the source to which the collector (specified in the `-collname` argument) belongs.

Usage Notes

- On successful completion of this command, the collector is moved to a STOPPED state.
- If an error is encountered, the collector is moved to an ERROR state.
- Audit Vault accepts audit records only from collectors in the RUNNING state.
- This is usually a maintenance operation.

Example

The following example shows how to stop the collector in Oracle Audit Vault:

```
avctl stop_collector -collname STREAMSCOLLECTOR
-srcname ORCL.REGRESS.RDBMS.DEV.US.ORACLE.COM
AVCTL started
Stopping Collector...
Collector stopped successfully.
```

stop_oc4j

Stops the agent OC4J. This command is run on the Audit Vault Agent.

Syntax

```
avctl stop_oc4j
```

Arguments

None

Usage Notes

This is usually a maintenance operation.

Example

The following example shows how to stop the agent OC4J:

```
avctl stop_oc4j
AVCTL started
Stopping agent OC4J...
OC4J stopped successfully.
```

C

Audit Vault Oracle Database (AVORCLDB) Reference

Audit Vault Oracle Database (AVORCLDB) is a command-line utility that provides the ability to configure (add, alter, and drop) Oracle audit sources and Oracle collectors, verify source compatibility with the collectors, and set up Oracle Database audit sources for audit data collection by establishing the connection to the source through the collector.

Table C–1 describes the AVORCLDB commands and where each is used, whether on the Audit Vault Server, on the Audit Vault Agent, or in both places.

Table C–1 AVORCLDB Commands

Command	Where Used?	Description
add_collector	Server	Adds a collector to Audit Vault
add_source	Server	Registers an audit source with Audit Vault
alter_collector	Server	Alters the attributes of a collector
alter_source	Server	Alters the attributes of a source
drop_collector	Server	Drops a collector from Audit Vault
drop_source	Server	Drops a source from Audit Vault
-help	Both	Displays Help for the AVORCLDB commands
setup	Agent	Sets up the database link from the source database through the Audit Vault Agent to the Audit Vault database (repository) and verifies the connection using the wallet
verify	Both	Verifies that the source is compatible with the collectors that are specified for setup

avorcldb

The AVORCLDB command-line utility.

Syntax

```
avorcldb <command> -help

avorcldb <command> [<options>] <arguments>
```

Arguments

Argument	Description
`<command>`	One of the following commands: `add_source`, `alter_source`, `drop_source`, `add_collector`, `alter_collector`, `drop_collector`, `setup`, or `verify`
`[<options>]`	The optional AVORCLDB options
`<arguments>`	One or more of the AVORCLDB command arguments
`-help`	Displays Help for the AVORCLDB commands

Options

Table C–2 describes the options for the AVORCLDB commands.

Table C–2 AVORCLDB Options

Option	Description
`-verbose`	Provides more detailed output to standard output
`-trace <level>`	Controls the amount of information logged. The `<level>` argument can be one of the following: ERROR, WARN, or INFO.

Usage Notes

- Issuing an AVORCLDB command generates the following log file: `$ORACLE_HOME/av/log/avorcldb.log`.
- The AVORCLDB command can be issued any number of times. The AVORCLDB command checks to see if a step has already been completed, and returns a warning in each such case, then skips that step and continues until it is completed.

Example

The following output is from the `avorcldb` command executed in the Audit Vault Server home shell.

```
$ avorcldb -help

  Oracle DB Setup for Audit Vault
  -------------------------------

  Usage :
    avorcldb help
    avorcldb <command> -help
    avorcldb <command> <arguments>
```

```
Source setup commands

    verify
          -src <host:port:service> -srcusr <usr>/<pwd>
          -colltype [OSAUD,DBAUD,REDO,EVTLOG,ALL]

    add_source
          -src <host:port:service> -srcusr <usr>/<pwd> -avsrcusr <usr>
          [-srcname <srcname>] [-desc <desc>] [-agentname <agentname>]

    alter_source
          -srcname <srcname> [attrname=value]+

    drop_source
          -srcname <srcname>

Collector setup commands

    add_collector
          -srcname <srcname> -srcusr <usr>/<pwd> -agentname <agentname>
          -colltype [OSAUD|DBAUD|REDO|EVTLOG] [-collname <collname>]
          [-desc <desc>] [-avsrcusr <usr>/<pwd>] [-av <host:port:service>]
          [-instname <instname>]

    alter_collector
          -srcname <srcname> -collname <collname> [attrname=value]+

    drop_collector
          -srcname <srcname> -collname <collname>
```

The following output is from the `avorcldb` command executed in the Audit Vault Agent home shell.

```
$ avorcldb -help

  Oracle DB Setup for Audit Vault
  -------------------------------

  Usage :
    avorcldb help
    avorcldb <command> -help
    avorcldb <command> <arguments>


Agent Commands

    verify
          -src <host:port:service> -srcusr <usr>/<pwd>
          -colltype [OSAUD,DBAUD,REDO,EVTLOG,ALL]

    setup
          -srcname <srcname> -srcusr <usr>/<pwd> -wpwd <pwd>
```

add_collector

Adds a collector for the given source to Audit Vault. The source is verified for requirements of the collector. This command is run on the Audit Vault Server.

Syntax

```
avorcldb add_collector -srcname <srcname> -srcusr <usr>/<pwd>
-agentname <agentname> -colltype [OSAUD,DBAUD,REDO,EVTLOG] [-collname <collname>]
[-desc <desc>] [-avsrcusr <usr>/<pwd>] [-av <host:port:service>]
[-instname <instname>]
```

Arguments

Argument	Description
`-srcname <srcname>`	The source name for which the collector is to be added
`-srcusr <usr>/<pwd>`	The credentials of the user on the source database to collect audit data. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`usr/pwd`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
`-agentname <agentname>`	The agent name where the collector is to be added
`-colltype [OSAUD,DBAUD,REDO,EVTLOG]`	The collector type to be added
`[-collname <collname>]`	The collector name. This argument is optional. If this argument is not specified, `<colltype>_Collector` will be used.
`[-desc <desc>]`	A brief description of the collector. This argument is optional.
`[-avsrcusr <usr>/<pwd>]`	The user on Audit Vault associated with the given source. This argument is required if the `-colltype` argument is REDO; otherwise, this argument is optional. The `-avsrcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_AVSRCUSR` is set to *`usr/pwd`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
`[-av <host:port:service>]`	The connection information for Audit Vault used for the database link from the source database to Audit Vault. This argument is required if the `-colltype` argument is REDO; otherwise, this argument is optional.
`[-instname <instname>]`	The instance name of Audit Vault Oracle RAC installation. This argument must be used to add multiple OSAUD collectors (one for each instance).

Usage Notes

- Run any collector-specific preparation scripts before you execute the AVCA add_collector command.
- The user specified in the -srcusr argument must exist on the source database.

Example

The following example shows how to add an OSAUD collector to Oracle Audit Vault on Linux and UNIX platforms in an Oracle Real Application Clusters (Oracle RAC) installation using the -instname argument. In these examples, the AVORCLDB_SRCUSR environment variable is set to srcusr1/*pwd* and the -srcusr argument is omitted.

```
avorcldb add_collector -srcname source1db.domain.com
-agentname 'Agent1' -colltype OSAUD -instname av01
source SOURCE1DB.DOMAIN.COM verified for OS File Audit Collector collector
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): OSAUD_Collector
```

The following example shows how to add an OSAUD collector to Oracle Audit Vault on Windows platforms for the event log:

```
avorcldb add_collector -srcname source1db.domain.com
-agentname agent1
-colltype EVTLOG
source SOURCE1DB.DOMAIN.COM verified for Windows Event Log Audit Collector
collector
Adding collector...
Collector added sucessfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): EVTLOG_Collector
```

The following example shows how to add a DBAUD collector to Audit Vault:

```
avorcldb add_collector -srcname source1db.domain.com
-agentname 'Agent1' -colltype DBAUD
source SOURCE1DB.DOMAIN.COM verified for Aud$/FGA_LOG$ Audit Collector collector
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): DBAUD_Collector
```

The following example shows how to add a REDO collector to Audit Vault. In this example, the AVORCLDB_AVSRCUSR environment variable is set to avsrcuser1/*pwd* and the -avsrcusr argument is omitted.

```
avorcldb add_collector -srcname source1db.domain.com
-agentname 'Agent1' -colltype REDO
-av system1.domain.com:1521:av
source SOURCE1DB.DOMAIN.COM verified for REDO Log Audit Collector collector
Adding collector...
Collector added successfully.
```

```
collector successfully added to Audit Vault

remember the following information for use in avctl
Collector name (collname): REDO_Collector
initializing REDO Collector
setting up APPLY process on Audit Vault server
setting up CAPTURE process on source database
```

add_source

Registers an audit source with Audit Vault for audit data consolidation. This command is run on the Audit Vault Server.

Syntax

```
avorcldb add_source -src <host:port:service> -srcusr <usr>/<pwd>
-avsrcusr <usr> [-srcname <srcname>] [-desc <desc>] [-agentname <agentname>]
```

Arguments

Argument	Description
`-src <host:port:service>`	Source database connection information: host name, port number, and service ID (SID), separated by a colon
`-srcusr <usr>/<pwd>`	Credentials of the user on the source database to collect audit data. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`usr/password`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
`-avsrcusr <usr>`	The user on Audit Vault used to send audit data
`[-srcname <srcname>]`	Optional source name. If this argument is not specified, the global database name of the source will be used.
`[-desc <desc>]`	Optional description of the source
`[-agentname <agentname>]`	Optional agent name to configure policy management

Usage Notes

- For the REDO collector, you should run any source-specific preparation scripts on the agent and on the Audit Vault system before you execute the AVORCLDB `add_source` command.
- The global database name of the source database is used as the source name in Oracle Audit Vault.
- The user specified in the `-srcusr` argument must exist on the source database.
- The user specified in the `-avsrcusr` argument must exist on Oracle Audit Vault.

Example

The following example shows how to register a source with Oracle Audit Vault. In this example, the `AVORCLDB_SRCUSR` environment variable is set to `srcusr1/`*`pwd`* and the `-srcusr` argument is omitted.

```
avorcldb add_source -src lnxserver:4523:hrdb.domain.com
-avsrcusr srcusr1 -desc 'HR Database'
Adding source...
Source added successfully.
source successfully added to Audit Vault

remember the following information for use in avctl
Source name (srcname): RDBMSRC1.US.ORACLE.COM
map_source_to_agent
```

```
map_source_to_agent
```

alter_collector

Modifies the attributes of a collector. This command is run on the Audit Vault Server.

Syntax

```
avorcldb alter_collector -srcname <srcname> -collname <collname>
      [<attrname>=<attrvalue>...<attrname>=<attrvalue>]
```

Arguments

Argument	Description
`-srcname <srcname>`	Specify the source (by source name) to which this collector belongs.
`-collname <collname>`	Specify the collector (by collector name) to be modified.
`[<attrname>=<attrvalue>]`	Specify the pair (attribute name, new attribute value) for mutable collector attributes for this collector type. This argument is optional. Separate multiple pairs by a space on the command line.

Usage Notes

You can modify one or more collector attributes at a time. Table C–3, Table C–4, and Table C–5 list the collector attributes (parameters) by collector type, whether the parameter is mutable, and its default value.

Table C–3 DBAUD Collector Attributes

Parameter	Mutable	Default Value
AUDAUDIT_DELAY_TIME	Yes	20 seconds
AUDAUDIT_SLEEP_TIME	Yes	5000 seconds
AUDAUDIT_ACTIVE_SLEEP_TIME	Yes	1000 seconds
AUDAUDIT_MAX_PROCESS_RECORDS	Yes	1000 centiseconds
AUDAUDIT_SORT_POLICY	Yes	NULL
AUDAUDIT_AUDIT_VAULT_ALIAS	No	NULL
AUDAUDIT_SOURCE_ALIAS	No	NULL

Table C–4 OSAUD Collector Attributes

Parameter	Mutable	Default Value
OSAUDIT_DEFAULT_FILE_DEST	Yes	$ORACLE_HOME/audit
OSAUD_FILE_DEST	Yes	$ORACLE_HOME/aidit
OSAUDIT_NLS_LANGUAGE	Yes	AMERICAN
OSAUDIT_NLS_TERRITORY	Yes	AMERICA
OSAUDIT_NLS_CHARSET	Yes	WE8ISO8859P1
OSAUDIT_LOG_LEVEL	Yes	WARNING
OSAUDIT_MAX_PROCESS_TIME	Yes	600 centiseconds

Table C–4 (Cont.) OSAUD Collector Attributes

Parameter	Mutable	Default Value
OSAUDIT_MAX_PROCESS_RECORDS	Yes	10000
OSAUDIT_CHANNEL_TYPE	No	NULL
OSAUDIT_AUDIT_VALUE_ALIAS	No	NULL
OSAUDIT_NT_ORACLE_SID	Yes	NULL

Table C–5 REDO Collector Attributes

Parameter	Mutable	Default Value
STRCOLL_SRCADM_NAME	No	NULL
STRCOLL_SRCADM_ALIAS	No	NULL
STRCOLL_HEARTBEAT_TIME	Yes	60 seconds
STRCOLL_DBSERVICE	No	NULL
STRCOLL_DBPORT	Yes	NULL
AV.DATABASE.NAME	No	NULL

Example

The following example shows how to alter the `AUDAUDIT_DELAY_TIME` attribute for the DBAUD_Collector collector in Audit Vault:

```
avorcldb alter_collector -srcname lnxserver.domain.com -collname DBAUD_Collector
AUDAUDIT_DELAY_TIME=60
Altering collector...
Collector altered successfully.
```

alter_source

Modifies the attributes of the source. This command is run on the Audit Vault Server.

Syntax

```
avorcldb alter_source -srcname <srcname>
      [<attrname>=<attrvalue>...<attrname>=<attrvalue>]
```

Arguments

Argument	Description
`-srcname <srcname>`	Specify the source (by source name) to be modified.
`[<attrname>=<attrvalue>]`	Specify the pair (attribute name, new attribute value) for the mutable source attributes of this source to be modified. This argument is optional. Separate multiple pairs by a space on the command line.

Usage Notes

You can modify one or more source attributes at a time. Table C–6 lists the source attributes (parameters), the values allowed for certain parameters, whether the parameter is mutable, and its default value.

Table C–6 Source Attributes

Parameter	Description	Mutable	Default Value
SOURCETYPE	A new source type name for this source	Yes	NULL
NAME	A new name for this source	Yes	NULL
HOST	A new source host name	Yes	NULL
HOSTIP	A new source host IP address	Yes	NULL
VERSION	A new source version	Yes	NULL
TIMEZONE	A new time zone for this source	Yes	NULL
USERNAME	A new user name used to connect to this audit data source	Yes	NULL
PASSWORD	The password of the user used to connect to this audit data source	Yes	NULL
AUTHETICATION	A new authentication method, either AUTH_TYPE_PWD or AUTH_TYPE_SSL	Yes	NULL
DESCRIPTION	A new description for this source	Yes	NULL
DB_SERVICE	A new audit data source service name	Yes	NULL
PORT	A new port number for this system where the source audit data resides	Yes	NULL
GLOBAL_DATABASE_NAME	The new global database name	Yes	NULL
WALLET_LOC	The new wallet location, if used, for this audit data source	Yes	NULL

Example

The following example shows how to alter the DESCRIPTION and SOURCE_HOST attributes for the source named lnxserver.domain.com in Oracle Audit Vault:

```
avorcldb alter_source -srcname lnxserver.domain.com DESCRIPTION='HR Database'
SOURCE_HOST='lnxserver.domain.com'
Altering source...
Source altered successfully.
```

drop_collector

Drops a collector from Oracle Audit Vault. This command is run from the Audit Vault Server.

Syntax

```
avorcldb drop_collector -srcname <srcname> -collname <collname>
```

Arguments

Argument	Description
`-srcname <srcname>`	Specify the name of the source to which the collector (specified in the `-collname` argument) belongs.
`-collname <collname>`	Specify the collector (by collector name) to be dropped from Oracle Audit Vault.

Usage Notes

The `drop_collector` command will not delete the collector from Oracle Audit Vault; it actually disables the collector. The user can neither add the same collector name again nor enable the old name.

Example

The following example shows how to drop the collector named 'DBAud_Collector' from Oracle Audit Vault:

```
avorcldb drop_collector -srcname lnxserver.domain.com -collname DBAud_Collector
Dropping collector...
Collector dropped successfully.
```

drop_source

Drops a source from Oracle Audit Vault. This command is run on the Audit Vault Server.

Syntax

```
avorcldb drop_source -srcname <srcname>
```

Arguments

Argument	Description
-srcname <srcname>	Specify the source (by source name) to be dropped from Oracle Audit Vault.

Usage Notes

- The drop_source command does not delete the source from Oracle Audit Vault; it disables the source. The user can neither add the same source name again nor enable the old source. Audit data from this source is no longer collected once the source has been dropped, but the information of this source is maintained in Oracle Audit Vault with a status as dropped (inactive) for future reporting purposes.
- A source cannot be dropped or deleted if there are any active collectors for this source. All collectors must be inactive (dropped) to successfully drop a source from Oracle Audit Vault.

Example

The following example shows how to drop the source named lnxserver.domain.com from Oracle Audit Vault:

```
avorcldb drop_source -srcname lnxserver.domain.com
Dropping source...
Source dropped successfully.
```

-help

Displays Help for the AVORCLDB commands. This command is run on both the Audit Vault Server and the Audit Vault Agent.

Syntax

```
avorcldb -help

avorcldb <command> -help
```

Arguments

Argument	Description
`<command>`	The name of an AVORCLDB command for which you want Help to appear

Usage Notes

None

Example

The following example shows how to display general AVORCLDB utility Help in Audit Vault:

```
avorcldb -help
```

The following example shows how to display specific AVORCLDB Help for the `add_source` command in the Audit Vault Server home shell.

```
$ avorcldb add_source -help
  avorcldb add_source command

    add_source
          -src <host:port:service> -srcusr <usr>/<pwd> -avsrcusr <usr>
          [-srcname <srcname>] [-desc <desc>] [-agentname <agentname>]

  Purpose: The source is added to Audit Vault. The global DB Name
       of the source database is used as the Source Name in Audit Vault.
       The user specified in -srcusr argument must exist on the source DB.
       The user specified in -avsrcusr argument must exist on Audit Vault.

  Arguments:
       -src        : Source DB connection information
       -srcusr     : Credentials of user on Source DB to collect audit data
       -avsrcusr   : User on Audit Vault used to send audit data
       -srcname    : Optional name of source, default : <global_dbname>
       -desc       : Optional description of the source
       -agentname  : Optional agent name to configure policy management

  Examples:
     avorcldb add_source -src lnxserver:4523:hrdb.domain.com
         -srcusr srcusr/passwd -avsrcusr avsrcuser -desc 'HR Database'
```

setup

Sets up the database link from the source database through the Audit Vault Agent to the Audit Vault database (repository) and verifies the connection using the wallet. This command is run on the Audit Vault Agent.

Syntax

```
avorcldb setup -srcname <srcname> -srcusr <usr>/<pwd> -wpwd <pwd>
```

Arguments

Argument	Description
`-srcname <srcname>`	The name of the source database
`-srcusr <usr>/<pwd>`	Credentials of the user on the source database to collect audit data. The `-srcusr` argument can be omitted if the corresponding environment variable, `AVORCLDB_SRCUSR` is set to *`usr/pwd`*. If the command-line argument `-srcusr` is specified, then the command-line argument overrides the environment variable.
`-wpwd <pwd>`	The wallet password (the password needed to open the wallet). This is the password of the agent user granted the `AV_AGENT` role. The `-wpwd` argument can be omitted if the corresponding environment variable, `AVORCLDB_WPWD` is set to *pwd*. If the command-line argument `-wpwd` is specified, then the command-line argument overrides the environment variable.

Options

See Table C–2 command for a list of options.

Usage Notes

- The source is verified for compatibility with the collectors. The source and collectors are added to Oracle Audit Vault. The source users are created as necessary (unless Oracle Database Vault is installed).
- The setup operation for the REDO collector does not start the source collector and the destination collector. Use the AVCTL start_collector command to start the REDO, OSAUD, and DBAUD collectors.

Example

The following example sets up the REDO and OSAUD collectors. In this example, the `AVORCLDB_SRCUSR` environment variable is set to `srcusr1/`*`pwd`* and the `AVORCLDB_WPWD` environment variable is set to *pwd* and the `-srcusr` and `-wpwd` arguments are omitted.

```
avorcldb setup -verbose -srcname lnxserver:hrdb.domain.com
updated tnsnames.ora with alias [SRCDB1] to source database
adding credentials for user srcdba2 for connection [SRCDB1]
Storing user credentials in wallet...
Create credential oracle.security.client.connect_string2
done.
verifying SRCDB1 connection using wallet
```

verify

Verifies that the source is compatible for setting up the specified collectors. This command can be run on both the Audit Vault Server and the Audit Vault Agent.

Syntax

```
avorcldb verify -src <host:port:service> -srcusr <usr>/<pwd>
       -colltype [OSAUD,DBAUD,REDO,EVTLOG,ALL]
```

Arguments

Argument	Description
-src <host:port:service>	Source database connection information: host name, port number, and service ID (SID), separated by a colon
-srcusr <usr>/<pwd>	Credentials of the user with privileges required to verify the source. The -srcusr argument can be omitted if the corresponding environment variable, AVORCLDB_SRCUSR is set to *usr/pwd*. If the command-line argument -srcusr is specified, then the command-line argument overrides the environment variable.
-colltype [OSAUD,DBAUD,REDO,EVTLOG,ALL]	List of collector types [REDO, DBAUD, OSAUD, EVTLOG] or ALL

Options

See Table C–2 for a list of options.

Usage Notes

None

Example

The following example verifies that the source is compatible with the OSAUD, DBAUD, and REDO collectors on a Linux or UNIX-based system. For Windows systems, one additional OS File Audit Collector type is displayed for collecting audit records from the Windows event log. In this example, the AVORCLDB_SRCUSR environment variable is set to srcusr1/*pwd* and the -srcusr argument is omitted.

```
avorcldb verify -src lnxserver:4523:hrdb.domain.com -colltype ALL
source HRDB.DOMAIN.COM verified for OS File Audit Collector collector
source HRDB.DOMAIN.COM verified for Aud$/FGA_LOG$ Audit Collector collector
source HRDB.DOMAIN.COM verified for REDO Log Audit Collector collector
```

D

REDO Collector Database Reference

This appendix describes recommendations for setting initialization parameters for participating source sites for Oracle Database audit sources for the following releases: Oracle9*i* Database release 2 (9.2), Oracle Database 10*g* release 1 (10.1), and Oracle Database 10*g* release 2 (10.2). It is divided into the following sections:

- Initialization Parameter Recommendations for Audit Sources on Oracle9i Database Release 2 (9.2)
- Initialization Parameter Recommendations for Audit Sources on Oracle Database 10g Release 1 (10.1)
- Initialization Parameter Recommendations for Audit Sources on Oracle Database 10g Release 2 (10.2)

After changing these initialization parameters described in these sections, the DBA must restart the source database before an Oracle Redo Log Collector is set up to collect audit data.

D.1 Initialization Parameter Recommendations for Audit Sources on Oracle9*i* Database Release 2 (9.2)

At each participating source site, configure the initialization parameters for each database to include the following hidden parameters (see Table D–1).

Table D–1 Hidden Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_first_spare_parameter=200M/(current_shared_pool_size+200M)	Mandatory	10	The threshold (percent) of shared_pool_size memory at which spillover to disk is triggered for captured messages
_kghdsidx_count=1	Recommended	Range: 10 to 80	This parameter prevents the shared_pool from being divided among cpus.
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue
_spin_count=5000	Recommended	2000	See the *Oracle Magazine* Tuning article from March 2003 for a discussion of this parameter. Set this parameter if Memory Queue and Memory Queue Subscriber latch sleeps are high.

At each participating source site, confirm that the following required initialization parameters are set appropriately for each database (see Table D–2). The SHARED_POOL_SIZE parameter is of particular importance for REDO collectors.

Table D–2 Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
AQ_TM_PROCESSES=4	Mandatory	Default: 0 Range: 0 to 10	Establishes queue monitor processes. Setting the parameter to 1 or more starts the specified number of queue monitor processes. These queue monitor processes are responsible for managing time-based operations of messages such as delay and expiration, cleaning up retained messages after the specified retention time, and cleaning up consumed messages if the retention time is zero. This parameter is required for both Streams captured messages and user-enqueued messages.
COMPATIBLE=9.2.0	Mandatory	Default: `8.1.0` Range: `8.1.0` to Current Release Number	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use Streams, this parameter must be set to `9.2.0` or higher.
GLOBAL_NAMES=true	Recommended	Default: `false` Range: `true` or `false`	Specifies whether a database link is required to have the same name as the database to which it connects. If you want to use Streams to share information between databases, then set this parameter to true at each database that is participating in your Streams environment.
JOB_QUEUE_ PROCESSES=4	Mandatory	Default: 0 Range: 0 to 1000	Specifies the number of Jnnn job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by `DBMS_JOB`. You can change the setting for `JOB_QUEUE_PROCESSES` dynamically by using the `ALTER SYSTEM` statement. This parameter must be set to at least 2 at each database that is propagating events in your Streams environment, and should be set to the same value as the maximum number of jobs that can run simultaneously plus two.
LOG_PALALLELISM=1 This parameter has to be set to 1. Note that the default value is 1.	Mandatory	Default: 1 Range: 1 to 255	Specifies the level of concurrency for redo allocation within Oracle. If you plan to run one or more capture processes on a database, then this parameter must be set to 1. Setting this parameter to 1 does not affect the parallelism of capture. You can set parallelism for a capture process using the `SET_PARAMETER` procedure in the `DBMS_CAPTURE_ADM` package.
LOGMNR_MAX_ PERSISTENT_ SESSIONS=3 This parameter must be set to at least 1 which is also the default value.	Mandatory	Default: 1 Range: 1 to `LICENSE_MAX_ SESSIONS`	Specifies the maximum number of persistent LogMiner mining sessions that are concurrently active when all sessions are mining redo logs generated by instances. If you plan to run multiple Streams capture processes on a single database, then set this parameter equal to or higher than the number of planned capture processes.
OPEN_LINKS=4	Recommended	Default: 4 Range: 0 to 255	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In a Streams environment, ensure that this parameter is set to the default value of 4 or higher.

Table D–2 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
PARALLEL_MAX_ SERVERS=20	Mandatory	Default: Derived from the values of the following parameters: CPU_COUNT PARALLEL_ ADAPTIVE_MULTI_ USER PARALLEL_ AUTOMATIC_ TUNING Range: 0 to 3599	Specifies the maximum number of parallel execution processes and parallel recovery processes for an instance. As demand increases, Oracle will increase the number of processes from the number created at instance startup up to this value. In a Streams environment, each capture process and apply process can use multiple parallel execution servers. Set this initialization parameter to an appropriate value to ensure that there are enough parallel execution servers.
PROCESSES	Recommended	Default: Derived from PARALLEL_ MAX_SERVERS Range: 6 to operating system dependent limit	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 231	Specifies the maximum number of sessions that can be created in the system. If you plan to run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE Increase by at least 200M	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system dependent limit	Specifies the maximum size of SGA for the lifetime of a database instance. If you plan to run multiple capture processes on a single database, then you may need to increase the size of this parameter.

Table D–2 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE= (Increase by at least 200M)	Mandatory	Default: 32-bit platforms: 8 MB, rounded up to the nearest granule size 64-bit platforms: 64 MB, rounded up to the nearest granule size Range: Minimum: the granule size Maximum: operating system-dependent	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. You should increase the size of the shared pool by 10 MB for each capture process on a database. Additional memory is required from the shared_pool for storing logical change records (LCRs) in the buffer queue. This parameter should be sized so that LCRs remain in memory as much as possible. Use the formula shared_pool_size*_first_spare_parameter/100 to calculate the point at which LCRs will spill to disk.
TIMED_STATISTICS	Recommended	Default: If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. Range: true or false	Specifies whether or not statistics related to time are collected. If you want to collect elapsed time statistics in the data dictionary views related to Streams, then set this parameter to true. The views that include elapsed time statistics include: V$STREAMS_CAPTURE V$STREAMS_APPLY_COORDINATOR V$STREAMS_APPLY_READER V$STREAMS_APPLY_SERVER
TRANSACTION_AUDITING=TRUE	Mandatory	Default: TRUE Range: true or false	If TRANSACTION_AUDITING is true, Oracle generates a special redo record that contains the user logon name, username, the session ID, some operating system information, and client information. For each successive transaction, Oracle generates a record that contains only the session ID. These subsequent records link back to the first record, which also contains the session ID. These records might be useful if you are using a redo log analysis tool. You can access the records by dumping the redo log. If TRANSACTION_AUDITING is false, no redo record will be generated. TRANSACTION_AUDITING must be set to TRUE for databases with a Streams capture process configured

An additional initialization parameter must be configured at each instance involved in the Oracle Real Application Clusters (Oracle RAC) configuration. In addition to the parameters referenced previously, the parameter Table D–3 should be included.

Table D–3 An Additional Initialization Parameter to Be Configured at Each Instance Involved in the Oracle RAC Configuration at the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
ARCHIVE_LAG_TARGET=1800	Recommended	Default: 0 Range: 0 or any integer in [60, 7200]	Limits the amount of data that can be lost and effectively increases the availability of the standby database by forcing a log switch after a user-specified time period elapses. If you are using Streams in a Real Application Clusters environment, then set this parameter to a value greater than zero to switch the log files automatically. See Also: The section titled "Streams Capture Processes and Oracle Real Application Clusters" in *Oracle9i Streams* release 2 (9.2)

D.2 Initialization Parameter Recommendations for Audit Sources on Oracle Database 10*g* Release 1 (10.1)

At each participating source site, configure the initialization parameters for each database to include the following hidden parameters (see Table D–4).

Table D–4 Hidden Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue
_spin_count=5000	Recommended	2000	See the Oracle Magazine Tuning article from March 2003 for a discussion of this parameter. Set this parameter if Memory Queue and Memory Queue Subscriber latch sleeps are high.

At each participating source site, confirm that the following required initialization parameters are set appropriately for each database (see Table D–5).

Table D–5 Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE= 10.1.0	Mandatory	Default: `9.2.0` Range: `9.2.0` to Current Release Number Modifiable?: No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10*g*, this parameter must be set to `10.1.0` or higher. To use downstream capture, this parameter must be set to `10.1.0` or higher at both the source database and the downstream database.
Cursor_space_for_time= FALSE This parameter has to be set to FALSE. Note that FALSE is the default value for this parameter.	Mandatory	Default: `FALSE` Range: `FALSE` or `TRUE`	Do not change this parameter when using Streams or Logical Standby.
GLOBAL_NAMES=true	Recommended	Default: `false` Range: `true` or `false` Modifiable?: Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to `true` at each database that is participating in your Streams environment.

Table D–5 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
JOB_QUEUE_ PROCESSES=4	Mandatory	Default: 0 Range: 0 to 1000 Modifiable?: Yes	Specifies the number of Jnnn job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by DBMS_JOB. This parameter must be set to at least 2 at each database that is propagating events in your Streams environment, and should be set to the same value as the maximum number of jobs that can run simultaneously plus two.
LOG_ARCHIVE_ DEST_n	Recommended	Default: None Range: None Modifiable?: Yes	Defines up to ten log archive destinations, where n is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process. See Also: *Oracle Data Guard Concepts and Administration*

LOG_ARCHIVE_ DEST_STATE_n	Recommended	Default: `enable`
		Range: One of the following: `alternate`
		`reset`
		`defer`
		`enable`
		Modifiable?: Yes
			Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding LOG_ARCHIVE_DEST_n destination parameters.
			To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_ DEST_n destination for the downstream database is set to enable.

OPEN_LINKS	Recommended	Default: 4 Range: 0 to 255 Modifiable?: No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In a Streams environment, ensure that this parameter is set to the default value of 4 or higher.

PARALLEL_MAX_ SERVERS
Set this parameter to at least 20.
	Mandatory	Default: Derived from the values of the following parameters: `CPU_COUNT`
		`PARALLEL_ ADAPTIVE_ MULTI_USER`
		`PARALLEL_ AUTOMATIC_ TUNING`
		Range: 0 to 3599
		Modifiable?: Yes
			Specifies the maximum number of parallel execution processes and parallel recovery processes for an instance. As demand increases, Oracle will increase the number of processes from the number created at instance startup up to this value.
			In a Streams environment, each capture process and apply process can use multiple parallel execution servers. Set this initialization parameter to an appropriate value to ensure that there are enough parallel execution servers.

PROCESSES	Recommended	Default: Derived from PARALLEL_ MAX_SERVERS Range: 6 to operating system dependent limit Modifiable?: No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
REMOTE_ARCHIVE_ ENABLE	Recommended	Default: true Range: true or false Modifiable?: No	Enables or disables the sending of redo archival to remote destinations and the receipt of remotely archived redo. To use downstream capture and copy the redo log files to the downstream database using log transport services, this parameter must be set to `true` at both the source database and the downstream database.

Table D–5 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 231 Modifiable?: No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE Increase by at least 200M	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system dependent limit Modifiable?: No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter.
SHARED_POOL_SIZE	Recommended	Default: 32-bit platforms: 32 MB, rounded up to the nearest granule size 64-bit platforms: 84 MB, rounded up to the nearest granule size Range: Minimum: the granule size Maximum: operating system dependent Modifiable?: Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If the `STREAMS_POOL_SIZE` initialization parameter is set to zero, then Streams can use up to 10% of the shared pool.

Table D–5 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_ SIZE>200M If using sga_target, also increase this value by at least 200M.	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system dependent Modifiable?: Yes	Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, the Streams pool is used for internal communications during parallel capture and apply. If the size of the Streams pool is greater than zero, then any SGA memory used by Streams is allocated from the Streams pool. If the Streams pool size is set to zero, then SGA memory used by Streams is allocated from the shared pool and can use up to 10% of the shared pool. This parameter is modifiable. However, if this parameter is set to zero when an instance starts, then increasing it beyond zero has no effect on the current instance because it is using the shared pool for Streams allocations. Also, if this parameter is set to a value greater than zero when an instance starts and is then reduced to zero when the instance is running, then Streams processes and jobs will not run. You should increase the size of the Streams pool for each of the following factors: 10 MB for each capture process parallelism 1 MB for each apply process parallelism 10 MB or more for each queue staging captured events For example, if parallelism is set to 3 for a capture process, then increase the Streams pool by 30 MB. If parallelism is set to 5 for an apply process, then increase the Streams pool by 5 MB.

TIMED_STATISTICS	Recommended	Default: If `STATISTICS_ LEVEL` is set to `TYPICAL` or `ALL`, then `true`
		If `STATISTICS_ LEVEL` is set to `BASIC`, then `false`
		The default for `STATISTICS_ LEVEL` is `TYPICAL`.
		Range: `true` or `false`
		Modifiable?: Yes
			Specifies whether or not statistics related to time are collected.
			To collect elapsed time statistics in the data dictionary views related to Streams, set this parameter to true. The views that include elapsed time statistics include:
			`V$STREAMS_CAPTURE`
			`V$STREAMS_APPLY_COORDINATOR`
			`V$STREAMS_APPLY_READER`
			`V$STREAMS_APPLY_SERVER`

UNDO_ RETENTION=3600	Mandatory	Default: 900 Range: 0 to 2^32-1 (max value represented by 32 bits) Modifiable?: Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least `3600`. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the `UNDO_RETENTION` setting. See Also: *Oracle Database Administrator's Guide* for more information about the retention period and the undo tablespace

D.3 Initialization Parameter Recommendations for Audit Sources on Oracle Database 10*g* Release 2 (10.2)

For best results in a REDO collector environment, set the following initialization parameters at each participating database: compatible, global_names, _job_queue_interval, sga_target, streams_pool_size.

At each participating source site, configure the initialization parameters for each database to include the following hidden parameters (see Table D–6).

Table D–6 Hidden Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue
_spin_count=5000	Recommended	2000	See the Oracle Magazine Tuning article from March 2003 for a discussion of this parameter. Set this parameter if Memory Queue and Memory Queue Subscriber latch sleeps are high.

At each participating source site, confirm that the following required initialization parameters are set appropriately for each database (see Table D–7). Enable autotuning of the various pools within the SGA, by setting SGA_TARGET to a large nonzero value. Leave the STREAMS_POOL_SIZE value set to 0. The combination of these to parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table D–7 Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE= 10.2.0	Mandatory	Default: `10.0.0` Range: `9.2.0` to Current Release Number Modifiable?: No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10*g* release 1, this parameter must be set to `10.1.0` or higher. To use downstream capture, this parameter must be set to `10.1.0` or higher at both the source database and the downstream database. To use the new Streams features introduced in Oracle Database 10*g* release 2, this parameter must be set to `10.2.0` or higher.
GLOBAL_NAMES=true	Recommended	Default: false Range: true or false Modifiable?: Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to `true` at each database that is participating in your Streams environment.
JOB_QUEUE_PROCESSES=4	Mandatory	Default: 0 Range: 0 to 1000 Modifiable?: Yes	Specifies the number of Jnnn job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by `DBMS_JOB`. This parameter must be set to at least 2 at each database that is propagating events in your Streams environment, and should be set to the same value as the maximum number of jobs that can run simultaneously plus two.

Table D–7 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_ARCHIVE_ DEST_n	Recommended	Default: None Range: None Modifiable?: Yes	Defines up to ten log archive destinations, where n is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process. See Also: *Oracle Data Guard Concepts and Administration*

LOG_ARCHIVE_ DEST_STATE_n	Recommended	Default: enable
		Range: One of the following: `alternate`
		`reset`
		`defer`
		`enable`
		Modifiable?: Yes
			Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding `LOG_ARCHIVE_DEST_n` destination parameters.
			To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the `LOG_ARCHIVE_DEST_n` destination for the downstream database is set to `enable`.

OPEN_LINKS	Recommended	Default: 4 Range: 0 to 255 Modifiable?: No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In a Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PARALLEL_MAX_ SERVERS Set this parameter to at least 20.	Mandatory	Default: Derived from the values of the following parameters: CPU_ COUNT PARALLEL_ ADAPTIVE_ MULTI_USER PARALLEL_ AUTOMATIC_ TUNING Range: 0 to 3599 Modifiable?: Yes	Specifies the maximum number of parallel execution processes and parallel recovery processes for an instance. As demand increases, Oracle will increase the number of processes from the number created at instance startup up to this value. In a Streams environment, each capture process and apply process can use multiple parallel execution servers. Set this initialization parameter to an appropriate value to ensure that there are enough parallel execution servers.
PROCESSES	Recommended	Default: Derived from PARALLEL_ MAX_SERVERS Range: 6 to operating system dependent limit Modifiable?: No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
REMOTE_ARCHIVE_ ENABLE	Recommended	Default: `true` Range: `true` or `false` Modifiable?: No	Enables or disables the sending of redo archival to remote destinations and the receipt of remotely archived redo. To use downstream capture and copy the redo log files to the downstream database using log transport services, this parameter must be set to `true` at both the source database and the downstream database.
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 231 Modifiable?: No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.

Table D–7 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SGA_MAX_SIZE Increase by at least 200M	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system dependent limit Modifiable?: No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter.
SGA_TARGET >0 Increase this parameter by at least 200M.	Mandatory	Default: 0 (SGA autotuning is disabled) Range: 64 to operating system-dependent Modifiable?: Yes	Specifies the total size of all System Global Area (SGA) components. If this parameter is set to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management.
SHARED_POOL_ SIZE=0	Recommended	Default: 32-bit platforms: 32 MB, rounded up to the nearest granule size 64-bit platforms: 84 MB, rounded up to the nearest granule size Range: Minimum: the granule size Maximum: operating system-dependent Modifiable?: Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If the `SGA_TARGET` and `STREAMS_POOL_SIZE` initialization parameters are set to zero, then Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Streams pool.

Table D–7 (Cont.) Initialization Parameters to Be Configured for the Database Source

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_ SIZE=0	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system-dependent Modifiable?: Yes	Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, the Streams pool is used for internal communications during parallel capture and apply. If the SGA_TARGET initialization parameter is set to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and STREAMS_POOL_SIZE specifies the minimum size. This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Streams processes and jobs will not run. You should increase the size of the Streams pool for each of the following factors: 10 MB for each capture process parallelism 10 MB or more for each buffered queue. The buffered queue is where the Logical Change Records(LCRs) are stored. 1 MB for each apply process parallelism You can use the V$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter. For example, if parallelism is set to 3 for a capture process, then increase the Streams pool by 30 MB. If parallelism is set to 5 for an apply process, then increase the Streams pool by 5 MB.
TIMED_STATISTICS	Recommended	Default: If STATISTICS_ LEVEL is set to TYPICAL or ALL, then true If STATISTICS_ LEVEL is set to BASIC, then false The default for STATISTICS_ LEVEL is TYPICAL. Range: true or false Modifiable?: Yes	Specifies whether or not statistics related to time are collected. To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to true. The views that include elapsed time statistics include: V$STREAMS_CAPTURE V$STREAMS_APPLY_COORDINATOR V$STREAMS_APPLY_READER V$STREAMS_APPLY_SERVER
UNDO_ RETENTION=3600	Mandatory	Default: 900 Range: 0 to 2^32-1 (max value represented by 32 bits) Modifiable?: Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting. See Also: *Oracle Database Administrator's Guide* for more information about the UNDO_RETENTION parameter

E

Audit Vault Error Messages

The following sections describe the Oracle Audit Vault error messages.

E.1 Audit Vault Server Error Messages

This section describes the Oracle Audit Vault Server-side error message codes.

E.1.1 Generic Error Codes

This section describes the generic error codes.

46501, invalid %s

Cause: Invalid value specified.

Action: Provide a valid non-NULL value with a valid length.

46502, NULL in %s

Cause: NULL value specified.

Action: Provide a non-NULL value.

46503, object %s already exists

Cause: Object specified was already present in the system.

Action: Provide a different value.

46504, duplicate %s

Cause: Value was repeated in the input.

Action: Remove the duplicates.

46505, object %s does not exist

Cause: Object specified was not present in the system.

Action: Provide a different value.

46506, attribute %s exists in %s

Cause: Attribute specified was already present.

Action: Provide a different attribute.

46507, invalid data or type name for attribute %s

Cause: Data type of the value specified was different from the type name of the attribute.

Action: Change the type name or the type of the value for the attribute.

46508, too many attributes of type %s specified

Cause: Specified number of attributes of this type exceeded the maximum number supported.

Action: Specify fewer number of attributes of this type.

E.1.2 Source and Event Error Codes

This section describes the source and event error codes.

46521, NULL value passed for a mandatory attribute

Cause: A mandatory attribute was set to a NULL value.

Action: Provide a non-NULL value for the mandatory attribute.

46522, mandatory attribute %s missing in the input

Cause: Mandatory attribute name was missing in the attribute value list.

Action: Provide the value for mandatory attribute.

46523, attempting to drop Event Category with active Events

Cause: Event Category specified had active Events.

Action: Drop the active Events before dropping this Event Category.

46524, active Collectors exist for the Source

Cause: Source specified had Collectors which were active.

Action: Drop active Collectors for the given Source.

46525, Sourcetype-specific extension for Category already exists

Cause: Event Category was specified which already has a Format extension for the given Sourcetype.

Action: Provide an Event Category which does not have a Sourcetype-specific extension.

46526, attempting to drop an in-use Event mapping

Cause: Event mapping specified was in use.

Action: Provide an Event mapping that is not being used.

46527, attempting to change an immutable attribute

Cause: An immutable attribute was specified.

Action: Provide a mutable attribute.

46528, attempting to drop system-defined Event

Cause: Event specified was system-defined.

Action: Provide a user-defined Event.

46529, attempting to drop Event with active mappings

Cause: Event specified had active Event mappings.

Action: Drop the active mappings before dropping this Event.

46530, attempting to drop Sourcetype with active Sources

Cause: Sourcetype specified had active Sources.

Action: Drop the active Sources before dropping this Sourcetype.

46531, unsupported Source version

Cause: Version specified for the Source was not supported.

Action: Provide a Source version that is equal to or greater than the minimum supported version for the corresponding Sourcetype.

E.1.3 Collector Error Codes

This section describes the collector error codes.

46541, attempting to drop Collector Type with active Collectors

Cause: One or more Collectors for this Collector Type were active.

Action: Drop all active Collectors for this Collector Type.

46542, attempting to drop an Agent with active Collectors

Cause: One or more Collectors for this Agent were active.

Action: Drop all active Collectors for this Agent.

46543, attempting to drop a Collector before disabling the collection

Cause: The collection for the Collector specified was not disabled.

Action: Disable the collection before dropping the Collector.

46544, attempting to drop an Agent before disabling it

Cause: The Agent specified was not disabled.

Action: Disable the Agent before dropping it.

E.1.4 Attribute Definition Error Codes

This section describes the attribute definition error codes.

46551, attempting to change the type of an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46552, attempting to drop an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46553, attempting to change the type of an attribute without providing a new default value

Cause: Current type of the default value did not match with the new type specified.

Action: Provide a new default value for the attribute.

E.1.5 Alert Error Codes

This section describes the alert error codes.

46561, no Format defined for the Source Type and Category

Cause: Format for the specified Source Type and Category pair was not present in the system.

Action: Provide Source Type and Category pair which already has a Format defined.

46562, error in Alert condition

Cause: Invalid Alert condition was specified.

Action: Correct the Alert condition.

46563, attempting to drop a nonuser-defined Alert

Cause: Nonuser-defined Alert was specified.

Action: Provide a user-defined Alert.

46599, Internal error %s

Cause: Internal error occurred in Audit Vault.

Action: Contact Oracle Support Services.

E.1.6 Server-Side Audit Service Error Messages

This section describes the server-side audit service error codes.

46601, The authenticated user is not authorized with audit source

Cause: User is not authorized to send audit data on behalf of this audit source.

Action: Connect as the user who is associated with the source. Or grant this user appropriate authorization by changing the source's properties.

46602, Error on audit record insert as RADS partition full

Cause: RADS partition table is full.

Action: Purge the RADS partition table through archive.

46603, Error on audit record insert as RADS_INVALID table full

Cause: RADS_INVALID table is full.

Action: Need to purge RADS_INVALID table or make its size larger.

46604, Error on insert as Error table full

Cause: Error table is full.

Action: Need to purge the error table.

46605, There are more recovery entries than the maximum member can be returned

Cause: There are more recovery entries for this collector.

Action: Need to purge the old entries from the recovery table.

46606, There is no recovery entry for the given name

Cause: There was no recovery context matching to the given name.

Action: Need to check if the name was correct or if the recovery context was saved for this name.

46607, There are more configuration entries than the maximum member can be returned

Cause: There were more configuration entries for this collector.

Action: Need to reduce the configuration entries for this collector.

E.1.7 Data Warehouse Error Messages

This section describes messages from the data warehouse.

46620, invalid interval %s for data warehouse duration; must be positive

Cause: Invalid interval was specified for data warehouse duration.

Action: Specify valid interval, the interval should be positive.

46621, invalid start date %s for data warehouse operation; must be less than %s

Cause: Invalid start date was specified for data warehouse load/purge operation.

Action: Specify valid start date, the start date must be less than current date - warehouse duration.

46622, invalid number of days %s for data warehouse operation; must be greater than 0

Cause: Invalid number of days was specified for data warehouse load/purge operation.

Action: Specify valid number of days, the number of days must be positive

46623, cannot execute warehouse operation; another operation is currently running

Cause: A warehouse operation was executed while another operation is currently running.

Action: Wait for the operation to complete before reissuing the command.

46624, invalid schedule %s for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null schedule.

46625, invalid repeat interval %s for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null repeat interval.

46640, specified source name %s was not found

Cause: Invalid source name was specified.

Action: Specify a valid source name.

46641, archive does not exist

Cause: Invalid archive id was specified.

Action: Specify valid archive ID.

46642, database audit type invalid

Cause: Invalid database audit type specified.

Action: Database audit type must be S for standard or F for FGA.

46643, audit frequency invalid

Cause: Invalid audit frequency specified.

Action: Audit frequency must be A for "by access" or S for "by session".

46644, return type invalid

Cause: Return type was invalid.

Action: Return type must be S for "success", F for "failure", or B for "both".

46645, privilege flag invalid

Cause: Privilege flag is invalid.

Action: The privilege flag must be Y or N.

46646, specified Agent name %s was not found

Cause: Invalid Agent name was specified.

Action: Specify a valid Agent name.

E.2 Audit Vault Client Error Messages

This section describes the Oracle Audit Vault client error messages.

E.2.1 General Error Messages

This section describes the general error messages.

46800, Normal, successful completion

Cause: Normal exit.

Action: None.

46801, Out of memory

Cause: The process ran out of memory.

Action: Increase the amount of memory on the system.

E.2.2 CSDK Error Messages

This section describes the CSDK error messages.

46821, generic CSDK error (line %d)

Cause: There was a generic error in CSDK.

Action: Contact Oracle Support Services.

46822, no collector details for collector %s

Cause: Collector is not properly set up in AV tables.

Action: Configure collector.

46823, attribute %s is not valid for category

Cause: Collector attempted to set invalid attribute.

Action: Contact collector owner.

46824, type is not valid for attribute %s

Cause: Collector attempted to set value of wrong type to attribute.

Action: Contact collector owner.

46825, invalid record

Cause: Collector attempted to pass invalid record.

Action: Contact collector owner.

46826, invalid parameter %s (line %d)

Cause: Collector attempted to pass invalid parameter.

Action: Contact collector owner.

46827, invalid context

Cause: Collector attempted to pass invalid context.

Action: Contact collector owner.

46828, OCI layer error %d

Cause: OCI layer returned error.

Action: Contact collector owner.

46829, category %s unknown

Cause: Collector attempted to pass category not configured in AV.

Action: Contact collector owner.

46830, null pointer (line %d)

Cause: Collector attempted to pass null pointer.

Action: Contact collector owner.

46831, invalid source event id (%s)

Cause: Collector passed source event id not suitable for category.

Action: Contact collector owner.

46832, internal error (line %d)

Cause: Internal error occurred in CSDK.

Action: Contact Oracle Support Services.

46833, invalid error record

Cause: Collector attempted to pass invalid error record.

Action: Contact collector owner.

46834, missing attribute in error record

Cause: One or more attributes of error record is missing.

Action: Contact collector owner.

46835, duplicate error attribute

Cause: Collector attempted to set already set attribute.

Action: Contact collector owner.

46836, error record in use

Cause: Attempt to create a new error record before sending or dropping the previous one.

Action: Contact collector owner.

46837, missing eventid attribute in audit record

Cause: Eventid attributes of audit record is missing.

Action: Contact collector owner.

E.2.3 OSAUD Collector Error Messages

This section describes the OSAUD collector error messages.

46901, internal error, %s

Cause: There was a generic internal exception for OS Audit Collector.

Action: Contact Oracle Support Services.

46902, process could not be started, incorrect arguments

Cause: Wrong number of arguments or invalid syntax used.

Action: Please verify that all the required arguments are provided. The required arguments are Host name, Source name, Collector name, and the Command.

46903, process could not be started, operating system error

Cause: The process could not be spawned because of an operating system error.

Action: Please consult the log file for detailed operating system error.

46904, collector %s already running for source %s

Cause: Collector specified was already running.

Action: Provide a different collector or source name.

46905, collector %s for source %s does not exist

Cause: Collector specified was not running.

Action: Provide a different collector or source name.

46906, could not start collector %s for source %s, reached maximum limit

Cause: No more collectors could be started for the given source.

Action: None.

46907, could not start collector %s for source %s, configuration error

Cause: Some collector parameters were not configured correctly.

Action: Check the configuration parameters added during ADD_COLLECTOR.

46908, could not start collector %s for source %s, directory access error for %s

Cause: Access to specified directory was denied.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46909, could not start collector %s for source %s, internal error: [%s], [%d]

Cause: An internal error occurred while starting the collector.

Action: Contact Oracle Support Services.

46910, error processing collector %s for source %s, directory access error for %s

Cause: Access to specified directory was denied.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46911, error processing collector %s for source %s, internal error: [%s], [%d]

Cause: An internal error occurred while processing the collector.

Action: Contact Oracle Support Services.

46912, could not stop collector %s for source %s

Cause: An error occurred while closing the collector.

Action: None.

46913, error in recovery of collector %s for source %s: %s

Cause: An error occurred while accessing the file.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46914, error in recovery of collector %s for source %s, internal error: [%s], [%d]

Cause: An internal error occurred while getting recovery information for collector.

Action: Contact Oracle Support Services.

46915, error in parsing of collector %s for source %s: %s

Cause: An error occurred while accessing the file.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46916, error in parsing of collector %s for source %s, internal error [%s], [%d]

Cause: An internal error occurred while parsing data for collector.

Action: Contact Oracle Support Services.

46917, error processing request, collector not running

Cause: OS Audit Collector was not running and a command was issued.

Action: Start the collector using command START.

46918, could not process the command; invalid command

Cause: An invalid value was passed to the command argument.

Action: Please verify that a valid value is passed to command argument. The valid values are START, STOP and METRIC.

46919, error processing METRIC command; command is not in the required format

Cause: METRIC command was not in the required METRIC:XYZ format.

Action: Please verify that the metric passed is in METRIC:XYZ format where XYZ is the type of metric (Example: METRIC:ISALIVE).

46920, could not start collector %s for source %s, directory or file name %s is too long

Cause: The name of directory or file was too long.

Action: Verify the length of the path is less than the system-allowed limit.

46921, error processing collector %s for source %s, directory or file name %s is too long

Cause: The name of directory or file was too long.

Action: Verify the length of the path is less than the system-allowed limit.

46922, could not start collector %s for source %s, cannot open Windows event log

Cause: Windows event log could not be opened.

Action: Verify event log exists.

E.2.4 DBAUD Collector Error Messages

This section describes the DBAUD collector error messages.

46941, internal error, %d

Cause: There was a generic internal exception for AUD$ Audit Collector.

Action: Contact Oracle Support Services.

46942, invalid AUD Collector context

Cause: The AUD Collector context passed to collector was invalid.

Action: Be sure that the context that is passed is the context returned by zaac_start.

46943, NULL AUD Collector context

Cause: The pointer to AUD Collector context passed to Collector was NULL.

Action: Make sure that context passed is the context returned by zaac_start.

46944, conversion error

Cause: The VARCHAR retrieved from AUD$ or FGA_LOG$ table cannot be converted to ub4.

Action: Correct value in source database.

46945, bad recovery record

Cause: The recovery record retrieved from Audit Vault was damaged.

Action: None. The record will be corrected automatically.

46946, too many active sessions

Cause: The number of active sessions exceeds the specified number in the GV$PARAMETER table.

Action: Contact Oracle Support Services.

46947, CSDK layer error

Cause: CSDK layer returned error indication.

Action: Action should be specified in CSDK error report.

46948, already stopped

Cause: AUD collector already stopped because of previous fatal error.

Action: Restart the Collector.

46949, log level

Cause: Specified log level was invalid.

Action: Use a legal log level (1,2,3).

46950, log file

Cause: Error during opening of log file.

Action: Make sure that the log directory exists, and that the directory and log file are writable.

46951, bad value for AUD collector attribute

Cause: Specified collector attribute was invalid.

Action: Correct the attribute value in the Audit Vault table AV$ATTRVALUE.

46952, bad name for AUD collector metric

Cause: The specified metric name was undefined.

Action: Use a correct metric name.

46953, unsupported version

Cause: The specified version of the Source database is not supported.

Action: Update to supported version.

46954, recovery context of 10.x

Cause: Source database (9.x) was incompatible with 10.x recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46955, recovery context of 9.x

Cause: Source database (10.x) was incompatible with 9.x recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46956, FGA_LOG$ table of 9.x

Cause: Source database (10.x) was incompatible with 9.x rows of FGA_LOG$.

Action: Clean up FGA_LOG$ table.

46957, RAC recovery context

Cause: Non-RAC source database was incompatible with RAC recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46958, Non-RAC recovery context

Cause: RAC source database was incompatible with Non RAC recovery context

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46959, bad authentication information

Cause: Incorrect format of authentication information in the column COMMENT$TEXT.

Action: Contact Oracle Support Services.

Glossary

agent

A process within which collectors run. An agent sets up the connection between the collector and the audit service and interacts with the management service to manage and monitor collectors. An example of an agent is the Oracle agent within which run the collectors for Oracle Database OS audit logs (OSAUD), Oracle Database DB audit logs (DBAUD), and Oracle Database redo logs (REDO).

alert

An indicator signifying that a particular metric condition has been encountered. An alert is triggered when one of the following conditions is true:

- A metric threshold is reached.
- The availability of a monitored service changes. For example, the availability of the host changes from up to down.
- A metric-specific condition occurs. For example, an alert is triggered whenever an error message is written to a database alert log file.

alert rule

A rule in an audit policy setting that specifies an audit condition or other abnormal condition that causes an alert to be raised. An alert rule is based on the data in a single audit record.

audit data source

The database instance running on a computer. Because multiple instances of databases can run on the same computer, there may be multiple sources.

The audit data source consists of databases, applications, or systems that generate audit data. For the current release of Oracle Audit Vault, audit data sources are Oracle Database instances running on the same computer, giving rise to multiple sources on that system. Audit data from audit sources represents a variety of audit formats. Each audit source is categorized by its source type, which represents a class of audit sources. For example, audit sources with the same audit formats, audit events, and collection mechanisms represent an audit source type and will have a DBAUD collector, an OSAUD collector, and a REDO collector. All Oracle Database 10*g* sources must have these collectors.

See also **DBAUD collector**; **OSAUD collector**; and **REDO collector**.

audit data warehouse

A data store that stores within Audit Vault a translated or processed set of audit data from the raw audit data store that is of interest to audit administrators for data analysis and from which administrative and custom reports can be generated.

See also **data warehouse**.

audit rule

A rule in a audit setting that specifies the action to be audited, for example, a logon attempt or a user accessing a table.

audit setting

A set of rules that specifies what audit events should be collected in Audit Vault, and how each audit event should be evaluated after it is inserted into the raw audit data store. The types of rules in an audit setting include alert rules, audit rules, and capture rules. An audit setting can be composed of two or more sets of rules known as a composite audit setting.

See also **alert rule**; **audit rule**; and **capture rule**.

Audit Vault administrator user

A user granted the AV_ADMIN role. This user configures and manages collectors, agents, and warehouse settings and scheduling. This user also configures sources, enables and disables systemwide alerts, views audit event categories, and monitors audit errors.

Audit Vault agent user

A user granted the AV_AGENT role. This user is created prior to an Audit Vault Agent installation. This user must be created before an agent is added to Audit Vault and before an agent is initialized.

Audit Vault archive user

A user granted the AV_ARCHIVER role. This is an internal user role used to run back-end archiving jobs.

Audit Vault auditor user

A user granted the AV_AUDITOR role. This user monitors audit event categories for alert activity to detect security risks, creates detail and summary reports of events across systems, and manages the reports. This user also manages audit policies that include creating alerts and evaluating alert scenarios, and managing audit settings. This user can use the data warehouse services to further analyze the audit data to assist in looking for trends, intrusions, anomalies, and other items of interest.

Audit Vault Configuration Assistant (AVCA)

See **AVCA**.

Audit Vault Control (AVCTL)

See **AVCTL**.

Audit Vault Oracle Database (AVORCLDB)

See **AVORCLDB**.

Audit Vault source user

A user granted the AV_SOURCE role. This user must be created before a source and its collector can be registered (added) to Audit Vault. This user is used to connect to the source and to set up the source's collectors.

AVCA

Audit Vault Configuration Assistant. A command-line utility that enables the Audit Vault administrator to manage various Oracle Audit Vault components, manage agents (add/alter/drop), secure communication between the Audit Vault Server and Audit Vault Agent, set warehouse scheduling and audit data retention settings, and as needed create a wallet and certificates on the agent.

AVCTL

Audit Vault Control. A command-line utility that enables the Audit Vault administrator granted the AV_ADMIN role to manage Audit Vault components, such as agents (start/stop/show status), collectors (start/stop/show status), Audit Vault Console (start/stop), and Agent OC4J (start/stop).

AVORCLDB

Audit Vault Oracle Database. A command-line utility that provides the ability to configure sources (add/alter/drop), configure collectors (add/alter/drop), verify that the source is compatible with its collector, set up the database link from the source to the Audit Vault Agent, and verify the connection using the wallet.

capture rule

A rule in an audit policy setting that specifies an audit event that is sent to Audit Vault.

certificate

A digitally signed statement by a Certificate Authority (CA), saying that the identity of an entity is certified in some way. When an entity requests certification, the CA verifies its identity and grants a certificate, which is signed with the CA's private key. A digitally signed certificate is verified to have been checked for data integrity and authenticity, where integrity means that data has not been modified or tampered with, and authenticity means data indeed comes from the entity claiming to have created and signed it.

A digital identification of an entity that contains the following:

- SSL public key of the server
- Information about the server
- Expiration date
- Digital signature by the issuer of the certificate, used to verify the authenticity of the certificate

collector

A component that collects audit data for a source and sends the audit records to Audit Vault. Audit Vault uses the DBAUD collector, OSAUD collector for OS files, OSAUD collector for Windows event logs, and REDO collector to collect Oracle Database audit data.

See also **DBAUD collector**; **OSAUD collector**; and **REDO collector**.

composite audit setting

See **audit setting**.

configuration data

The Audit Vault metadata stored within Audit Vault that describes how to process and control the audit data as it passes through the Audit Vault system.

data warehouse

A relational database that is designed for query and analysis rather than transaction processing. A data warehouse usually contains historical data that is derived from transaction data, but it can include data from other sources. It separates analysis workload from transaction workload and enables a business to consolidate data from several sources.

See also **audit data warehouse**.

DBAUD collector

Oracle Database DB audit log collector. This collector converts SYS.AUD$ table rows into audit records. The DBAUD collector belongs to the ORCLDB_DBAUD collector type.

digital certificate

See certificate.

fact table

A table in a star schema that contains facts. A fact table typically has two types of columns: those that contain facts and those that are foreign keys to dimension tables. The primary key of a fact table is usually a composite key that is made up of all of its foreign keys.

A fact table might contain either detail level facts or facts that have been aggregated (fact tables that contain aggregated facts are often instead called summary tables). A fact table usually contains facts with the same level of aggregation.

Hypertext Transmission Protocol, Secure

See HTTPS.

HTTPS

Hypertext Transmission Protocol, Secure. The use of Secure Sockets Layer (SSL) as a sublayer under the regular HTTP application layer.

key store

A repository that includes the following:

- Certificates identifying trusted entities. When a key store contains only certificates of trusted entities, it can be called a trust store.
- Private-key and the matching certificate. This certificate is sent as a response to SSL authentication challenges.

keytool

A key and certificate management utility used by Audit Vault located at $ORACLE_HOME/jdk/bin/keytool for generating the key store. With a key store and certificate in place at the Audit Vault Agent, an Audit Vault administrator can issue an AVCA secure_av command on the Audit Vault Server to secure Audit Vault communications by enabling mutual authentication with the Audit Vault Agent. Likewise, an Audit Vault administrator can issue an AVCA secure_agent command to enable mutual authentication with Audit Vault Server. This utility enables users to self-authenticate by administering their own public/private key pairs and associated certificates or data integrity and authentication services, using digital signatures.

LCR

A logical change record. This is a message with a specific format that describes a database change.

logical change record (LCR)

See **LCR**.

mapping

The definition of the relationship and data flow between source and target objects.

metric

Unit of measurement used to report the health of the system.

Oracle Database DB audit logs collector (DBAUD)

See **DBAUD collector**.

Oracle Database OS audit logs collector (OSAUD)

See **OSAUD collector**.

Oracle Database redo logs collector (REDO)

See **REDO collector**.

OSAUD collector

Oracle Database OS audit log collector. This collector parses operating system (OS) log file entries into audit records. The OSAUD collector belongs to the ORCLDB_OSAUD collector type.

On Windows, the OS audit trail goes to the Windows event log. The OSAUD collector on Windows has a special mode called EVTLOG.

PKI

A public key infrastructure. This information security technology uses the principles of public key cryptography. Public key cryptography involves encrypting and decrypting information using a shared public and private key pair. It provides for secure, private communications within a private network.

public key infrastructure

See PKI.

raw audit data store

The sole repository of Audit Vault. It stores unprocessed audit data in partitioned tables based on time stamp, and in unpartitioned tables based on source ID.

REDO collector

Oracle Database redo log collector. This collector translates logical change records (LCRs) into audit records. The REDO collector belongs to the ORCLDB_REDO collector type.

secure audit warehouse

A data warehouse with greatly reduced Administrator user role access. It contains Audit Vault audit data for query and analysis.

silo

Traditionally, a tall, cylindrical tower used to store grain or fodder on a farm. In information management, a silo system is vertical, isolated, independent, and incapable of reciprocal operations with other, related management systems. The result of this independence and isolation is that multiple versions of the same data are stored.

star schema

A relational schema whose design represents a multidimensional data model. The star schema consists of one or more fact tables and one or more dimension tables that are related through foreign keys.

trust store

See key store.

X.509

A widely used standard for defining digital certificates. X.509 defines a standard certificate format for public key certificates and certificate validation.

Index