

Oracle® Audit Vault

Administrator's Guide

Release 10.2.3.2

E14459-12

February 2012

Oracle Audit Vault Administrator's Guide, Release 10.2.3.2

E14459-12

Copyright © 2007, 2012, Oracle and/or its affiliates. All rights reserved.

Primary Authors: Patricia Huey, Rodney Ward

Contributors: Tammy Bednar, Janet Blowney, Manish Chandra, Naveen Gopal, Raghavendran Hanumantharau, Srivatsan Kannan, K. Karun, Ravi Kumar, Valarie Moore, Dongwon Park, Dinesh Pathak, Anurag Prasad, Srividya Tata, Harm ten Napel, Vipul Shah, Prahlada Varadan Thirumalai, Lok Sheung

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xv
Audience	xv
Documentation Accessibility	xv
Related Documents	xv
Conventions	xvii
 What's New in Oracle Audit Vault for Administrators?	xix
Oracle Audit Vault Release 10.2.3.2 New Features	xix
Oracle Audit Vault Release 10.2.3.1 New Features	xxiv
 1 Introducing Oracle Audit Vault for Administrators	
1.1 How Do Administrators Use Oracle Audit Vault?	1-1
1.2 General Steps for Administering Oracle Audit Vault	1-2
1.2.1 Step 1: Understand the Oracle Audit Vault Architecture	1-2
1.2.2 Step 2: Plan the Oracle Audit Vault Source Database and Collector Configuration .	1-2
1.2.3 Step 3: Configure Collectors to Collect Audit Data	1-2
1.2.4 Step 4: Monitor and Maintain the Audit Record Collection Process	1-2
1.3 Components of Oracle Audit Vault	1-3
1.3.1 Source Databases	1-3
1.3.2 Oracle Audit Vault Server	1-4
1.3.2.1 General Oracle Audit Vault Server Components	1-4
1.3.2.2 Default Oracle Audit Vault Server Port Numbers.....	1-6
1.3.3 Oracle Database Vault.....	1-6
1.3.4 Audit Vault Collection Agent and Collectors.....	1-6
1.3.4.1 What Are Collection Agents and Collectors?.....	1-7
1.3.4.2 General Audit Vault Collection Agent and Collector Components	1-7
1.3.4.3 Default Audit Vault Collection Agent and Collector Port Numbers.....	1-8
1.3.5 How the Oracle Audit Vault Components Work Together	1-9
1.4 Administrative Tools for Managing Oracle Audit Vault.....	1-10
1.5 Default Oracle Audit Vault Roles.....	1-11
1.6 Planning the Source Database and Collector Configuration.....	1-12
1.6.1 About Planning the Source Database and Collector Configuration	1-12
1.6.2 Planning the Oracle Source Database and Collector Configuration	1-12
1.6.3 Planning the Microsoft SQL Server Source Database and Collector Configuration	1-14
1.6.4 Planning the Sybase ASE Source Database and Collector Configuration.....	1-15

1.6.5	Planning the IBM DB2 Source Database and Collector Configuration.....	1-16
-------	---	------

2 Registering Source Databases and Collectors

2.1	General Steps for Adding Sources and Deploying Collectors	2-1
2.2	Checking and Setting Environment Variables.....	2-2
2.2.1	About Checking and Setting Linux and UNIX Environment Variables.....	2-2
2.2.2	Setting the Audit Vault Server Linux and UNIX Environment Variables	2-2
2.2.3	Setting the Collection Agent Linux and UNIX Environment Variables	2-4
2.2.4	Using Oracle Audit Vault in a Microsoft Windows Environment	2-5
2.2.5	Setting the Oracle Source Database Linux and UNIX Environment Variables	2-5
2.3	Registering Oracle Database Sources and Collectors	2-5
2.3.1	Step 1: Create a User Account on the Oracle Source Database	2-5
2.3.2	Step 2: Verify That the Source Database Is Compatible with the Collectors	2-7
2.3.3	Step 3: Register the Oracle Source Database with Oracle Audit Vault	2-9
2.3.4	Step 4: Add the Oracle Collectors to Oracle Audit Vault	2-10
2.3.5	Step 5: Enable the Audit Vault Agent to Run the Oracle Database Collectors.....	2-13
2.4	Registering Microsoft SQL Server Database Sources and Collector	2-13
2.4.1	Step 1: Download the Microsoft SQL Server JDBC Driver	2-14
2.4.2	Step 2: Create a User Account on the Microsoft SQL Server Database Instance.....	2-14
2.4.3	Step 3: Verify That the Database Instance Is Compatible with the Collector	2-15
2.4.4	Step 4: Register the SQL Server Source Database Instance with Audit Vault	2-15
2.4.5	Step 5: Add the MSSQLDB Collector to Oracle Audit Vault.....	2-16
2.4.6	Step 6: Enable the Audit Vault Agent to Run the MSSQLDB Collector	2-17
2.4.7	Step 7: Optionally, Schedule an Audit Trail Cleanup for SQL Server Audit Files .	2-18
2.5	Registering Sybase ASE Database Sources and Collector.....	2-19
2.5.1	Step 1: Download the jConnect for JDBC Driver	2-19
2.5.2	Step 2: Create a User Account on the Sybase ASE Source Database.....	2-19
2.5.3	Step 3: Verify That the Source Database Is Compatible with the Collector	2-20
2.5.4	Step 4: Register the Sybase ASE Source Database with Oracle Audit Vault.....	2-20
2.5.5	Step 5: Add the SYBDB Collector to Oracle Audit Vault.....	2-21
2.5.6	Step 6: Enable the Audit Vault Agent to Run the SYBDB Collector.....	2-21
2.6	Registering IBM DB2 Database Sources and Collector	2-22
2.6.1	Step 1: Copy the DB2 JDBC and SQLJ Driver to the Audit Vault Homes.....	2-22
2.6.2	Step 2: Designate a User Account on the IBM DB2 Source Database	2-23
2.6.3	Step 3: Verify That the Source Database Is Compatible with the Collector	2-23
2.6.4	Step 4: Register the IBM DB2 Source Database with Oracle Audit Vault	2-23
2.6.5	Step 5: Add the DB2 Collector to Oracle Audit Vault	2-24
2.6.6	Step 6: Convert the Binary DB2 Audit File to an ASCII Text File.....	2-25
2.6.6.1	Step 6A: Complete the Preparation Steps	2-25
2.6.6.2	Step 6B: Run the Conversion Script	2-26
2.7	Starting the Collection Agents	2-27
2.7.1	Starting the Oracle Audit Vault Release 10.2.3.2 Collection Agents	2-28
2.7.2	Starting the Oracle Audit Vault Release 10.2.3.1 or Earlier Collection Agents	2-28
2.8	Starting the Collectors	2-28
2.8.1	Starting the Collectors from the Audit Vault Console	2-28
2.8.2	Starting the Collectors from the Audit Vault Server	2-29
2.9	Checking the Status of the Collectors	2-30

2.9.1	Checking the Status of Collectors from the Audit Vault Console	2-30
2.9.2	Checking the Status of Collectors from a Command Line	2-31
2.10	Checking If the Collectors Are Collecting Audit Records	2-31

3 Managing Oracle Audit Vault

3.1	About Managing Oracle Audit Vault	3-1
3.2	Managing the Audit Vault Server	3-1
3.2.1	About Managing the Audit Vault Console	3-1
3.2.2	Checking the Audit Vault Console Status	3-2
3.2.3	Starting and Logging into the Audit Vault Console.....	3-2
3.2.4	Stopping the Audit Vault Server Console.....	3-3
3.2.5	Globally Disabling and Enabling Alert Settings	3-3
3.2.6	Viewing Audit Event Categories.....	3-3
3.2.7	Viewing Operational Errors That Oracle Audit Vault Catches	3-5
3.3	Altering Collector Properties and Attributes.....	3-6
3.3.1	About Collector Properties and Attributes	3-6
3.3.2	Altering Collector Properties and Attributes Using the Audit Vault Console.....	3-6
3.3.3	Altering Collector Properties and Attributes from a Command Line	3-6
3.4	Managing the Oracle Audit Vault Data Warehouse.....	3-7
3.4.1	About Managing the Oracle Audit Vault Data Warehouse	3-8
3.4.2	Setting the Audit Vault Data Warehouse Retention Period	3-8
3.4.2.1	About Setting a Retention Period.....	3-8
3.4.2.2	Creating a Retention Period Using the Audit Vault Console	3-9
3.4.2.3	Creating a Retention Period from a Command Line.....	3-9
3.4.3	Loading Data to the Oracle Audit Vault Data Warehouse.....	3-10
3.4.3.1	About Loading Data into the Oracle Audit Vault Warehouse	3-10
3.4.3.2	Loading Data Warehouse Data Using the Audit Vault Console.....	3-10
3.4.3.3	Loading Data Warehouse Data from a Command Line	3-11
3.4.4	Purging Data from the Oracle Audit Vault Data Warehouse	3-11
3.4.4.1	About Purging the Oracle Audit Vault Data Warehouse.....	3-11
3.4.4.2	Purging Data Warehouse Data Using the Audit Vault Console	3-11
3.4.4.3	Purging Data Warehouse Data from a Command Line.....	3-12
3.5	Altering Source Database Attributes	3-12
3.5.1	About Source Database Attributes	3-12
3.5.2	Altering Source Database Attributes Using the Audit Vault Console.....	3-12
3.5.3	Altering Source Database Attributes from a Command Line	3-13
3.6	Configuring E-Mail Notifications.....	3-14
3.6.1	About E-Mail Notification Usage with Oracle Audit Vault	3-14
3.6.2	Configuring the E-Mail Notification Service	3-15
3.7	Configuring Oracle Audit Vault for the Remedy Trouble Ticket System.....	3-16
3.7.1	About Using the Remedy Trouble Ticket System with Oracle Audit Vault.....	3-16
3.7.2	Configuring the Remedy Trouble Ticket Server Connection.....	3-16
3.8	Removing Source Databases from Oracle Audit Vault.....	3-17
3.8.1	About Removing Source Databases from Oracle Audit Vault	3-17
3.8.2	Removing a Source Database Using the Audit Vault Console	3-18
3.8.3	Removing a Source Database from a Command Line	3-18

4 Administering the Oracle Audit Vault Repository

4.1	About the Administrative Tasks in This Chapter	4-1
4.2	Monitoring the Audit Vault Server SYSAUX Tablespace Space Usage.....	4-1
4.3	Monitoring Audit Vault Server Archive Log Disk Space Usage	4-2
4.4	Monitoring the Audit Vault Server Flash Recovery Area.....	4-2
4.5	Managing Oracle Audit Vault Backup and Recovery Operations	4-2
4.5.1	Backing Up the Database.....	4-3
4.5.2	Backing Up Audit Vault Server Home and Audit Vault Collection Agent Home	4-3
4.6	Managing the Audit Vault Console in an Oracle RAC Configuration	4-3
4.7	Using a Collection Agent to Listen to Oracle RAC Nodes	4-4
4.8	Configuring Collection Agent Connectivity for Oracle RAC.....	4-5
4.9	Changing the Port Numbers Used by Oracle Audit Vault.....	4-5
4.9.1	Changing Port Numbers for the Audit Vault Server	4-6
4.9.1.1	Changing the Audit Vault Server Listener Port Number.....	4-6
4.9.1.2	Changing the Audit Vault Console HTTP Port Number	4-8
4.9.1.3	Changing the Oracle Enterprise Manager Database Control Port Number	4-8
4.9.1.4	Changing the Audit Vault PL/SQL Gateway Port Number.....	4-9
4.9.2	Changing Port Numbers for the Audit Vault Collection Agents	4-9
4.9.2.1	Changing the Collection Agent HTTP Port Number	4-9
4.9.2.2	Changing the Collection Agent RMI and JMS Port Numbers	4-10
4.9.3	Changing Port Numbers for the Oracle Source Database	4-10
4.10	Purging the Oracle Source Database Audit Trail.....	4-11
4.10.1	About Purging the Oracle Source Database Audit Trail.....	4-11
4.10.2	Scheduling an Automated Purge Job for an Oracle Audit Vault Environment	4-12
4.11	Purging the Oracle Audit Vault Repository Audit Trail.....	4-13

5 Managing Oracle Audit Vault Security

5.1	About Managing Oracle Audit Vault Security.....	5-1
5.2	Managing Oracle Audit Vault User Accounts.....	5-1
5.3	Managing Authentication Metadata Using Oracle Advanced Security	5-3
5.4	Changing Oracle Audit Vault User Passwords on a Regular Basis	5-4
5.4.1	About Oracle Audit Vault User Passwords.....	5-4
5.4.2	Changing the AV_ADMIN User Password.....	5-5
5.4.3	Changing the AVREPORTUSER Password.....	5-6
5.4.4	Changing the AV_AGENT Password.....	5-6
5.4.5	Changing the Source User Password.....	5-7
5.4.6	Changing the AV_AUDITOR Password.....	5-9
5.4.7	Ensuring That All Changed User Name Passwords Work Correctly	5-9
5.5	Using Oracle Database Vault within Oracle Audit Vault.....	5-10
5.6	Configuring HTTPS and SSL Communication for Oracle Audit Vault.....	5-11
5.6.1	About Configuring HTTPS and SSL Communication for Oracle Audit Vault	5-11
5.6.2	Step 1: Generate the Keystore	5-12
5.6.3	Step 2: Create an Audit Vault Agent Keystore by Using the keytool Utility.....	5-14
5.6.4	Step 3: Secure the XDB Services.....	5-17
5.6.5	Step 4: Secure Audit Vault Server	5-18
5.6.6	Step 5: Secure Audit Vault Agent.....	5-18
5.7	Updating XDB Certificates	5-19

6 Audit Vault Configuration Assistant (AVCA) Reference

6.1	add_agent	6-3
6.2	alter_remedy	6-4
6.3	alter_smtp.....	6-4
6.4	create_credential	6-6
6.5	create_wallet	6-7
6.6	deploy_av	6-7
6.7	disable_remedy	6-9
6.8	disable_smtp	6-9
6.9	drop_agent.....	6-10
6.10	enable_remedy	6-10
6.11	enable_smtp	6-11
6.12	generate_csr	6-12
6.13	-help	6-13
6.14	import_cert.....	6-15
6.15	redeploy.....	6-16
6.16	register_remedy	6-17
6.17	register_smtp	6-18
6.18	remove_cert.....	6-19
6.19	secure_agent	6-20
6.20	secure_av	6-21
6.21	secure_remedy.....	6-23
6.22	secure_smtp	6-23
6.23	set_server_tz	6-24
6.24	set_warehouse_retention	6-25
6.25	show_remedy_config	6-26
6.26	show_server_tz.....	6-27
6.27	show_smtp_config	6-27
6.28	test_remedy.....	6-28
6.29	test_smtp	6-29

7 Audit Vault Control (AVCTL) Reference

7.1	-help	7-2
7.2	load_warehouse	7-4
7.3	purge_warehouse.....	7-5
7.4	show_agent_status.....	7-6
7.5	show_av_status	7-7
7.6	show_collector_status	7-7
7.7	show_remedy_status.....	7-8
7.8	show_smtp_status.....	7-9
7.9	start_agent.....	7-9
7.10	start_av	7-10
7.11	start_collector.....	7-11
7.12	stop_agent	7-12
7.13	stop_av.....	7-13
7.14	stop_collector.....	7-13

7.15	AVCTL Commands Used for Release 10.2.3.1 Collection Agents	7-14
7.15.1	show_oc4j_status	7-14
7.15.2	start_oc4j	7-15
7.15.3	stop_oc4j.....	7-17

8 Audit Vault Oracle Database (AVORCLDB) Utility Commands

8.1	avorcldb.....	8-2
8.2	add_collector.....	8-2
8.3	add_source.....	8-5
8.4	alter_collector	8-6
8.5	alter_source	8-10
8.6	drop_collector.....	8-11
8.7	drop_source	8-12
8.8	-help	8-13
8.9	setup.....	8-14
8.10	verify	8-15

9 Audit Vault SQL Server (AVMSSQLDB) Utility Commands

9.1	avmssqldb	9-2
9.2	add_collector.....	9-2
9.3	add_source.....	9-3
9.4	alter_collector	9-4
9.5	alter_source	9-8
9.6	drop_collector.....	9-9
9.7	drop_source	9-10
9.8	-help	9-10
9.9	setup	9-11
9.10	verify	9-12

10 Audit Vault Sybase ASE (AVSYBDB) Utility Commands

10.1	avsybdb	10-2
10.2	add_collector.....	10-2
10.3	add_source.....	10-3
10.4	alter_collector	10-4
10.5	alter_source	10-6
10.6	drop_collector.....	10-7
10.7	drop_source	10-8
10.8	-help	10-9
10.9	setup.....	10-10
10.10	verify	10-11

11 Audit Vault IBM DB2 (AVDB2DB) Utility Commands

11.1	avdb2db.....	11-1
11.2	add_collector.....	11-2
11.3	add_source.....	11-3
11.4	alter_collector	11-4

11.5	alter_source	11-5
11.6	drop_collector	11-6
11.7	drop_source	11-7
11.8	-help	11-8
11.9	verify	11-9

12 REDO Collector Database Reference

12.1	About the Recommended Settings for the REDO Collector	12-1
12.2	Recommended Oracle Streams Supplemental Logging	12-1
12.3	Oracle Database 11g Release 2 (11.2) Audit Source Parameter Recommendations	12-2
12.4	Oracle Database 11g Release 1 (11.1) Audit Source Parameter Recommendations	12-6
12.5	Oracle Database 10g Release 2 (10.2) Audit Source Parameter Recommendations	12-10
12.6	Oracle Database 10g Release 1 (10.1) Audit Source Parameter Recommendations	12-14
12.7	Oracle9i Database Release 2 (9.2) Audit Source Parameter Recommendations	12-18

A Troubleshooting an Oracle Audit Vault System

A.1	Location of Audit Vault Server Log and Error Files	A-1
A.2	Location of Audit Vault Collection Agent Log and Error Files	A-3
A.3	Troubleshooting Tips	A-6
A.3.1	Checking Trace Files for Detailed Information About Oracle Database Errors	A-6
A.3.2	Troubleshooting Audit Vault Server	A-6
A.3.2.1	Tuning Audit Vault Server Performance for the REDO Collector	A-6
A.3.3	Troubleshooting Audit Vault Collection Agent	A-7
A.3.3.1	Blank Status on Windows Services Panel for Audit Vault Agent	A-7
A.3.3.2	Debugging a Collection Agent Problem	A-7
A.3.3.3	The Agent OC4J or Audit Vault Console OC4J Failing to Start	A-8
A.3.3.4	Failed Source Database Connection Due to Invalid Wallet Credentials	A-9
A.3.4	Troubleshooting the Audit Vault Collectors	A-9
A.3.4.1	ORA-01031 Error When You Try to Create a an Oracle Database Collector	A-9
A.3.4.2	Oracle Source Database DBAUD Log Errors When Starting DBAUD Collector	A-10
A.3.4.3	DBAUD Collector Does Not Start and the Listener Is Not Available	A-11
A.3.4.4	Not Sure if the DBAUD and OSAUD Collectors Are Working	A-11
A.3.4.5	ORA-01017 Error When You Try to Start the DBAUD or REDO Collectors	A-12
A.3.4.6	MSSQLDB, SYBDB, or DB2 Collector Log Indicates Jar File Is Missing	A-12
A.3.4.7	Collector Unable to Connect to the Source Database	A-13
A.3.4.8	Failure of the Computer on Which a Collector Resides	A-13
A.3.4.9	DB2 Collector Connection Being Denied Due to Lack of License	A-13
A.3.5	Troubleshooting Oracle Audit Vault Console	A-14
A.3.5.1	Audit Vault Console Not Appearing in the Web Browser	A-14
A.3.5.2	Audit Vault Console Problem Requiring Debugging	A-14
A.3.5.3	Oracle RAC Node Containing the Audit Vault Console Becomes Disabled ...	A-14
A.3.6	Troubleshooting the Oracle Audit Vault Audit Reports	A-15
A.3.6.1	Oracle Audit Vault Reports Not Displaying	A-15
A.3.6.2	Oracle Audit Vault Reports Not Showing Any Data	A-16
A.3.6.3	Not Sure if Audit Data Is Appearing in the Data Warehouse	A-16

A.3.6.4	Advanced Alerts Unable to Fire and New Alerts Cannot Be Created	A-16
A.3.7	Troubleshooting Oracle Audit Vault in an Oracle Real Application Clusters Environment A-17	
A.3.7.1	avca drop_agent Command Failing.....	A-17

B Oracle Audit Vault Error Messages

B.1	Audit Vault Server Error Messages.....	B-1
B.1.1	Generic Error Codes	B-1
B.1.2	Source Database and Event Error Codes.....	B-2
B.1.3	Collector Error Codes.....	B-3
B.1.4	Attribute Definition Error Codes.....	B-4
B.1.5	Alert Error Codes.....	B-4
B.1.6	Server-Side Audit Service Error Messages.....	B-5
B.1.7	Data Warehouse Error Messages.....	B-6
B.1.8	Other Audit Vault Policy Error Messages.....	B-7
B.2	Oracle Audit Vault Client Error Messages.....	B-8
B.2.1	General Error Messages	B-8
B.2.2	CSDK Error Messages	B-8
B.2.3	Command-Line Interface Error Messages	B-10
B.2.4	OSAUD Collector Error Messages	B-12
B.2.5	DBAUD Collector Error Messages	B-14

Glossary

Index

List of Examples

2-1	Partially Successful Verify Operation of Source Compatibility with the Collectors	2-8
2-2	Successful Verify Operation of Source Compatibility with the REDO Collector	2-9
2-3	Adding the OSAUD Collector to Oracle Audit Vault for UNIX Platforms.....	2-11
2-4	Adding the OSAUD Collector to Oracle Audit Vault on Microsoft Windows.....	2-12
2-5	Adding the DBAUD Collector to Oracle Audit Vault	2-12
2-6	Adding the REDO Collector to Oracle Audit Vault	2-12

List of Figures

1-1	Overview of the Oracle Audit Vault Components	1-9
3-1	Audit Event Category Management Page.....	3-4
3-2	Audit Errors Page	3-5

List of Tables

1-1	Supported Source Database Products.....	1-3
1-2	Oracle Audit Vault Server Components.....	1-5
1-3	Oracle Audit Vault Server Ports	1-6
1-4	Oracle Audit Vault Collection Agent Components	1-7
1-5	Oracle Audit Vault Collector Types and Audit Trails.....	1-8
1-6	Oracle Audit Vault Agent Ports.....	1-8
1-7	Oracle Audit Vault Administrator Roles and Their Assigned Tasks.....	1-11
1-8	Oracle Database Operating System Audit Settings for the OSAUD Collector	1-13
1-9	Oracle Database Audit Trail Settings for the DBAUD Collector	1-13
1-10	Oracle Database Redo Log Setting for the REDO Collector	1-14
1-11	Microsoft SQL Server Source Database Audit Settings for the MSSQLDB Collector ...	1-15
1-12	Sybase ASE Database Audit Setting for the SYBDB Collector	1-15
1-13	IBM DB2 Database Audit Setting for the DB2DB Collector.....	1-16
2-1	Audit Vault Server Environment Variable Settings.....	2-2
5-1	Storage Location of Audit Vault and Source User Name Passwords	5-4
5-2	Roles and Privileges Granted to Audit Vault or Database Vault Administrators	5-10
5-3	Database Core Accounts Created and Privileges Use	5-11
6-1	Audit Vault Configuration Assistant Commands	6-1
7-1	Audit Vault Control Commands for Release 10.2.3.2.....	7-1
7-2	Audit Vault Control Commands for Release 10.2.3.1.....	7-14
8-1	AVORCLDB Commands	8-1
8-2	DBAUD Collector Attributes	8-7
8-3	OSAUD Collector Attributes.....	8-8
8-4	REDO Collector Attributes	8-9
8-5	Source Attributes	8-11
9-1	AVMSSQLDB Commands.....	9-1
9-2	MSSQLDB Collector Attributes	9-6
9-3	Source Attributes	9-8
10-1	AVSYBDB Commands	10-1
10-2	SYBDB Collector Attributes.....	10-5
10-3	Source Attributes	10-7
11-1	AVDB2DB Commands.....	11-1
11-2	DB2 Collector Attributes.....	11-5
11-3	Source Attributes	11-6
12-1	Initialization Parameters to Be Configured for the 11.2 Source Database.....	12-2
12-2	Hidden Initialization Parameters to Be Configured for the 11.1 Source Database	12-6
12-3	Initialization Parameters to Be Configured for the 11.1 Source Database.....	12-6
12-4	Hidden Initialization Parameters to Be Configured for the 10.2 Source Database	12-10
12-5	Initialization Parameters to Be Configured for the 10.2 Source Database.....	12-10
12-6	Hidden Initialization Parameters to Be Configured for the 10.1 Source Database	12-14
12-7	Initialization Parameters to Be Configured for the 10.1 Source Database.....	12-14
12-8	Hidden Initialization Parameters to Be Configured for the 9.2 Source Database	12-18
12-9	Initialization Parameters to Be Configured for the 9.2 Source Database.....	12-18
12-10	ARCHIVE_LAG_TARGET Recommended Setting.....	12-20
A-1	Names and Descriptions of Audit Vault Server Log and Error Files.....	A-1
A-2	Names and Descriptions of Audit Vault Collection Agent Log and Error Files	A-3

Preface

Oracle Audit Vault Administrator's Guide explains how Oracle Audit Vault administrators can perform administrative tasks on an Oracle Audit Vault system. This guide assumes that you have completed the installation tasks covered in *Oracle Audit Vault Server Installation Guide* and *Oracle Audit Vault Collection Agent Installation Guide*.

This preface contains:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This document is intended for anyone who is responsible for administering an Oracle Audit Vault system.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the following documents. See also the platform-specific Oracle Audit Vault Server installation guides.

- *Oracle Audit Vault Patch Set Release Notes*
- *Oracle Audit Vault Server Installation Guide for Linux x86*
- *Oracle Audit Vault Collection Agent Installation Guide*

- *Oracle Audit Vault Licensing Information*
- *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*

Oracle Documentation Search Engine

To access the database documentation search engine directly, visit:

<http://tahiti.oracle.com/>

Oracle Technology Network (OTN)

You can download free release notes, installation documentation, updated versions of this guide, white papers, or other collateral from the Oracle Technology Network (OTN). Visit

<http://www.oracle.com/technetwork/index.html>

For security-specific information on OTN, visit

<http://www.oracle.com/technetwork/topics/security/whatsnew/index.html>

For the latest version of the Oracle documentation, including this guide, visit

<http://www.oracle.com/technetwork/documentation/index.html>

Oracle Audit Vault-Specific Sites

For OTN information specific to Oracle Audit Vault, visit

<http://www.oracle.com/technetwork/database/audit-vault/overview/index.html>

For the Oracle Audit Vault Discussion Forums, visit

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

Oracle Store

Printed documentation is available for sale in the Oracle Store at:

<https://shop.oracle.com>

My Oracle Support (formerly Oracle*MetaLink*)

You can find information about security patches, certifications, and the support knowledge base by visiting My Oracle Support at:

<https://support.oracle.com>

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Audit Vault for Administrators?

This section describes new features in Oracle Audit Vault that affect administrators, and provides pointers to additional information. These new features reflect changes since Release 10.2.3.1.

This section contains:

- [Oracle Audit Vault Release 10.2.3.2 New Features](#)
- [Oracle Audit Vault Release 10.2.3.1 New Features](#)

Oracle Audit Vault Release 10.2.3.2 New Features

This section contains:

- [E-Mail Notifications for Oracle Audit Vault Alerts](#)
- [Trouble Ticket Integration](#)
- [Real-Time Oracle Audit Vault Data Warehouse Refreshes](#)
- [Changes to Audit Trail Cleanup](#)
- [Time Zone Configuration for Oracle Audit Vault Reports and Alerts](#)
- [Failover Recovery for Collectors](#)
- [Changes to Server-Side Oracle Audit Vault Utilities](#)
- [Changes to Oracle Audit Vault Collection Agent Utilities](#)
- [Updated Oracle Database Release for the Oracle Audit Vault Server](#)
- [Information About Checking and Modifying Port Numbers](#)

E-Mail Notifications for Oracle Audit Vault Alerts

In this release of Oracle Audit Vault, auditors can configure e-mail notifications in response to Audit Vault alerts. For example, if an alert is triggered, an e-mail can be sent automatically to the persons who must respond to it. Before an auditor can create e-mail notifications, you must configure an SMTP server for the outgoing e-mail.

For more information, see [Section 3.6](#).

Trouble Ticket Integration

Oracle Audit Vault can now generate a Remedy trouble ticket in response to an Audit Vault alert. To accomplish this, you must configure the Audit Vault Server to

communicate with the BMC Remedy Action Request (AR) System Server 7.x that is responsible for managing the trouble tickets. After you complete this configuration, an Audit Vault auditor can create the conditions necessary to automatically trigger the trouble ticket creation.

For more information, see [Section 3.7](#).

Real-Time Oracle Audit Vault Data Warehouse Refreshes

Starting with this release, the Oracle Audit Vault data warehouse is automatically refreshed with incoming audit data as it collects audit data. Because the warehouse is refreshed in real-time, auditors can generate more accurate reports on audited activities.

Because of this enhancement, the `avctl refresh_warehouse` and `avca set_warehouse_schedule` commands are deprecated.

Note: If you have just upgraded to the current release of Oracle Audit Vault, be aware that the upgrade process removes any warehouse job refresh settings that you had created before the upgrade.

See [Section 3.4](#) for more information about managing the data warehouse.

Changes to Audit Trail Cleanup

This section contains:

- [Audit Trail Cleanup DBMS_AUDIT_MGMT PL/SQL Package Installed](#)
- [Audit Trail Cleanup Initialized on the Audit Vault Server](#)
- [Audit Trail Cleanup Default Purge Job for the Audit Vault Server Database](#)
- [Audit Trail Cleanup for Microsoft SQL Server Source Database Audit Data](#)
- [Audit Trail Cleanup for IBM DB2 Source Database Audit Data](#)

Audit Trail Cleanup DBMS_AUDIT_MGMT PL/SQL Package Installed

By default, the DBMS_AUDIT_MGMT PL/SQL package is installed in the Oracle Audit Vault Server. You no longer need to download this package from My Oracle Support (formerly OracleMetaLink) if you want to automatically purge the Audit Vault Server audit trail.

See [Section 4.10](#) for more information about purging the Audit Vault Server audit trail.

Audit Trail Cleanup Initialized on the Audit Vault Server

Starting with this release, the audit trail cleanup process is initialized from the Audit Vault Server, so that you can manage the Audit Vault Server database audit trail. As part of this change, the SYS.AUD\$ and SYS.FGA_LOG\$ tables are moved from the SYSTEM to the SYSAUX tablespace.

See [Section 4.10](#) for more information about purging the Audit Vault Server audit trail.

Audit Trail Cleanup Default Purge Job for the Audit Vault Server Database

By default, the audit trail generated by the Audit Vault Server is now purged every 24 hours. You can modify or remove the cleanup operation if you want.

See [Section 4.11](#) for more information purging the Audit Vault Server database audit trail.

Audit Trail Cleanup for Microsoft SQL Server Source Database Audit Data

You now can purge the C2 audit trace files and server-side trace files from a SQL Server source database automatically after all audit data has been collected by Audit Vault.

See [Section 2.4.7](#) for more information.

Audit Trail Cleanup for IBM DB2 Source Database Audit Data

Before Oracle Audit Vault can collect audit records from an IBM DB2 source database, you must run the `DB282ExtractionUtil` or `DB295ExtractionUtil` script. These scripts convert the IBM DB2 audit file from a binary to an ASCII file format. Starting with this release, these scripts support automatic cleanup of the binary audit trail data, in addition to purging ASCII-formatted data.

See [Section 2.6.6](#) for more information.

Time Zone Configuration for Oracle Audit Vault Reports and Alerts

Starting with this release, you can set the time zone format for Oracle Audit Vault reports and alerts. This enables auditors to generate reports that are timestamped using their local times. In addition, alert notifications and Remedy trouble tickets can contain local times. To accomplish this, you use the `avca set_server_tz` command. To find the status of the current time zone setting, you can run the `avca show_server_tz` command.

See the following sections for more information:

- [Section 6.23](#) for `avca set_server_tz`
- [Section 6.26](#) for `avca show_server_tz`

Failover Recovery for Collectors

Depending on the audit trail type, you can now configure the Oracle Database, Microsoft SQL Server, and Sybase ASE source databases to move the collector from one agent to another. This feature is useful for failover recovery if the host computer running the original agent fails. To accomplish this, you configure the agent for the collector by setting its `AGENTNAME` property by using the `avorclpdb`, `avmssqldb`, `avsybdb alter_collector` commands.

See the following sections for more information:

- **Oracle Database source databases.** This feature applies to the `DBAUD` collector only. See [Section 8.4](#) for more information about the `avorclpdb alter_collector` command.
- **Microsoft SQL Server source databases.** This feature applies to server-side trace files only. See [Section 9.4](#) for more information about the `avmssqldb alter_collector` command.
- **Sybase ASE source databases.** See [Section 10.4](#) for more information about the `avsybdb alter_collector` command.

Changes to Server-Side Oracle Audit Vault Utilities

This section contains:

- [New Oracle or Changed Audit Vault Utility Commands](#)
- [Deprecated Oracle Audit Vault Utility Commands](#)

New Oracle or Changed Audit Vault Utility Commands

The following utilities have been enhanced for this release:

- **Audit Vault Configuration Assistant (AVCA).** AVCA now has several new commands.

Commands used to configure e-mail notifications:

- register_smtp
- secure_smtp
- test_smtp
- show_smtp_config
- alter_smtp
- enable_smtp
- disable_smtp

Commands used to configure the Remedy trouble ticket service:

- register_remedy
- secure_remedy
- test_remedy
- show_remedy_config
- alter_remedy
- enable_remedy
- disable_remedy

Commands used to configure time zones for reports:

- set_server_tz
- show_server_tz

See [Chapter 6, "Audit Vault Configuration Assistant \(AVCA\) Reference"](#) for more information.

- **Audit Vault Control (AVCTL).** AVCTL now has the following new commands:
 - show_smtp_status
 - show_remedy_status

See [Chapter 7, "Audit Vault Control \(AVCTL\) Reference"](#) for more information.

- **Audit Vault Oracle Database (AVORCLDB).** AVORCLDB has a new attribute for the alter_collector command: AGENTNAME. See [Section 8.4](#) for more information about the avorcldb alter_collector command.
- **Audit Vault Microsoft SQL Server (AVMSSQLDB).** AVMSSQLDB has the following changes for these commands:

- `add_source` and `verify`: In previous releases, you specified the source database through the host name and port number. Now, you can specify the source database connection information by using one of the following formats:

```
myhost:myport
'myhost\myinstance'
```

The ability to specify the port or the instance name is useful for configurations in which the instance is not on the default port or does not have a default name. For configurations with multiple instances on one server, you *must* specify the host and instance name.

See [Section 9.3](#) for information about `avmssqldb add_source` and [Section 9.10](#) for information about `avmssqldb verify`.

- `alter_collector`: There is now a new attribute for the `alter_collector` command: `AGENTNAME`. See [Section 9.4](#) for more information about the `avmssqldb alter_collector` command.
- **Audit Vault Sybase ASE (AVSYBDB)**. AVSYBDB has a new attribute for the `alter_collector` command: `AGENTNAME`. See [Section 10.4](#) for more information about the `avsybdb alter_collector` command.

Deprecated Oracle Audit Vault Utility Commands

The following commands have been deprecated on the Audit Vault Server:

- `avca set_warehouse_schedule`
- `avctl refresh_warehouse`
- `avctl show_agent_status`
- `avctl start_agent`
- `avctl stop_agent`

See ["Real-Time Oracle Audit Vault Data Warehouse Refreshes"](#) on page xx for more information about enhancements to the data warehouse refresh feature.

Changes to Oracle Audit Vault Collection Agent Utilities

The following Oracle Audit Vault collection agent commands names have changed:

Previous Name	New name
<code>avctl show_oc4j_status</code>	<code>avctl show_agent_status</code> ¹
<code>avctl start_oc4j</code>	<code>avctl start_agent</code>
<code>avctl stop_oc4j</code>	<code>avctl stop_agent</code>

¹ In addition, starting with this release, the `avctl show_agent_status` command no longer has any arguments.

See [Chapter 7, "Audit Vault Control \(AVCTL\) Reference"](#) for more information about the AVCTL commands.

Updated Oracle Database Release for the Oracle Audit Vault Server

For this release, the Oracle Audit Vault Server uses Oracle Database Release 10.2.0.4.

See [Section 1.3.2](#) for more information about the Audit Vault Server components.

Information About Checking and Modifying Port Numbers

This guide now explains how you can check which ports are being used by an Oracle Audit Vault installation, and to modify them.

See the following sections for more information:

- [Section 1.3.2.2](#) for default Audit Vault Server port information
- [Section 1.3.4.3](#) for default Audit Vault collection agent and collector port information
- [Section 4.9](#) for information about changing port numbers

Oracle Audit Vault Release 10.2.3.1 New Features

This section contains:

- [Collectors for Sybase ASE and IBM DB2 Databases](#)

Collectors for Sybase ASE and IBM DB2 Databases

This release provides collectors for the Sybase Adaptive Server Enterprise (ASE) and IBM DB2 database products. The supported releases for these two database products are as follows:

- **Sybase ASE:** ASE 12.5.4 and ASE 15.0.2 on platforms based on Linux and UNIX, and on Microsoft Windows platforms
- **IBM DB2:** IBM DB2 Version 8.2 and Version 9.5 on platforms based on Linux and UNIX, and on Microsoft Windows platforms. If you are using Version 8.2, ensure that you have installed Fixpack 16.

See the following sections for more information:

- [Section 2.5](#) for information about registering a Sybase ASE source database with Oracle Audit Vault
- [Section 2.6](#) for information about registering an IBM DB2 source database with Oracle Audit Vault
- [Chapter 10, "Audit Vault Sybase ASE \(AVSYBDB\) Utility Commands"](#)
- [Chapter 11, "Audit Vault IBM DB2 \(AVDB2DB\) Utility Commands"](#)

Introducing Oracle Audit Vault for Administrators

This chapter contains:

- [How Do Administrators Use Oracle Audit Vault?](#)
- [General Steps for Administering Oracle Audit Vault](#)
- [Components of Oracle Audit Vault](#)
- [Administrative Tools for Managing Oracle Audit Vault](#)
- [Default Oracle Audit Vault Roles](#)
- [Planning the Source Database and Collector Configuration](#)

1.1 How Do Administrators Use Oracle Audit Vault?

By the time you begin to use this guide, you will have installed the Oracle Audit Vault Server and the Oracle Audit Vault collection agent, to prepare for the collection of audit data from your databases (called [source databases](#), or [audit data sources](#)). This guide explains how to configure the source databases so that Oracle Audit Vault can collect their audit data. After you have completed this configuration, then auditors can generate and customize reports that describe this audit data.

An Oracle Audit Vault administrator is responsible for the following tasks:

- Ensuring that the source databases have auditing enabled
- Understanding the type of auditing that each source database uses
- Selecting the correct Oracle Audit Vault component, called a [collector](#), to connect to the source database, based on the type of auditing that database uses
- Configuring this collector to connect Oracle Audit Vault to the source database
- Configuring and scheduling Audit Vault Server processes
- Ensuring that the collectors are collecting audit data from the source database
- Managing the day-to-day activities of Oracle Audit Vault, such as disk space usage and backup and recovery operations
- Managing security for Oracle Audit Vault
- Monitoring Oracle Audit Vault to ensure that it is consistently collecting audit data

Oracle Database administrators are responsible for running the Oracle Database audit trail cleanup procedures on the source database, which purge audit trail records from the Oracle source database after these records are archived.

1.2 General Steps for Administering Oracle Audit Vault

To administer Oracle Audit Vault, follow these steps:

- [Step 1: Understand the Oracle Audit Vault Architecture](#)
- [Step 2: Plan the Oracle Audit Vault Source Database and Collector Configuration](#)
- [Step 3: Configure Collectors to Collect Audit Data](#)
- [Step 4: Monitor and Maintain the Audit Record Collection Process](#)

1.2.1 Step 1: Understand the Oracle Audit Vault Architecture

In this chapter, [Section 1.3](#) describes the main components of Oracle Audit Vault, and explains how these components work together. [Section 1.4](#) describes the various tools that you use to administer Oracle Audit Vault. [Section 1.5](#) describes the predefined roles that are created during the Oracle Audit Vault installation process. Understanding how these pieces fit together provides the foundation you need to administer Oracle Audit Vault.

1.2.2 Step 2: Plan the Oracle Audit Vault Source Database and Collector Configuration

[Section 1.6](#) provides guidelines for selecting the correct Oracle Audit Vault collector (that is, the module that collects audit data from your source databases) based on the type of database from which you are collecting audit data. You must understand the audit settings and audit trail used in your source databases before you can select the correct collector.

1.2.3 Step 3: Configure Collectors to Collect Audit Data

After you have decided which collectors to use for your source database, you are ready to configure them. [Chapter 2](#) explains how to register (configure) collectors for the source databases.

To accomplish the configuration, you can use the command-line utilities described in [Section 1.4](#).

After you complete this step, Oracle Audit Vault is collecting audit data, which the auditors on your site can access by using the reporting tools described in *Oracle Audit Vault Auditor's Guide*.

1.2.4 Step 4: Monitor and Maintain the Audit Record Collection Process

After you have completed the configuration, you should monitor the audit collection activities to ensure that they are working properly. These tasks include the following:

- **Perform common management tasks.** For example, you may need to check whether the collectors are running, fine-tune how data is collected in the Oracle Audit Vault data warehouse, or modify the attributes of a source database. See the following chapters:
 - [Chapter 3](#) describes common management tasks.
 - [Chapter 4](#) provides advice on managing an Oracle Audit Vault installation on an Oracle Real Application Clusters environment, and what to do if you are concerned that your audit data will fill the default tablespace and disk space.
 - [Chapter 5](#) describes common security tasks and how Oracle Advanced Security and Oracle Database Vault enhance the security of an Oracle Audit Vault system.

- [Chapter 12](#) describes optimum initialization parameter settings for the REDO collector.
- **For Oracle Database administrators, periodically archive and purge the Oracle Database audit trail for the Oracle source database.** See the following:
 - [Section 4.10](#) describes steps to follow for archiving and purging the Oracle Database audit trail.
 - *Oracle Database SQL Reference* describes data dictionary views that you can query to ensure that your configuration settings are correct. These views are as follows:

DBA_AUDIT_MGMT_CONFIG_PARAMS

DBA_AUDIT_MGMT_LAST_ARCH_TS

DBA_AUDIT_MGMT_CLEANUP_JOBS

DBA_AUDIT_MGMT_CLEAN_EVENTS
 - *Oracle Database PL/SQL Packages and Types Reference* describes the DBMS_AUDIT_MGMT package, which contains the procedures and functions that you use to archive and purge the Oracle Database audit trail.
- **Troubleshoot problems that arise.** See the following:
 - [Appendix A](#) describes how to troubleshoot the Oracle Audit Vault system.
 - [Appendix B](#) explains how to resolve Oracle Audit Vault-specific error messages.

1.3 Components of Oracle Audit Vault

This section contains:

- [Source Databases](#)
- [Oracle Audit Vault Server](#)
- [Oracle Database Vault](#)
- [Audit Vault Collection Agent and Collectors](#)
- [How the Oracle Audit Vault Components Work Together](#)

1.3.1 Source Databases

A source database is a database from which Oracle Audit Vault collects audit data. Oracle Audit Vault can collect this audit data from the internal audit trail tables and operating system audit trail files of a source database.

[Table 1–1](#) lists the supported source database products.

Table 1–1 Supported Source Database Products

Database Product	Supported Versions
Oracle Database	<p>For the OSAUD and DBAUD collector types: Releases 9.2.x, 10.1.x, 10.2.x, and 11.x</p> <p>For the REDO collector type: Enterprise Edition Releases 9.2.0.8, 10.2.0.3, 10.2.0.4 and later, 11.1.0.6 and later, and 11.2 for the REDO collector type</p>

Table 1–1 (Cont.) Supported Source Database Products

Database Product	Supported Versions
Microsoft SQL Server	SQL Server 2000 and SQL Server 2005 on Windows 2000 Server and Windows 2003 Server platforms. SQL Server 2008. Only the Event Log, C2 and server-side trace audit trails are supported.
Sybase Adaptive Server Enterprise (ASE)	ASE 12.5.4 through ASE 15.0 on platforms based on Linux and UNIX, and on Microsoft Windows platforms
IBM DB2	IBM DB2 Version 8.2 through Version 9.5 on platforms based on Linux and UNIX, and on Microsoft Windows platforms. If you are using Version 8.2, ensure that you have installed Fixpack 16.

1.3.2 Oracle Audit Vault Server

The Oracle Audit Vault Server contains the tools necessary to configure Oracle Audit Vault to collect audit data from your source databases. The Audit Vault Server also contains an Oracle database, and makes it available to reporting tools through a data warehouse.

This section contains:

- [General Oracle Audit Vault Server Components](#)
- [Default Oracle Audit Vault Server Port Numbers](#)

1.3.2.1 General Oracle Audit Vault Server Components

The Audit Vault Server consists of:

- Audit data store (a repository containing the audit data that is collected by the Audit Vault collectors)
- Oracle Audit Vault Console
- The following services:
 - Audit data collection and storage management
 - Alert management
 - Collector management and monitoring
 - Report management
 - User entitlement management reports
 - Published data warehouse that can be used with reporting tools such as Oracle Business Intelligence Publisher to create customized reports

Configuration services help define information about the source databases that connect to Oracle Audit Vault. Oracle Audit Vault stores information (metadata) about the sources of audit data and policy information (database audit settings).

[Table 1–2](#) describes the Oracle Audit Vault Server components.

Table 1–2 Oracle Audit Vault Server Components

Components	Description
Oracle Container for Java (OC4J)	<p>Oracle Database container for Web applications. It hosts the following components:</p> <ul style="list-style-type: none"> ■ Audit Vault Console. User interface for administrators to administer Oracle Audit Vault. Also, Oracle Audit Vault auditors can use this interface to generate reports, create alerts, and create Oracle Database audit policies. ■ Oracle Enterprise Manager Database Control console. User interface to manage the raw audit data store or audit repository database. ■ Management Framework. Internal tool that sends management commands to the Audit Vault collection agent to start or stop collection agents and collectors, collect metrics, and receive management commands from the Oracle Audit Vault command-line tools using HTTP protocol or HTTPS mutual certificate-based authentication. Section 1.4 lists the Oracle Audit Vault command-line tools. ■ Audit Policy System. Internal service that retrieves and provisions audit settings from the Oracle Database source. It also enables users to create and manage alerts raised by audit events from all source databases while they are being stored in the audit event repository. ■ User Entitlement System. Internal service that retrieves user entitlement information from an Oracle Database source. ■ PDF scheduling and printing subsystem. Internal service that schedules and generates Oracle Audit Vault reports in PDF format. ■ SMTP integration system. Internal service that manages e-mail notifications for Oracle Audit Vault reports and alerts. ■ Remedy trouble ticket integration system. Internal service that manages the Remedy trouble ticket service for Oracle Audit Vault reports and alerts.
Database Client	<p>Infrastructure to communicate to the audit repository, consisting of:</p> <ul style="list-style-type: none"> ■ Oracle Wallet. Contains credentials to authenticate Oracle Audit Vault users ■ Configuration files. Files used by Oracle Audit Vault for networking, preferences, and so on.
Configuration and Management Tools	<p>Utilities used to configure and manage Oracle Audit Vault, which are described in detail in Section 1.4. They let you define and configure information about what source databases are known to Oracle Audit Vault.</p>
Logs	<p>Informational and error messages for Oracle Audit Vault. See Section A.1 for more information.</p>
Audit repository	<p>Oracle database (Release 10.2.0.4) to consolidate and manage audit trail records.</p> <p>It has the following components:</p> <ul style="list-style-type: none"> ■ Raw audit data store. A partitioned table where audit records are inserted as rows ■ Warehouse schema. An open schema of normalized audit trail records. This is a published data warehouse that auditors can use with reporting tools such as Oracle Business Intelligence Publisher to create customized reports. ■ Job scheduler. Database jobs used to populate and manage the warehouse ■ Alerts. A queue that maintains auditor-created alerts

1.3.2.2 Default Oracle Audit Vault Server Port Numbers

[Table 1–3](#) describes the ports that the Audit Vault Server uses. To find the port numbers that were used when you installed Oracle Audit Vault, check the `portlist.ini` file, which is in the `$ORACLE_HOME/install` directory. Be aware that if you change the port numbers later on, the `portlist.ini` file does not reflect the changes. If you need to change the port numbers, see [Section 4.9](#).

Table 1–3 Oracle Audit Vault Server Ports

Component	Default Port Number ¹	Required to be Open	Finding the Current Port Number
SQL*Net listener	1521	Yes	At a command line, enter the following command: <code>lsnrctl status</code>
Enterprise Manager Database Control HTTP (OC4J)	1158, 5500	Yes, if you want to use Database Control with the Audit Vault Console	At a command line, enter the following command: <code>emctl status dbconsole</code>
Oracle Audit Vault Console HTTP	5700	Yes	At a command line, enter the following command: <code>avctl show_av_status</code>
OC4J RMI	5522	No	Search for <code>rmi-server</code> port in the following file in the Audit Vault Server: <code>\$ORACLE_HOME/oc4j/j2ee/OC4J_DBConsole_hostname_SID/config/rmi.xml</code>
OC4J JMS	5542	No	Search for <code>jms-server</code> port in the following file in the Audit Vault Server: <code>\$ORACLE_HOME/oc4j/j2ee/OC4J_DBConsole_hostname_SID/config/jms.xml</code>
Oracle Audit Vault Reports HTTP	5707	Yes	In SQL*Plus, run the following query: <code>SELECT DBMS_XDB.GETHTTPPORT FROM DUAL;</code>

¹ The default port number can vary, depending on your installation. When you install Oracle Audit Vault, Oracle Universal Installer uses a range of port numbers. If another process is using the first default port number it finds, then it checks for the next free port number.

1.3.3 Oracle Database Vault

Oracle Database Vault is included in the Audit Vault Server. Database Vault protects the Audit Vault Server data, including restricting the audited data from administrative access. By default, Database Vault is enabled.

For more information about how Oracle Database Vault is integrated with Oracle Audit Vault, see [Section 5.5](#).

1.3.4 Audit Vault Collection Agent and Collectors

This section contains:

- [What Are Collection Agents and Collectors?](#)
- [General Audit Vault Collection Agent and Collector Components](#)
- [Default Audit Vault Collection Agent and Collector Port Numbers](#)

1.3.4.1 What Are Collection Agents and Collectors?

A **collector** retrieves the audit trail data from a source database and sends it to the Audit Vault Server. The **collection agent** manages the collectors. The collectors send both valid and invalid audit records, get configuration information, and send error records using Oracle Call Interface (OCI) and JDBC password-based authentication. If the collection agent is stopped, then the source database will still create an audit trail (assuming auditing is enabled). The next time you restart the collection agent, then Oracle Audit Vault retrieves the audit data that had been accumulating since the agent was stopped.

You configure one collection agent for each host and one or more collectors for each individual source database. For example, if a host contains four databases, then you would configure one collection agent for that host and one or more collectors for each of the four databases. The number of collectors that you configure and the collection agent that you use to manage them depends on the source database type and the audit trails that you want to collect from it.

The collector that you configure for each source database is based on the type of audit trail the source database is configured to use. For example, if an Oracle source database is configured to write the audit trail to the database audit trail, then it uses the DBAUD collector.

You can create the collection agent on one computer and manage multiple collection agents from there. For example, suppose you have 25 source databases on 25 servers. You must configure a collector for each of these source databases, but you do not need to configure a collection agent of each of the 25 servers. Instead, just create one collection agent to manage the 25 collectors. Be aware, however, that for Oracle databases, you cannot use a remote collection agent to collect audit data from users who have logged in with the SYSDBA or SYSOPER privilege.

1.3.4.2 General Audit Vault Collection Agent and Collector Components

[Table 1–4](#) describes the components of the collection agent.

Table 1–4 Oracle Audit Vault Collection Agent Components

Component	Description
OC4J	Oracle container for Web applications. It contains the Audit Vault Collector Manager , which receives management commands from the Audit Vault Server to start and stop collectors, collect and return metrics, and so on.
Database Server	Infrastructure to communicate to the audit repository, consisting of: <ul style="list-style-type: none"> ■ Oracle Wallet. Contains credentials to authenticate Audit Vault users ■ Configuration Files. Files used by Oracle Audit Vault for networking, preferences, and so on
Configuration and Management Tools	Utilities used to configure and manage Oracle Audit Vault. These are the AVCA, AVCTL, AVORCLDB, AVMSSQLDB, AVSYBDB, and AVDB2DB command-line utilities.
Logs	Informational and error messages for Oracle Audit Vault (see Section A.1)
Collectors	Table 1–5 shows the type of collectors deployed by the Oracle Audit Vault collection agents and the audit trail from which audit records are extracted and collected.

[Table 1–5](#) describes the types of collectors and their corresponding audit trail types.

Table 1–5 Oracle Audit Vault Collector Types and Audit Trails

Audit Source	Collector Type	Audit Trail
Oracle Database	DBAUD	<p>Collects from the following audit trails:</p> <ul style="list-style-type: none"> Oracle Database audit trail, where standard audit events are written to the <code>SYS.AUD\$</code> dictionary table Oracle Database fine-grained audit trail, where audit events are written to the <code>SYS.FGA_LOG\$</code> dictionary table Oracle Database Vault audit trail, where audit events are written to the <code>DVSYS.AUDIT_TRAIL\$</code> dictionary table
Oracle Database	OSAUD	<p>Collects data from the following audit trails:</p> <ul style="list-style-type: none"> On Linux and UNIX platforms: The Oracle database audit files written to the operating system (<code>.aud</code>) files, and syslog files (but not compressed syslog files) On Windows platforms: The operating system Windows Event Log and operating system logs (audit logs) XML (<code>.xml</code>) files
Oracle Database	REDO	Collects audit data from logical change records (LCRs) from the REDO logs. If you plan to use the REDO collector, you can define the data to audit by creating capture rules for the tables from which the REDO collector will capture audit information. See <i>Oracle Audit Vault Auditor's Guide</i> for more information.
Microsoft SQL Server	MSSQLDB	Collects audit data from C2 audit logs, server-side trace logs, and Windows Event Logs
Sybase ASE	SYBDB	Collects audit data from system audit tables (<code>sysaudits_01</code> through <code>sysaudits_08</code>) in the <code>sybsecurity</code> database
IBM DB2	DB2DB	Collects audit data from ASCII text files extracted from the binary audit log (<code>db2audit.log</code>). These files are located in the <code>security</code> subdirectory of the DB2 database instance.

1.3.4.3 Default Audit Vault Collection Agent and Collector Port Numbers

[Table 1–6](#) describes the default port numbers that the Audit Vault agent uses. To find the port numbers that were used when you installed Oracle Audit Vault, check the `portlist.ini` file, which is in the `$ORACLE_HOME/install` directory. Be aware that if you change the port numbers later on, the `portlist.ini` file does not reflect the changes. If you need to change the port numbers, see [Section 4.9](#).

Table 1–6 Oracle Audit Vault Agent Ports

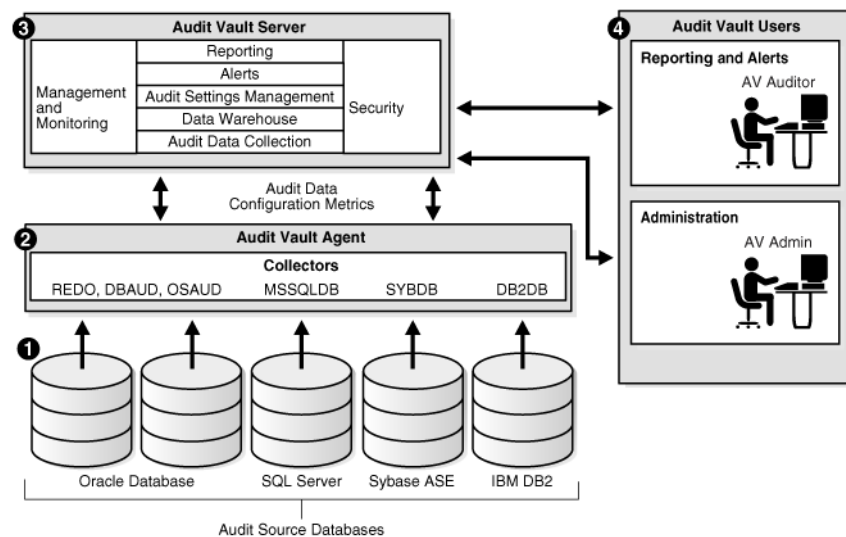
Component	Default Port Number ¹	Required to be Open	Finding the Current Port Number
OC4J RMI	3101	Yes	<p>Search for <code>rmi-server</code> port in the following file in the Audit Vault Agent home directory:</p> <p><code>\$ORACLE_HOME/oc4j/j2ee/home/config/rmi.xml</code></p>
OC4J JMS	3201	No	<p>Search for <code>jms-server</code> port in the following file in the Audit Vault Agent home directory:</p> <p><code>\$ORACLE_HOME/oc4j/j2ee/home/config/jms.xml</code></p>
Agent HTTP	7010	Yes	<p>Search for <code>web-site</code> port in the following file in the Audit Vault Agent home directory:</p> <p><code>\$ORACLE_HOME/oc4j/j2ee/home/config/http-web-site.xml</code></p>

¹ The default port number can vary, depending on your installation. When you install Oracle Audit Vault, Oracle Universal Installer uses a range of port numbers. If another process is using the first default port number it finds, then it checks for the next free port number.

1.3.5 How the Oracle Audit Vault Components Work Together

Figure 1–1 provides a high-level overview of how the Oracle Audit Vault components work together.

Figure 1–1 Overview of the Oracle Audit Vault Components



The process flow for the Oracle Audit Vault components works as follows:

1. The source databases, Oracle Database, SQL Server, Sybase ASE, and IBM DB2, have all been configured to use their respective collectors:
 - Oracle Database uses the REDO, DBAUD, and OSAUD collectors.
 - SQL Server uses the MSSQLDB collector.
 - Sybase ASE uses the SYBDB collector.
 - IBM DB2 uses the DB2DB collector.

As Figure 1–1 shows, you can configure multiple databases from different database product families using the same Audit Vault collection agent to connect to the same Audit Vault Server.

2. The collectors listed in Step 1 retrieve the audit data from their source databases and send this data to the Audit Vault Server.
3. The Audit Vault Server collects and stores this data in the database, and then makes it available in the warehouse.

The data warehouse organizes this data into a set of internal dimension tables. The Audit Vault Server stores other information as well, for both the auditor and the administrator.

4. Once the audit data is in the data warehouse dimension tables, an auditor can retrieve this data to generate and customize reports, as well as send e-mail notifications and trouble ticket alerts.

Any settings that you, the administrator, create, such as security settings, are contained in this server. The Audit Vault Server stores all the tools that you need to configure the Audit Vault components and source databases.

The details of the process flow for the Audit Vault components works as follows:

1. The OC4J components in the Audit Vault Server and Audit Vault collection agent connect using HTTP or HTTPS.

The OC4J is a container for Web applications that consists of the Audit Vault Console, the Oracle Enterprise Manager Database Control console, the Audit Vault internal tools (management framework), and the audit policy system used to retrieve and make available the audit settings. The HTTP (or HTTPS) connection is used for starting and stopping agents, managing metrics, and running commands related to policy retrieval.

The Audit Vault Server contains its own database server, and an Oracle wallet containing the administrator's credentials. It also stores configuration information from utility settings (such as AVCA, AVCTL, and the command-line utilities used for the four database products) and log files that store operational information, such as broken database connections and missing files.

In addition to its HTTP or HTTPS connection, each collector in the Oracle Audit Vault collection agent maintains an OCI and a JDBC connection to the Audit Vault Server using the credentials from the client wallet.

2. The collectors retrieve audit records from the source databases and send this data to the audit repository, which contains the Audit Vault data warehouse.

The data warehouse organizes this data into a set of dimension tables. *Oracle Audit Vault Auditor's Guide* describes the data warehouse dimension tables in detail. In addition to the data warehouse, the audit repository contains auditor-created alert information.

3. Oracle Audit Vault receives data from the Oracle Database redo logs using a database link. The Oracle Database redo logs bypass the collectors.

1.4 Administrative Tools for Managing Oracle Audit Vault

You can use the following tools to administer Oracle Audit Vault:

- **Audit Vault Console.** This graphical user interface provides most of the functionality that you need to administer Oracle Audit Vault.
- **Audit Vault Configuration Assistant (AVCA) command-line utility.** Use AVCA to perform operations such as adding, deploying, and dropping agents, or managing wallets. See [Chapter 6](#) for more information.
- **Audit Vault Control (AVCTL) command-line utility.** Use AVCTL to load, refresh, start, and stop Oracle Audit Vault collection agents and collectors. You also can load and purge data in the Oracle Audit Vault data warehouse with this utility. See [Chapter 7](#) for more information.
- **Audit Vault Oracle Database (AVORCLDB) command-line utility.** Use AVORCLDB to configure Oracle Database source databases with Oracle Audit Vault. See [Chapter 8](#) for more information.
- **Microsoft SQL Server Database (AVMSSQLDB) command-line utility.** Use AVMSSQLDB to configure SQL Server source databases with Oracle Audit Vault. See [Chapter 9](#) for more information.

- **Sybase ASE Database (AVSYBDB) command-line utility.** Use AVSYBDB to configure Sybase ASE source databases with Oracle Audit Vault. See [Chapter 10](#) for more information.
- **IBM DB2 Database (AVDB2DB) command-line utility.** Use AVDB2DB to configure IBM DB2 source databases with Oracle Audit Vault. See [Chapter 11](#) for more information.

1.5 Default Oracle Audit Vault Roles

[Table 1–7](#) describes the various Oracle Audit Vault administrator roles and the tasks permitted for each role. See also [Table 5–2](#) on page 5-10 for a listing of the roles and privileges that are granted to these administrator roles.

Table 1–7 Oracle Audit Vault Administrator Roles and Their Assigned Tasks

Role	When Is the Role Granted?	Role Is Granted to Whom?	Description
AV_ADMIN	During Server installation	Audit Vault administrator	<p>Accesses Oracle Audit Vault services to administer, configure, and manage a running Oracle Audit Vault system. A user who is granted this role configures and manages metadata for audit source databases, collection agents, collectors, the configuration of the source database with the collection agent, and the data warehouse. The installation process creates and grants a user account with this role. Only the user granted the AV_ADMIN role can grant the AV_ADMIN role to other Oracle Audit Vault administrators.</p> <p>You can consider the AV_ADMIN role a super-user account for Oracle Audit Vault, except that a user who has been granted this role cannot view, update, or delete audit data.</p>
AV_AUDITOR	During Server installation	Audit Vault auditor	<p>Accesses Oracle 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 who is granted this role manages central audit settings and alerts. This user also uses the data warehouse services to further analyze the audit data to look for trends, intrusions, anomalies, and other items of interest.</p> <p>The installation process creates and grants a user account with this role. However, during installation, you optionally can bypass creating this user account. In that case, the roles and privileges normally granted to AV_AUDITOR are granted to AV_ADMIN instead. 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.</p>
AV_AGENT	During collection agent registration	Collection agent software component	Manages collection agents and collectors by starting and stopping them. Oracle Audit Vault creates this role for internal use only.
DV_ACCTMGR	During Audit Vault Server installation	Database Vault account manager	<p>Manages database user accounts. Be aware that the inclusion of Oracle Database Vault in the Audit Vault Server prevents users SYS and SYSTEM from creating, altering, or dropping user accounts. See <i>Oracle Database Vault Administrator's Guide</i> for more information about how Oracle Database Vault affects user privileges. See also Section 5.5.</p> <p>In a default Oracle Audit Vault installation, this account name is based on the default Oracle Audit Vault AV_ADMIN user account, with dva appended. For example, if during the installation you created avadmin as the AV_ADMIN user, then the DV_ACCTMGR account name is avadmin dva.</p>
DV_OWNER	During Audit Vault Server installation	Database Vault owner	<p>Manages Oracle Database Vault roles and configuration.</p> <p>In a default Oracle Audit Vault installation, this account name is based on the default Oracle Audit Vault AV_ADMIN user account, with dvo appended. For example, if you created avadmin as the AV_ADMIN user, then the DV_OWNER account name is avadmin dvo.</p>

1.6 Planning the Source Database and Collector Configuration

This section contains:

- [About Planning the Source Database and Collector Configuration](#)
- [Planning the Oracle Source Database and Collector Configuration](#)
- [Planning the Microsoft SQL Server Source Database and Collector Configuration](#)
- [Planning the Sybase ASE Source Database and Collector Configuration](#)
- [Planning the IBM DB2 Source Database and Collector Configuration](#)

1.6.1 About Planning the Source Database and Collector Configuration

This section provides guidelines for selecting the correct Oracle Audit Vault collector for the source databases from which you want to extract audit data. In brief, for Oracle Database, the type of collector that you select depends on the type of auditing that you have enabled in the source database. The Microsoft SQL Server, Sybase ASE, and IBM DB2 databases each use one collector specific to each of these database products.

After you understand which collector to choose, you are ready to register the source database and collector with Oracle Audit Vault.

1.6.2 Planning the Oracle Source Database and Collector Configuration

To plan the Oracle Database source database and collector configuration:

1. Ensure that auditing has been enabled, and find the type of auditing that the Oracle source database uses.

See *Oracle Audit Vault Auditor's Guide* for more information about the Oracle Database requirements.

2. Based on the audit trail setting, determine which collector to use.

The type of auditing that has been enabled determines the collector you will choose. The types of collectors available are as follows:

- **OSAUD collector.** Use this collector if the audit trail is being written to operating system files. The agent for the OSAUD collector must reside on the same server as the source database. [Table 1-8](#) on page 1-13 lists the operating system audit trail settings that use the OSAUD collector.
- **DBAUD collector.** Use this collector if the audit trail is being written to the database audit trail. The agent for the DBAUD collector must reside on a computer in which SQL*Net can communicate with the source database. [Table 1-9](#) on page 1-13 lists of the database audit trail settings that use the DBAUD collector.
- **REDO collector.** Use this collector if the database is collecting audit data from the redo logs. The agent for the REDO collector must reside on a computer in which SQL*Net can communicate with the source database. On Oracle RAC installations, the REDO collector can reside on just one database instance, because REDO logs are usually stored in a shared location. [Table 1-10](#) on page 1-14 shows more information about redo logs.

To find the names and source database locations of existing agents, log in to Audit Vault Console, click the **Configuration** tab, and then click **Agent** to display the Agent page. This page lists the agent, host (source database), port, and user.

3. Register the Oracle source database and the appropriate collector with Oracle Audit Vault, as described in [Section 2.3](#).

The OSAUD operating system audit settings capture the following activities:

- SELECT statements
- Data definition language (DDL) and data manipulation language (DML) statements
- Succeeded and failed actions
- SYS operations (Set the AUDIT_SYS_OPERATIONS initialization parameter to TRUE to perform administrator auditing. SYS auditing collects SQL text information.)

[Table 1–8](#) lists the Oracle Database operating system audit settings that use the OSAUD collector.

Table 1–8 Oracle Database Operating System Audit Settings for the OSAUD Collector

Audit Trail	Audit Trail Setting	Comments
Linux and UNIX-based platforms (.aud)	For standard audit records: The AUDIT_TRAIL initialization parameter is set to OS. For fine-grained audit records: Not applicable.	None
Linux and UNIX-based platforms (.xml)	For standard audit records: The AUDIT_TRAIL initialization parameter is set to XML or XML, EXTENDED. For fine-grained audit records: The audit_trail parameter of the DBMS_FGA.ADD_POLICY procedure is set to DBMS_FGA.XML or DBMS_FGA.XML + DBMS_FGA.EXTENDED.	EXTENDED writes SQL text and SQL bind information to the audit trail.
Linux and UNIX-based platforms (syslog)	For standard audit records: The AUDIT_TRAIL initialization parameter is set to OS, and the AUDIT_SYSLOG_LEVEL parameter is set. For fine-grained audit records: Not applicable	More secure than audit records stored in operating system audit trail. Note: You cannot collect from compressed syslog files
Windows platform Windows Event Log	For standard audit records: The AUDIT_TRAIL initialization parameter is set to OS. For fine-grained audit records: Not applicable	None
Windows platform Operating system XML files (.xml)	For standard audit records: The AUDIT_TRAIL initialization parameter is set to XML or XML, EXTENDED. For fine-grained audit records: The audit_trail parameter of the DBMS_FGA.ADD_POLICY procedure is set to DBMS_FGA.XML or DBMS_FGA.XML + DBMS_FGA.EXTENDED.	EXTENDED writes SQL text and SQL bind information to the audit trail.

[Table 1–9](#) lists the Oracle Database database audit trail settings, which must use the DBAUD collector.

Table 1–9 Oracle Database Audit Trail Settings for the DBAUD Collector

Audit Trail	Audit Trail Setting	Audited Operations	Comments
SYS.AUD\$	For standard audit records: The AUDIT_TRAIL initialization parameter is set to DB or DB, EXTENDED. For fine-grained audit records: Not applicable	SELECT, DML, DDL, success and failure, SQL text, SQL bind	EXTENDED writes SQL text and SQL bind data to the audit trail.

Table 1–9 (Cont.) Oracle Database Audit Trail Settings for the DBAUD Collector

Audit Trail	Audit Trail Setting	Audited Operations	Comments
SYS.FGA_LOG\$	<p>For standard audit records: Not applicable</p> <p>For fine-grained audit records: The <code>audit_trail</code> parameter of the <code>DBMS_FGA.ADD_POLICY</code> procedure is set to <code>DBMS_FGA.DB</code> or <code>DBMS_FGA.DB + DBMS_FGA.EXTENDED</code>.</p>	Very specific user-defined audited conditions, such as the time a user modified a table column	None
DVSYSAUDIT_TRAIL\$	Not applicable. The Oracle Database Vault audit trail collects data even if Oracle Database auditing is disabled.	Oracle Database Vault audit activity specified by audit options on realms, command rules, and so on	None

Table 1–10 shows the redo log audit trail setting that uses the REDO collector.

Table 1–10 Oracle Database Redo Log Setting for the REDO Collector

Audit Trail	Audit Trail Setting	Audited Operations	Comments
Redo logs	Audit Vault capture rule (see <i>Oracle Audit Vault Auditor's Guide</i>)	DML, DDL, before and after values	Tracks before and after changes to sensitive data columns.

1.6.3 Planning the Microsoft SQL Server Source Database and Collector Configuration

To plan the Microsoft SQL Server source database instance configuration:

1. Ensure that auditing has been enabled in the SQL Server source database instance. See the Microsoft SQL Server product documentation for more information.
2. Ensure that the agent for the MSSQLDB collector was installed on the same computer as the Microsoft SQL Server source database. To find the names and source database locations of existing agents, log in to Audit Vault Console, click the **Configuration** tab, and then click **Agent** to display the Agent page. This page lists the agent, host (source database), port, and user.
3. Understand the audit trail settings used for SQL Server databases.

Table 1–11 lists the SQL Server audit trail settings.

4. Configure the MSSQLDB collector to collect audit data from the SQL Server database, as described in [Section 2.4](#).

Table 1–11 describes the SQL Server audit trail.

Table 1–11 Microsoft SQL Server Source Database Audit Settings for the MSSQLDB Collector

Audit Trail - Audit Logs	Audit Trail Settings	Audited Operations	Comments
C2 audit logs	Configure SQL Server security properties through SQL Server Enterprise Manager.	Auditing compliant with C2 certification Records both failed and successful attempts to access statements and objects Uses all or nothing approach to auditing	Records all actions
Server-side trace logs	Run stored procedures to start and stop tracing, to configure and filter traces.	Records fine-grained security-related activity Can choose exactly which events to audit and what information about each event to record Trace configuration information is not persistent. It is deleted when you restart SQL Server.	Records specific activity Traces can be configured to record only specific activity. Results can be filtered to record only activity that matches a certain pattern, such as a SQL verb (for example, <code>SELECT</code> , <code>INSERT</code> , <code>UPDATE</code> , <code>DELETE</code>), or that involve a particular object (for example, a specific table).
Windows Event Log	Running by default.	Provides a standard, centralized way for applications (and the operating system) to record important software and hardware events.	None

1.6.4 Planning the Sybase ASE Source Database and Collector Configuration

To plan the Sybase ASE source database configuration:

1. Ensure that auditing has been enabled in the Sybase ASE source database.
See the Sybase ASE product documentation for more information.
2. Understand the audit trail setting information used for Sybase ASE databases.
Table 1–12 shows the Sybase ASE audit trail setting information.
3. Ensure that the agent for the SYBDB collector was installed on a computer in which SQL*Net can communicate with the source database. To find the names and source database locations of existing agents, log in to Audit Vault Console, click the **Configuration** tab, and then click **Agent** to display the Agent page. This page lists the agent, host (source database), port, and user.
4. Configure the SYBDB collector to collect audit data from the Sybase ASE database, as described in Section 2.5.

Table 1–12 describes the Sybase ASE audit trail.

Table 1–12 Sybase ASE Database Audit Setting for the SYBDB Collector

Audit Trail - Audit Logs	Audit Trail Setting	Audited Operation	Comments
System audit table logs	Run system procedures to set global audit options, and then to enable, disable, or restart auditing.	Records standard to fine-grained audit and security-related activity Can choose exactly what to audit Can choose to audit everything or just very specific events	Implement your best practices for Sybase ASE database auditing

1.6.5 Planning the IBM DB2 Source Database and Collector Configuration

To plan the IBM DB2 source database configuration:

1. Ensure that auditing has been enabled in the IBM DB2 source database.
See the IBM DB2 product documentation for more information.
2. Understand the audit trail information used for IBM DB2 databases.
[Table 1–13](#) shows the IBM DB2 audit trail setting information.
3. Ensure that the agent for the DB2DB collector was installed on the same computer as the IBM DB2 source database. To find the names and source database locations of existing agents, log in to Audit Vault Console, click the **Management** tab, and then click **Collectors** to display the Collectors page.
4. Configure the DB2DB collector to collect audit data from the DB2 database, as described in [Section 2.6](#).

[Table 1–13](#) describes the DB2DB audit trail.

Table 1–13 IBM DB2 Database Audit Setting for the DB2DB Collector

Audit Trail - Audit Logs	Audit Trail Setting	Audited Operation	Comments
ASCII text files	Run the DB2AUDIT command to enable auditing, disable auditing, and set auditing operations.	<p>Audit (AUDIT). Changes to audit records or times that the audit log is accessed</p> <p>Authorization Checking (CHECKING). Authorization checking during attempts to access or manipulate DB2 database objects or functions</p> <p>Security Maintenance (SECMAINT). Grants or revokes to object or database privileges or to the DBADM privilege; also modification of the SYSADM_GROUP, SYSCTRL_GROUP, or SYSMAINT_GROUP configuration parameters</p> <p>Object Maintenance (OBJMAINT). Creating and dropping data objects</p> <p>System Administration (SYSADMIN). Operations requiring SYSADM, SYSMAINT, or SYSCTRL privileges</p> <p>User Validation (VALIDATE). Authentication of users or retrieval of system security information</p> <p>Operation Context (CONTEXT). Database operation context performed. Helps when interpreting the audit log file. See the IBM DB2 documentation for more information about how the operation context of a DB2 database is audited.</p> <p>In addition to these categories, you can audit successes, failures, or both.</p>	Implement your best practices for IBM DB2 database auditing

Registering Source Databases and Collectors

This chapter contains:

- [General Steps for Adding Sources and Deploying Collectors](#)
- [Checking and Setting Environment Variables](#)
- [Registering Oracle Database Sources and Collectors](#)
- [Registering Microsoft SQL Server Database Sources and Collector](#)
- [Registering Sybase ASE Database Sources and Collector](#)
- [Registering IBM DB2 Database Sources and Collector](#)
- [Starting the Collection Agents](#)
- [Starting the Collectors](#)
- [Checking the Status of the Collectors](#)
- [Checking If the Collectors Are Collecting Audit Records](#)

2.1 General Steps for Adding Sources and Deploying Collectors

You must perform the following general tasks to add source databases to Oracle Audit Vault and then deploy collectors:

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 Collection Agent.
See [Section 2.2](#).
2. Add an Oracle source database and collectors using the AVORCLDB command-line utility.
See [Section 2.3](#).
3. To add a Microsoft SQL Server source database and collector, use the AVMSSQLDB command-line utility
See [Section 2.4](#).
4. To add a Sybase ASE source database and collector, use the AVSYBDB command-line utility
See [Section 2.5](#).

5. To add an IBM DB2 source database and collector, use the AVDB2DB command-line utility.
See [Section 2.6](#).
6. Start the collection agents and collectors using the AVCTL command-line utility.
See [Section 2.7](#) and [Section 2.8](#).
7. Periodically ensure that the collectors are running and collecting audit data.
See [Section 2.9](#) and [Section 2.10](#).

2.2 Checking and Setting Environment Variables

This section contains:

- [About Checking and Setting Linux and UNIX Environment Variables](#)
- [Setting the Audit Vault Server Linux and UNIX Environment Variables](#)
- [Setting the Collection Agent Linux and UNIX Environment Variables](#)
- [Using Oracle Audit Vault in a Microsoft Windows Environment](#)
- [Setting the Oracle Source Database Linux and UNIX Environment Variables](#)

2.2.1 About Checking and Setting Linux and UNIX Environment Variables

For Linux and UNIX platforms, you must set environment variables before you begin the procedures in this chapter. You set these variables in the three shells that you will use to perform the configuration. *Keep these shells open throughout the configuration process.* You will need to access them periodically as you complete the configuration steps. If you close and then reopen a shell, then you must reset its environment variables.

Throughout this manual, when you are instructed to open a shell for the Audit Vault Server or the collection agent, remember to set the appropriate environment variables.

2.2.2 Setting the Audit Vault Server Linux and UNIX Environment Variables

You use the Audit Vault Server shell to interact with the Audit Vault Server. To set the environment variables for the Audit Vault Server, you can run either of two scripts, `coraenv` (for the C shell) or `oraenv` (for the Bourne, Bash, or Korn shell).

[Table 2–1](#) describes how the `coraenv` and `oraenv` scripts set the environment variables.

Table 2–1 Audit Vault Server Environment Variable Settings

Environment Variable	Behavior
ORACLE_HOME	Sets to the Audit Vault Server home directory.
ORACLE_SID	Prompts for the Oracle system identifier (SID) for the Audit Vault Server. By default, this SID is <code>av</code> .
PATH	Appends <code>\$ORACLE_HOME/bin</code> to your <code>PATH</code> environment variable.
LD_LIBRARY_PATH	Appends <code>\$ORACLE_HOME/lib</code> to your <code>LD_LIBRARY_PATH</code> environment variable setting. Applies to Linux x86, Linux x86_64, and Solaris SPARC_64 installations only.
SHLIB_PATH	Appends <code>\$ORACLE_HOME/lib</code> to your <code>SHLIB_PATH</code> environment variable setting. Applies to HP-UX installations only.

Table 2–1 (Cont.) Audit Vault Server Environment Variable Settings

Environment Variable	Behavior
LIBPATH	Appends \$ORACLE_HOME/lib to your LIBPATH environment variable setting. Applies to AIX installations only.

To set environment variables for the Audit Vault Server shell:

1. In the server where you installed the Oracle Audit Vault Server, open a shell.
2. Run one of the following scripts, which are located in the `/usr/local/bin` directory:
 - **C shell:** `coraenv`
 - **Bourne, Bash, or Korn shell:** `oraenv`
3. To test that the script was successful, try invoking the following command:

```
$ avctl -help
```

It should return help information for the AVCTL utility, and the only way it can do that is if the `ORACLE_HOME` and `PATH` environment variables are correctly set. If the scripts fail, then manually set the environment variables listed in [Table 2–1](#).

4. If you plan to add Microsoft SQL Server, Sybase ASE, or IBM DB2 source databases to Oracle Audit Vault, then set the `LANG` and `NLS_LANG` environment variables.

For example:

- **C shell:**

```
setenv LANG de_DE.UTF-8
```

```
setenv NLS_LANG GERMAN_GERMANY.AL32UTF8
```

- **Bourne, Bash, or Korn shell:**

```
LANG=de_DE.UTF-8
```

```
NLS_LANG=GERMAN_GERMANY.AL32UTF8
```

```
export LANG NLS_LANG
```

See *Oracle Database Globalization Support Guide* for more information about the `NLS_LANG` environment variable, including supported character sets and languages.

Oracle Audit Vault supports the following languages for the `LANG` environment variable:

en: English	ja: Japanese
de: German	ko: Korean
es: Spanish	pt_BR: Brazilian Portuguese
fr: French	zh_CN: Simplified Chinese
it: Italian	zh_TW: Traditional Chinese

Optionally, you can set the `LANG` environment variable in the `.profile` or `.cshrc` file.

You do not need to set this variable for the Oracle Database AVORCLDB utility. This utility automatically uses the NLS_LANG environment variable setting, which is set during installation. See *Oracle Database Globalization Support Guide* for more information about language support for Oracle Database.

5. Leave the Audit Vault Server shell open for the remaining procedures in this chapter.

2.2.3 Setting the Collection Agent Linux and UNIX Environment Variables

To set environment variables for the Audit Vault collection agent shell:

1. In the server where you installed the Audit Vault collection agent, open a shell.
2. Check and manually set the ORACLE_HOME environment variable to the Audit Vault collection agent home directory.

For example:

```
$ echo $ORACLE_HOME  
  
/opt/oracle/av  
  
$ setenv /opt/oracle/av_agent
```

3. Check and set the LD_LIBRARY_PATH environment variable to include \$ORACLE_HOME/lib.

For example:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$ORACLE_HOME/lib
```

4. Check and set the PATH environment variable to include \$ORACLE_HOME/bin. Be sure that you append this information to the existing PATH information.

For example:

```
$ setenv PATH ${PATH}:$ORACLE_HOME/bin
```

5. Ensure that the following environment variables are not set: ORACLE_SID, TNS_ADMIN, and TWO_TASK.

For C shell:

```
$ unsetenv ORACLE_SID  
$ unsetenv TNS_ADMIN  
$ unsetenv TWO_TASK
```

For Bourne, Bash, or Korn:

```
$ unset ORACLE_SID  
$ unset TNS_ADMIN  
$ unset TWO_TASK
```

6. To test that you correctly set these environment variables, try invoking the following command:

```
$ avctl -help
```

It should return help information for the AVCTL utility, and the only way it can do that is if the ORACLE_HOME and PATH environment variables are correctly set.

7. If you plan to add Microsoft SQL Server, Sybase ASE, or IBM DB2 databases to Oracle Audit Vault, then set the LANG and NLS_LANG environment variables.

See Step 4 under [Section 2.2.2](#) for instructions.

8. Leave the Audit Vault collection agent shell open for the remaining procedures in this chapter.

2.2.4 Using Oracle Audit Vault in a Microsoft Windows Environment

If you installed the Audit Vault Server or the collection agent on Microsoft Windows, then you do not need to set any environment variables. Instead, run the Oracle Audit Vault command-line utilities from the Audit Vault home directory, which is `ORACLE_HOME\bin`.

2.2.5 Setting the Oracle Source Database Linux and UNIX Environment Variables

To set the environment variables for the source database, you can run the same scripts, `corenv` or `oraenv`, that you used to set the Audit Vault Server environment variables. [Table 2-1](#) on page 2-2 describes how these scripts set the environment variables, except that for the source database, they set the `ORACLE_SID` variable to `orcl`, unless you have given it a different name during installation.

To set environment variables for the source database:

1. In the server where you installed the Oracle source database, open a shell.
2. From the `/usr/local/bin` directory, run one of the following scripts:
 - **C shell:** `coraenv` script
 - **Bourne, Bash, or Korn shell:** `oraenv` script
3. Leave the Oracle source database shell open for the remaining procedures in this chapter.

2.3 Registering Oracle Database Sources and Collectors

This section contains:

- [Step 1: Create a User Account on the Oracle Source Database](#)
- [Step 2: Verify That the Source Database Is Compatible with the Collectors](#)
- [Step 3: Register the Oracle Source Database with Oracle Audit Vault](#)
- [Step 4: Add the Oracle Collectors to Oracle Audit Vault](#)
- [Step 5: Enable the Audit Vault Agent to Run the Oracle Database Collectors](#)

2.3.1 Step 1: Create a User Account on the Oracle Source Database

The collectors that you will configure later must use this user account to access audit data from the Oracle source database, such as audit trail settings. For an Oracle Real Application Clusters environment, create one user, for the Oracle RAC database.

To create the user account:

1. Open a shell for the Oracle source database.
2. Log in to SQL*Plus as a user who has been granted the `CREATE USER` privilege.

If the source database is protected by Oracle Database Vault, log in as a user who has been granted the `DV_ACCTMGR` (Database Vault Account Manager) role.

For example:

```
sqlplus trbokuksa
Enter password: password
Connected.
```

3. Create the Oracle source database user account.

For example:

```
SQL> CREATE USER srcuser_ora IDENTIFIED BY password;
```

4. Connect as user SYS with the SYSDBA privilege.

```
SQL> CONNECT SYS/AS SYSDBA
Enter password: password
```

5. Run the `zarsspriv.sql` script from either the Audit Vault Server or Audit Vault collection agent on Oracle source database.

This script grants the Oracle source database user account the privileges needed to enable the collectors to access audit data. By default, this script is located in the `$ORACLE_HOME/av/scripts/streams/source` directory in both the Audit Vault Server and the Audit Vault collection agent Oracle home directories.

Use the following syntax:

```
zarsspriv.sql srcusr mode
```

In this specification:

- *srcusr*: Enter the name of the source database user account that you created in Step 3.
- *mode*: Specify one of the following modes. Enter the modes in uppercase letters.
 - **SETUP**: For the OSAUD and DBAUD collectors, and for policy management
 - **REDO_COLL**: For the REDO log collector; includes all privileges that are granted using the argument mode **SETUP**

For example, to specify the **SETUP** mode for user `srcuser_ora`:

```
SQL> @/oracle/product/10.2.3/av_server/av/scripts/streams/source/zarsspriv.sql
Enter value for 1: srcuser_ora
Enter value for 2: SETUP
```

```
Granting privileges to SRCUSER_ORA ... Done.
```

6. If the source database has Oracle Database Vault installed, then log in as a user who has been granted the `DV_OWNER` (Database Vault Owner) role and add the source database user to the Oracle Data Dictionary realm.

For example:

```
SQL> CONNECT preston
Enter password: password
Connected.
```

```
SQL> EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('Oracle Data Dictionary', 'SRCUSER_
ORA', null, dbms_macutl.g_realm_auth_participant);
SQL> COMMIT;
```

7. If the source database has Oracle Database Vault installed, then grant the Oracle source database user account the DV_SECANALYST role.

The DV_SECANALYST role enables the user to run Oracle Database Vault reports and monitor Oracle Database Vault. This role also enables the Oracle source database user to collect Database Vault audit trail data from the source database.

For example:

```
SQL> GRANT DV_SECANALYST TO srcuser_ora;
```

8. If you plan to add the REDO collect to your source database, then grant the Oracle source database user account the DV_STREAMS_ADMIN role.

The DV_STREAMS_ADMIN role enables the management of Oracle Streams processes to be tightly controlled by Database Vault, but does not change or restrict the way an administrator would normally configure Oracle Streams.

For example:

```
SQL> GRANT DV_SECANALYST TO srcuser_ora;
```

9. Exit SQL*Plus.
10. Do not close this shell.

2.3.2 Step 2: Verify That the Source Database Is Compatible with the Collectors

Now you are ready to verify that the Oracle source database is compatible with the collector type in the Audit Vault collection agent home.

To verify the Oracle source database compatibility:

1. For the source database, run the following command and note the host, port, and service settings:

```
lsnrctl status
```

Alternatively, you can check the `tnsnames.ora` file.

```
cat $ORACLE_HOME/network/admin/tnsnames.ora
```

2. Log in to the source database and verify the type of auditing that has been configured.

For example, the following command confirms that you would need the DBAUD collector for this database:

```
sqlplus sys/as sysdba
Enter password: password
Connected.
```

```
SQL> SHOW PARAMETER AUDIT_TRAIL
```

NAME	TYPE	VALUE
audit_trail	string	DB

If you are unsure of which collector you should select, then see [Section 1.6.2](#).

3. Open a shell or command prompt for the Audit Vault Server or collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#) for the Audit Vault Server, or [Section 2.2.3](#) for the collection agent.

- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- 4. Run the `avorcldb verify` command, using the values that the `LSNRCTL` utility returned.

You must specify the host name, port number, and service name. Typically, for Oracle Database, the host is the fully qualified domain name or the IP address of the server on which the Oracle source database is running, and the port number is 1521.

For example, assuming that the host is `hrdb.example.com`, the port number is 1521, the service name is `orcl`, and the user account is `srcuser_ora`:

```
avorcldb verify -src hrdb.example.com:1521:orcl -colltype ALL
Enter Source user name: srcuser_ora
Enter Source password: password
```

Output similar to the following should appear:

```
source ORCL verified for Aud$/FGA_LOG$ Audit Collector collector
```

If instead errors are displayed, see the examples that follow this procedure.

See [Section 8.10](#) for detailed information about the `avorcldb verify` command.

- 5. Do not close this shell or command prompt.

The `AVORCLDB` utility checks if an Audit Vault collector can be run against the source database configuration.

[Example 2-1](#) shows what happens if the Oracle source database is not properly configured. In this case, you must set the initialization parameters listed in the output before you can use the REDO log collector.

Example 2-1 Partially Successful Verify Operation of Source Compatibility with the Collectors

```
avorcldb verify -src hrdb.example.com:1521:orcl -colltype ALL
Enter Source user name: srcuser_ora
Enter Source password: password

source ORCL verified for OS File Audit Collector
source ORCL verified 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 _JOB_QUEUE_INTERVAL not set; recommended value range [1 - ANY_VALUE]
Parameter JOB_QUEUE_PROCESSES = 0 not in recommended value range [4 - ANY_VALUE]
Parameter AQ_TM_PROCESSES = 0 is not in required value range [4 - 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
```

By default, the `init.ora` file resides in the `$ORACLE_HOME/dbs` directory.

After you correct the problems (in this case, setting all those missing or incorrect initialization parameters), rerun the `avorcldb verify` command to ensure that the result is as you want it. [Example 2-2](#) shows what happens after this source database has been properly configured. See also [Chapter 12, "REDO Collector Database Reference."](#)

Example 2–2 Successful Verify Operation of Source Compatibility with the REDO Collector

```

avorcldb verify -src hrdb.example.com:1521:orcl -colltype REDO
Enter Source user name: srcuser_ora
Enter Source password: password

source hrdb.EXAMPLE.COM verified for REDO Log Audit Collector collector

```

2.3.3 Step 3: Register the Oracle Source Database with Oracle Audit Vault

To register the Oracle source database with Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avorcldb add_source` command.

For example:

```

avorcldb add_source -src hrdb.example.com:1521:orcl
                    -srcname hr_db
                    -desc 'HR Database'
Enter Source user name: srcuser_ora
Enter Source password: password

Adding source...
Source added successfully.
source successfully added to Audit Vault

remember the following information for use in avctl
Source name (srcname): hr_db
Credential stored successfully.
Mapping Source to Agent...

```

In this example:

- `-src`: Enter the source database connection information: host name, port number, and service name, separated by a colon. If you are unsure of this information, run the `lsnrctl status` command on the computer where you installed the source database, or check the `tnsnames.ora` file.
- `-srcname`: Enter a name for the source database. If you omit this option, then Oracle Audit Vault names the source database after the global database name, which in this example is `ORCL`. Remember that the source database name is case sensitive.
- `-desc`: Optionally, enter a brief description for the source database.
- `Source user name and password`: Enter the user account information that you created in [Section 2.3.1](#).
- `Mapping Source to Agent`: This message in the output refers to the agent that you created just before you installed the Oracle Audit Vault agent.

See [Section 8.3](#) for detailed information about the `avorcldb add_source` command.

3. Note the source name return value from the output.

You will need this value, which represents the global database name, for subsequent steps in this section. In this example, the return value is `hr_db`.

4. Do not close this shell or command prompt.

2.3.4 Step 4: Add the Oracle Collectors to Oracle Audit Vault

You can add one or more collectors to Oracle Audit Vault, depending on your needs. The available collector types are listed in [Table 1–5](#) on page 1-8. For an Oracle Real Application Clusters environment, you can create collectors for each Oracle RAC node. If you plan to write the `.aud` or `.xml` audit file to a shared file system, then you only need one OSAUD collector for the Oracle RAC database.

To add a collector to Oracle Audit Vault:

1. If you plan to use the OSAUD collector, access the shell used for the Oracle source database.

If you plan to use either of the other collector types (DBAUD and REDO), then go to Step 4 of this procedure.

2. Log in to SQL*Plus as SYS with the SYSDBA privilege.

```
sqlplus sys as sysdba
Enter password: password
```

3. Set the maximum operating system file size to a setting equal to or less than 204800.

If the operating system file grows larger than 2 GB, then the OSAUD collector ignores all audit records created past this size. Use the following SQL statement to set the maximum size to 102400 KB, which translates as 2 GB.

```
BEGIN
  DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
    AUDIT_TRAIL_TYPE      => DBMS_AUDIT_MGMT.AUDIT_TRAIL_OS,
    AUDIT_TRAIL_PROPERTY  => DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE,
    AUDIT_TRAIL_PROPERTY_VALUE => 204800);
END;
/
```

Afterwards, if the operating system exceeds 2 GB, then Oracle Database stops appending audit records to the current file, and creates a new file to resume the audit data collection.

For reference information about the DBMS_AUDIT_MGMT PL/SQL package, see *Oracle Database PL/SQL Packages and Types Reference*.

4. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
5. Run the `avorcldb add_collector` command to add the collectors you want.

For example:

```
avorcldb add_collector -srcname hr_db
                      -agentname agent1
                      -colltype OSAUD
                      -orclhome /u01/app/oracle/product/10.2.0/db_1
```

In this example:

- `-srcname`: Enter the source name for this source database, which Oracle Audit Vault will refer to when collecting audit data. Remember that the source name is case-sensitive. This name was displayed when you ran the `avorcldb add_source` command in [Section 2.3.3](#).
- `-agentname`: Enter the name for the agent that you created using the `avca add_agent` command before you installed the Audit Vault collection agent, as described in *Oracle Audit Vault Collection Agent Installation Guide*. If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the **Configuration** tab, and then click the **Agent** tab to display the Agents page. The name of the agent is displayed in the Agent column.
- `-colltype`: Enter OSAUD, DBAUD, or REDO. If you plan to specify REDO, you must include the `-av` argument, which specifies the connection information for the database link from the source database to Oracle Audit Vault. See [Section 8.2](#) more information about the `-av` argument.
- `-orclhome`: Enter the Oracle source database home directory. For Microsoft Windows installations of Oracle Database, enter the path using forward slashes, or if you want to use back slashes, enclose the path in double quotation marks. For the DBAUD and REDO collectors, this parameter is optional.

See [Section 8.2](#) for detailed information about the `avorcldb add_collector` command. Examples of running the `avorcldb add_collector` command follow this procedure.

6. Note the collector name return from the output.

You will need this value whenever you configure settings for the collector. In this example, the return value in this example is `OSAUD_Collector`.

7. Optionally, modify the attributes associated with the collector.

The collector has a set of default attributes. You can modify these by using the `avorcldb alter_collector` command. See [Section 8.4](#).

8. Do not close this shell or command prompt.

[Example 2–3](#) shows how to add the OSAUD collector to Oracle Audit Vault for UNIX platforms. You must include the `-orclhome orclhome` parameter to specify the location of the source database as an absolute path, if `u01/app` is the Oracle base directory.

Example 2–3 Adding the OSAUD Collector to Oracle Audit Vault for UNIX Platforms

```
avorcldb add_collector -srcname hr_db
                    -agentname agent1
                    -colltype OSAUD
                    -orclhome /u01/app/oracle/product/10.2.0/db_1
```

```
source hr_db 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 2-4](#) shows how to add the OSAUD collector to Oracle Audit Vault on Microsoft Windows for the event log and XML audit trail. You must include the `-orclhome orclhome` parameter to specify the location of the source database. Use slashes (/) instead of backslashes (\) for the Microsoft Windows path. If you want to use backslashes, enclose the path in double quotation marks. For example:

```
-orclhome "c:\oracle\product\10.2.0\db_1"
```

Example 2-4 Adding the OSAUD Collector to Oracle Audit Vault on Microsoft Windows

```
avorcldb add_collector -srcname hr_db
                        -agentname agent1
                        -colltype OSAUD
                        -orclhome c:/oracle/product/10.2.0/db_1

source hr_db verified for Windows Event 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): OSAUD_Collector
```

[Example 2-5](#) shows how to add the DBAUD collector to Oracle Audit Vault.

Example 2-5 Adding the DBAUD Collector to Oracle Audit Vault

```
avorcldb add_collector -srcname hr_db
                        -agentname agent1 -colltype DBAUD

source hr_db 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 2-6](#) shows how to add the REDO collector to Oracle Audit Vault. Note that you must supply the `-av` argument for this collector type.

Example 2-6 Adding the REDO Collector to Oracle Audit Vault

```
avorcldb add_collector -srcname hr_db
                        -agentname agent1
                        -colltype REDO
                        -orclhome hrdb.example.com:1521:orcl

source hr_db 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
```

Note: If the REDO collector does not initialize, the APPLY process on the Audit Vault Server and CAPTURE process on the source database cannot start. This problem happens if the source user account does not have the correct privileges. Ensure that you ran the `zarsspriv.sql` script, described in [Section 2.3.1](#).

2.3.5 Step 5: Enable the Audit Vault Agent to Run the Oracle Database Collectors

You are now ready to add the collection agent credentials to the Oracle source database. This process adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet. This way, the Audit Vault collection agent can run the Oracle Database collectors. You must complete this step so that the collectors can start properly.

To enable to Audit Vault agent to run the Oracle Database collectors:

1. Access the shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
2. Use the `avorcldb setup` command to add the collection agent credentials.

For example:

```
avorcldb setup -srcname hr_db
```

```
Enter Source user name: srcuser_ora
```

```
Enter Source password: password
```

```
adding credentials for user srcuser_ora for connection [SRCDB1]
```

```
Credential stored successfully.
```

```
updated tnsnames.ora with alias [SRCDB1] to source database
```

```
verifying SRCDB1 connection using wallet
```

In this example:

- `-srcname`: Enter the name of the source database that you plan to use.
- `Source user name` and `Source password` prompts: Enter the source database user name and password that you created in [Section 2.3.1](#).

See [Section 8.9](#) for detailed information about the `avorcldb setup` command.

This step completes the registration for the Oracle source database and its collectors. Next, you must start the collection agents and collectors. See [Section 2.7](#) and [Section 2.8](#) for more information.

2.4 Registering Microsoft SQL Server Database Sources and Collector

This section contains:

- [Step 1: Download the Microsoft SQL Server JDBC Driver](#)
- [Step 2: Create a User Account on the Microsoft SQL Server Database Instance](#)
- [Step 3: Verify That the Database Instance Is Compatible with the Collector](#)
- [Step 4: Register the SQL Server Source Database Instance with Audit Vault](#)
- [Step 5: Add the MSSQLDB Collector to Oracle Audit Vault](#)

- [Step 6: Enable the Audit Vault Agent to Run the MSSQLDB Collector](#)
- [Step 7: Optionally, Schedule an Audit Trail Cleanup for SQL Server Audit Files](#)

2.4.1 Step 1: Download the Microsoft SQL Server JDBC Driver

Oracle Audit Vault requires a JDBC connection to the SQL Server database. Audit Vault supports Microsoft SQL Server JDBC Driver version 1.2. Ensure that you have downloaded the JDBC driver (`sqljdbc.jar`) to the `$ORACLE_HOME/jlib` directories in both the Audit Vault Server and Audit Vault collection agent homes. This driver provides high performance native access to Microsoft SQL Server 2000, 2005, 2008 database data sources. Verify that the `.jar` file is present in the Oracle Audit Vault collection agent before you start the collection agent.

See the following Web site for more information about the Microsoft SQL Server JDBC drivers:

<http://msdn.microsoft.com/en-us/data/aa937724.aspx>

See Also:

- *Oracle Audit Vault Server Installation Guide for Linux x86* for information about downloading and copying JDBC driver files for Microsoft SQL Server
- *Oracle Audit Vault Collection Agent Installation Guide* for information about downloading and copying JDBC driver files for Microsoft SQL Server
- *Oracle Audit Vault Collection Agent Installation Guide* to ensure that the `sqljdbc.jar` file is present in the Oracle Audit Vault OC4J before starting the agent OC4J

2.4.2 Step 2: Create a User Account on the Microsoft SQL Server Database Instance

The collector that you will configure later must use this user account to access audit data from the Microsoft SQL Server source database instance. After you create the user account, the privileges that you assign to this user depend on whether the source database instance is Microsoft SQL Server 2000, 2005, or 2008.

To create the user account:

1. Log in to the Microsoft SQL Server source database instance.
2. Create a user account.

For example, to create a user account named `srcuser_mss`:

```
EXEC sp_addlogin srcuser_mss, password
```

For a Microsoft SQL Server 2005 or 2008 database, grant this user the `alter_trace` privilege.

1. Log in as the `SYSADMIN` user.
2. Run the following command to grant the alter trace privilege to the user.

For example:

```
GRANT ALTER TRACE TO srcuser_mss
```

For a Microsoft SQL Server 2000 database instance, grant the user the `SYSADMIN` fixed server role.

1. Click **Security**.
2. Click **Logins**.
3. Right-click the login you created (for example, `srcuser_mss`).
4. Click **Properties**.
5. On the left pane, click **Server Roles**.
6. Select the **sysadmin option** setting, and then click **OK**.

2.4.3 Step 3: Verify That the Database Instance Is Compatible with the Collector

You can verify that the Microsoft SQL Server source database instance is compatible with the collector type in the Audit Vault collection agent home.

To verify the source database instance compatibility:

1. Access the shell or command prompt for the Audit Vault Server or collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#) for the Audit Vault Server, or [Section 2.2.3](#) for the collection.
 - **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
2. Run the `avmssqldb verify` command.

You must specify the host name and database instance, or the host name and port number. Typically, for Microsoft SQL Server, the host is the fully qualified domain name or the IP address of the server on which the SQL Server source database instance is running, and the port number is 1433.

For example, assume that the host is `hrdb.example.com`, the database instance is `hr_db`, and the user account is `srcuser_mss`:

```
avmssqldb verify -src 'hrdb.example.com\hr_db'
Enter a username : srcuser_mss
Enter a password: password

***** Source Verified *****
```

Enclose the `-src` value in single quotation marks, as shown in this example. If you specify the host name and port number, use the following convention, which omits the quotation marks and separates the host and port with a colon:

```
avmssqldb verify -src host:port
```

See [Section 9.10](#) for detailed information about the `avmssqldb verify -src` command.

3. Do not close this shell or command prompt.

2.4.4 Step 4: Register the SQL Server Source Database Instance with Audit Vault

To register the SQL Server source database instance with Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).

- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avmssqldb add_source` command.
For example:

```
avmssqldb add_source -src 'hrdb.example.com\hr_db' -srcname mssqldb4 -desc 'HR Database'
Enter a username: srcuser_mss
Enter a password : password

***** Source Verified *****
***** Source Added Successfully *****
```


In this example:
 - `-src`: Enter the fully qualified domain name (or IP address) and database instance name, or the domain name and port number for the source database instance that you specified in [Section 2.4.3](#).
 - `-srcname`: Create a name for the source database instance, which. Oracle Audit Vault will refer to when it collects audit data.
 - `-desc`: Optionally, enter a brief description for the source database instance.
 - `username` and `password`: Enter the user name and password that you created in [Section 2.4.2](#).See [Section 9.3](#) for detailed information about the `avmssqldb add_source` command.
 3. Do not close this shell or command prompt.

2.4.5 Step 5: Add the MSSQLDB Collector to Oracle Audit Vault

Now you are ready to add the MSSQLDB collector to Oracle Audit Vault. By default, the MSSQLDB collector collects audit records from all audit trails that have been enabled in the source database: C2 audit logs, server-side trace logs, and the Windows Event log.

To add the MSSQLDB collector to Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avmssqldb add_collector` command.

For example:

```
avmssqldb add_collector -srcname mssqldb4 -agentname agent1
Enter a username: srcuser_mss
Enter a password: password

***** Collector Added Successfully*****
```


In this example:

- `-srcname`: Enter the name of the SQL Server source database instance that you verified in [Section 2.4.3](#).
- `-agentname`: Enter the name for the agent that you created using the `avca add_agent` command before you installed the Audit Vault collection agent, as described in *Oracle Audit Vault Collection Agent Installation Guide*. If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the **Configuration** tab, and then click the **Agent** tab to display the Agents page. The name of the agent is displayed in the Agent column.

See [Section 9.2](#) for detailed information about the `avmssqldb add_collector` command.

3. Run the `avmssqldb alter_collector` command to alter the collector to specify the name of the file from which to collect the audit records.

For example:

```
avmssqldb alter_collector -srcname mssqldb4 -collname MSSQLCollector
SERVERSIDE_TRACE_FILEPATH="c:\SQLAuditFile*.trc"
```

See [Section 9.4](#) for more information about the `avmssqldb alter_collector` command.

4. Optionally, modify the attributes associated with the MSSQLDB collector.

The MSSQLDB collector has a set of default attributes. You can modify these by using the `avssqldb alter_collector` command. See [Section 9.4](#).

5. Do not close this shell or command prompt.

2.4.6 Step 6: Enable the Audit Vault Agent to Run the MSSQLDB Collector

Next, you must add the collection agent credentials to the Microsoft SQL Server source database instance. This process adds the source user credentials to the wallet, creates a database alias in the wallet for the source database instance user, and verifies the connection to the source database instance using the wallet. This way, the Oracle Audit Vault collection agent can run the MSSQLDB collector. You must complete this step so that the collectors can start properly.

To enable the Oracle Audit Vault agent to run the MSSQLDB collector:

1. On Windows, open a command prompt for the Audit Vault collection agent and then go to the `ORACLE_HOME\bin` directory.

(You cannot perform this procedure in a UNIX environment.)

2. Run the `avmssqldb setup` command.

For example:

```
avmssqldb setup -srcname mssqldb4
Enter a username : srcuser_mss
Enter a password : password
```

```
***** Credentials Successfully added *****
```

In this example:

- `-srcname`: Enter the source database instance name that you specified in [Section 2.4.3](#).

- username and password prompts: Enter the user name and password that you created in [Section 2.4.2](#).

See [Section 8.9](#) for detailed information about the `avmssqldb setup` command.

This step completes the registration for the Microsoft SQL Server source database and its collector. Next, you must start the collection agent and collector. See [Section 2.7](#) and [Section 2.8](#) for more information.

2.4.7 Step 7: Optionally, Schedule an Audit Trail Cleanup for SQL Server Audit Files

If the MSSQLDB collector has collected data from a trace file and the trace file is inactive, then you can clean up this file. The MSSQLDB collector writes the names of the SQL Server audit text files to a plain text file with the `.atc` extension. The `.atc` file resides in the `ORACLE_HOME/av/log` directory on the computer on which the agent is installed.

To manually clean up files that Oracle Audit Vault has completed extracting audit records from:

1. Go to the `ORACLE_HOME/bin` directory of the computer where the collection agent is installed.

Ensure that the `ORACLE_HOME` environment variable is correctly set.

2. Run the following utility:

```
c:\ORACLE_HOME\bin> SQLServerCleanupUtil -srcname source_name -collname
collector_name
```

For example:

```
c:\ORACLE_HOME\bin> SQLServerCleanupUtil -srcname mssqldb4 -collname
MSSQLCollector
```

To automate the cleanup of SQL Server trace files, you can use the Windows Scheduler.

Note: If the SQL Server trace definition is redefined or reinitialized, then you must ensure that the file names of the trace files do not overlap with trace files that were created earlier.

For example, suppose you start SQL Server with a trace definition in which the trace files names use the following format:

```
c:\serversidetraces.trc
c:\serversidetraces_1.trc
c:\serversidetraces_2.trc
...
c:\serversidetraces_259.trc
```

Then you restart the SQL Server with a new trace definition. This new trace definition must use a different file name from the current trace files (for example, the current one named `c:\serversidetraces.trc`). If you do not, then when you purge the audit trail (as described in [Section 4.10](#)), the new trace files that have same names as the old ones will be deleted.

2.5 Registering Sybase ASE Database Sources and Collector

This section contains:

- [Step 1: Download the jConnect for JDBC Driver](#)
- [Step 2: Create a User Account on the Sybase ASE Source Database](#)
- [Step 3: Verify That the Source Database Is Compatible with the Collector](#)
- [Step 4: Register the Sybase ASE Source Database with Oracle Audit Vault](#)
- [Step 5: Add the SYBDB Collector to Oracle Audit Vault](#)
- [Step 6: Enable the Audit Vault Agent to Run the SYBDB Collector](#)

2.5.1 Step 1: Download the jConnect for JDBC Driver

Ensure that you have downloaded the jConnect 6 JDBC driver (`jconn3.jar`) to the `$ORACLE_HOME/jlib` directories in both the Audit Vault Server and Audit Vault Agent homes. This driver provides high performance native access to Sybase ASE database data sources. Ensure that this jar file is present in the Oracle Audit Vault OC4J before starting the collection agent. The SYBDB collector uses this driver to collect audit data from Sybase ASE databases.

See Also:

- *Oracle Audit Vault Server Installation Guide for Linux x86* for information about downloading and copying JDBC driver files for Sybase ASE
- *Oracle Audit Vault Collection Agent Installation Guide* for information about downloading and copying JDBC driver files for Sybase ASE
- *Oracle Audit Vault Collection Agent Installation Guide* to ensure that the `sqljdbc.jar` file is present in the Oracle Audit Vault OC4J before starting the agent OC4J

2.5.2 Step 2: Create a User Account on the Sybase ASE Source Database

The collector that you will configure later must use this user account to access audit data from the Sybase ASE source database.

To create the user account:

1. Log in to the Sybase ASE source database.
2. Create a user account.

For example:

```
sp_addlogin srcuser_syb, password
```

3. Add this user to the Sybase ASE source database.

```
sp_adduser srcuser_syb
```

4. Grant the `SSO_role` privilege to the source user.

```
grant role sso_role to srcusr_syb
```

2.5.3 Step 3: Verify That the Source Database Is Compatible with the Collector

Now you are ready to verify that the Sybase ASE source database is compatible with the collector type in the Audit Vault collection agent home:

To verify the Sybase ASE source database compatibility:

1. Open a shell or command prompt for the Audit Vault Server or collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#) for the Audit Vault Server, or [Section 2.2.3](#) for the collection agent.
 - **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
2. Run the `avsybdb verify` command.

You must specify the host name and port number. Typically, for Sybase ASE, the host is the fully qualified domain name or IP address of the server on which the Sybase ASE source database is running, and the port number is 5000.

For example, assume that the host is `hrdb.example.com` and the port number is 5000, and the user account is `srcuser_syb`:

```
avsybdb verify -src hrdb.example.com:5000
Enter a username: srcuser_syb
Enter a password: password
```

```
***** Source Verified *****
```

See [Section 10.10](#) for detailed information about the `avsybdb verify` command.

3. Do not close this shell or command prompt.

2.5.4 Step 4: Register the Sybase ASE Source Database with Oracle Audit Vault

To register the Sybase ASE source database with Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avsybdb add_source` command.

For example:

```
avsybdb add_source -src hrdb.example.com:5000 -srcname sybdb4
Enter a username: srcuser_syb
Enter a password: password
```

```
***** Source Verified *****
***** Source Added Successfully *****
```

In this example:

- `-src`: Enter the fully qualified domain name (or IP address) and port number for the source database that you verified in [Section 2.6.3](#).
- `-srcname`: Create a name for this source database. Oracle Audit Vault refers to this name when it collects audit data.

- username and password prompts: Enter the user name and password that you created in [Section 2.5.2](#).

See [Section 10.3](#) for detailed information about the `avsybdb add_source` command.

3. Do not close this shell or command prompt.

2.5.5 Step 5: Add the SYBDB Collector to Oracle Audit Vault

To add the SYBDB collector to Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avsybdb add_collector` command.

For example:

```
avsybdb add_collector -srcname sybdb4 -agentname agent1
Enter a username: srcuser_syb
Enter a password: password
```

```
***** Collector Added Successfully*****
```

In this example:

- `-srcname`: Create a name for the source database. Oracle Audit Vault refers to this name when collecting audit data.
- `-agentname`: Enter the name for the agent that you created using the `avca add_agent` command before you installed the Audit Vault collection agent, as described in *Oracle Audit Vault Collection Agent Installation Guide*. If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the **Configuration** tab, and then click the **Agent** tab to display the Agents page. The name of the agent is displayed in the Agent column.
- username and password: Enter the user name and password that you created in [Section 2.5.2](#).

See [Section 10.2](#) for detailed information about the `avsybdb add_collector` command.

3. Optionally, modify the attributes associated with the collector.

The collector has a set of default attributes. You can modify these by using the `avsybdb alter_collector` command. See [Section 10.4](#).

4. Do not close this shell or command prompt.

2.5.6 Step 6: Enable the Audit Vault Agent to Run the SYBDB Collector

You now are ready to configure the collection agent credentials to the Sybase ASE source database. This process adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet. This way, the Oracle Audit Vault collection agent can run the SYBDB collector. You must complete this step so that the collectors can start properly.

To enable the Oracle Audit Vault collection agent to run the SYBDB collector:

1. Access the shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
2. Run the `avsybdb setup` command.

For example:

```
avsybdb setup -srcname sybdb4
Enter a username: srcuser_syb
Enter a password: password

***** Credentials Successfully added *****
```

In this example:

- `-srcname`: Enter the source database name that you created in [Section 2.5.5](#).
- `username` and `password`: Enter the user name and password that you created in [Section 2.5.2](#).

See [Section 10.9](#) for detailed information about the `avsybdb setup` command.

This step completes the registration for the Sybase ASE source database and its collector. Next, you must start the collection agent and collector. See [Section 2.7](#) and [Section 2.8](#) for more information.

2.6 Registering IBM DB2 Database Sources and Collector

This section contains:

- [Step 1: Copy the DB2 JDBC and SQLJ Driver to the Audit Vault Homes](#)
- [Step 2: Designate a User Account on the IBM DB2 Source Database](#)
- [Step 3: Verify That the Source Database Is Compatible with the Collector](#)
- [Step 4: Register the IBM DB2 Source Database with Oracle Audit Vault](#)
- [Step 5: Add the DB2 Collector to Oracle Audit Vault](#)
- [Step 6: Convert the Binary DB2 Audit File to an ASCII Text File](#)

2.6.1 Step 1: Copy the DB2 JDBC and SQLJ Driver to the Audit Vault Homes

Copy the IBM Data Server Driver for JDBC and SQLJ (`db2jcc.jar`) to the `$ORACLE_HOME/jlib` directories in both the Audit Vault Server and Audit Vault Agent homes. Oracle Audit Vault requires driver version 3.50 or later. This version of the `db2jcc.jar` file is available in either IBM DB2 UDB version 9.5 or IBM DB2 Connect version 9.5 or later.

This driver provides high performance native access to IBM DB2 database data sources. The DB2 collector uses this driver to collect audit data from IBM DB2 databases, so the driver must be present in Oracle Audit Vault OCFJ before you can start the collection agent.

You can verify the version of this `.jar` file that is currently installed as follows:

1. Ensure that the directory path to the `db2jcc.jar` file is included in the `CLASSPATH` environment variable setting.

2. Run the following command:

```
java com.ibm.db2.jcc.DB2Jcc -version
```

2.6.2 Step 2: Designate a User Account on the IBM DB2 Source Database

Designate an IBM DB2 user account to be used for the AVDB2DB utility, which you will use later to configure collectors for your DB2 database. This user must have privileges to run the IBM DB2 `SYSPROC.ENV_GET_PROD_INFO` procedure.

Note: If you are using IBM DB2 Version 8.2, ensure that you have installed FixPak 9. Otherwise, the `SYSPROC.ENV_GET_PROD_INFO` procedure is not available.

2.6.3 Step 3: Verify That the Source Database Is Compatible with the Collector

Now you are ready to verify that the IBM DB2 source database is compatible with the collector type in the Audit Vault collection agent home.

To verify the IBM DB2 source database compatibility:

1. Open a shell or command prompt for the Audit Vault Server or collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#) for the Audit Vault Server, or [Section 2.2.3](#) for the collection agent.
 - **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
2. Run the `avdb2db verify` command.

You must specify the host name and port number. Typically, for IBM DB2, the host is the fully qualified domain name or IP address of the server on which the IBM DB2 source database is running, and the port number is 50000.

For example, assume that the host is `hrdb.example.com`, the port number is 50000, the source database is `sales_db`, and the user account is `srcuser_db2`:

```
avdb2db verify -src hrdb.example.com:50000:sales_db
Enter a username: srcuser_db2
Enter a password: password
```

```
***** Source Verified *****
```

See [Section 11.9](#) for detailed information about the `avdb2db verify` command.

3. Do not close this shell or command prompt.

2.6.4 Step 4: Register the IBM DB2 Source Database with Oracle Audit Vault

To register the IBM DB2 source database with Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avdb2db add_source` command.

For example:

```
avdb2db add_source -src hrdb.example.com:50000 -srcname db2db4
Enter a username: srcuser_db2
Enter a password: password

***** Source Verified *****
***** Source Added Successfully *****
```

In this example:

- `-src`: Enter the fully qualified domain name (or IP address), port number, and optionally, the database name, for the source database that you verified in [Section 2.6.3](#).
- `-srcname`: Create a name for this source database. Oracle Audit Vault refers to this name when it collects audit data.
- `username` and `password`: Enter the user name and password that you designated in [Section 2.6.2](#).

See [Section 11.3](#) for detailed information about the `avdb2db add_source` command.

3. Do not close this shell or command prompt.

2.6.5 Step 5: Add the DB2 Collector to Oracle Audit Vault

To add the DB2 collector to Oracle Audit Vault:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX**: If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows**: Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avdb2db add_collector` command.

For example:

```
avdb2db add_collector -srcname db2db4 -agentname agent1
Enter a username: srcuser_db2
Enter a password: password

***** Collector Added Successfully*****
```

In this example:

- `-srcname`: Create a name for the source database. Oracle Audit Vault refers to this name when collecting audit data.
- `-agentname`: Enter the name for the agent that you created using the `avca add_agent` command before you installed the Audit Vault collection agent, as described in *Oracle Audit Vault Collection Agent Installation Guide*. If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the **Configuration** tab, and then click the **Agent** tab to display the **Agents** page. The name of the agent is displayed in the Agent column.
- `username` and `password` prompts: Enter the user name and password that you designated in [Section 2.6.2](#).

See [Section 11.2](#) for detailed information about the `avdb2db add_collector` command.

3. Modify the `SINGLE_FILEPATH` attribute of the `avdb2db alter_collector` command to point to the location of the DB2 audit directory. This is the directory where the DB2 collector will collect audit data. You must specify an absolute path, not a relative path.

For example:

```
avdb2db alter_collector -srcname db2db4 -collname DB2Collector
SINGLE_FILEPATH=DB2_HOME/sqlib/security/auditdata
```

```
***** Collector Altered Successfully *****
```

See [Section 11.4](#) for more information about the `avdb2db alter_collector` command.

4. Do not close this shell or command prompt.

2.6.6 Step 6: Convert the Binary DB2 Audit File to an ASCII Text File

IBM DB2 creates its audit files in a binary file format that is separate from the DB2 database. You must convert the binary file to an ASCII file before each time Oracle Audit Vault collects audit data from a DB2 database. Ideally, schedule the script to run periodically. If the script finds older text files that have already been collected by the DB2 collector, then the script deletes them. It creates a new, timestamped ASCII text file each time you run it. Optionally, you can set the script to purge the output audit files.

- [Step 6A: Complete the Preparation Steps](#)
- [Step 6B: Run the Conversion Script](#)

2.6.6.1 Step 6A: Complete the Preparation Steps

Follow these steps:

1. Identify a user who has privileges to run the `db2audit` command.
This user will extract the binary files to the text files.
2. Access the shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
3. Grant the user you identified in Step 1 execute privileges to run the conversion script from the Oracle Audit Vault directory.

Alternatively, you can copy the appropriate conversion script located in the `$ORACLE_HOME/bin` directory to a location where this user can run them. These scripts are as follows:

- **DB2 release 8.2 databases:** `DB282ExtractionUtil` (for Microsoft Windows, this file is called `DB282ExtractionUtil.bat`.)
 - **DB2 9.5 release databases:** `DB295ExtractionUtil` (for Microsoft Windows, this file is called `DB295ExtractionUtil.bat`.)
4. Grant the user you identified in Step 1 read permission for the `$ORACLE_HOME/av/log` directory and its contents.

This user needs read permission for this directory as part of the process of generating the text files that are extracted by the extraction utility.

2.6.6.2 Step 6B: Run the Conversion Script

Follow these steps:

1. In the server where you installed the IBM DB2 database, open a shell as the SYSADM DB2 user.
2. Set the following variables:
 - ORACLE_HOME (this directory points to the Audit Vault Server home)
 - DB2AUDIT_HOME (this directory points to the main directory that contains the db2audit command)
3. Ensure that the Oracle Audit Vault owner of the agent process has read permissions for the audit text files that will be generated by the extraction utility.
4. Log in as the DB2 user that you identified in Step 1 in [Section 2.6.6.1](#).
5. Make a note of the directory that you identified in Step 3 in [Section 2.6.5](#).

You will need to provide this directory path when you run the conversion script.

6. Run one of the following scripts, depending on the version of DB2 that you have installed:

- **DB2 release 8.2 databases:** Run the script as follows:

```
DB282ExtractionUtil -extractionpath default_DB2_audit_directory  
-audittrailcleanup yes_or_no -databasename database_name
```

In this specification:

- **extractionpath:** Enter the full directory path to the location of the DB2 audit directory. Typically, this directory is in the following locations:

UNIX: *DB2_HOME/sqlib/security/auditdata*

Microsoft Windows: *DB2HOME\instance\security\auditdata*

Ensure that this path is the same as the path that you specified for the avdb2db alter_collector SINGLE_FILEPATH attribute in Step 3 in [Section 2.6.5](#).

- **audittrailcleanup:** Enter yes or no, to enable or disable the audit trail cleanup. Entering yes deletes the IBM DB2 audit file up to the latest audit record which has been collected by the Oracle Audit Vault DB2 collector. If you omit this value, then the default is no.
- **databasename:** Optional. Specify the name of the database that contains the audit records. This parameter enables you to collect categories of audit records such as object maintenance (objmaint) records, which capture the creation and dropping of tables. You can specify multiple databases. If you omit this parameter, then no database-specific audit records are extracted. Only all instance-wide audit records are extracted.

For example, to extract audit files and enable the audit trail cleanup for the databases TOOLDB, TESTDB, and EMDB:

```
DB282ExtractionUtil -extractionpath /home/extract_dir -audittrailcleanup  
yes -database TOOLSDb TESTDB EMPDB
```

This script creates the ASCII text file in the `auditdata` directory, using the following format, which indicates the time the file was created:

```
db2audit.instance.log.0.YYYYDDMMHHMMSS.out
```

- **DB2 release 9.5 databases:** Run the script as follows:

```
DB295ExtractionUtil -archivepath archive_path -extractionpath extraction_  
path -audittrailcleanup yes_or_no -databasename database_name
```

In this specification:

- **archivepath:** This is the same directory as the directory that is used for DB2 release 9.5.
- **extractionpath.** Enter the directory that is specified by the `avdb2db alter_collector SINGLE_FILEPATH` attribute. See [Table 11–2 in Section 11.4](#) for more information. This file is created in using the `db2audit.instance.log.0.YYYYDDMMHHMMSS.out` format.
- **audittrailcleanup:** Optional. Enter `yes` or `no`, to enable or disable the audit trail cleanup. Entering `yes` deletes the IBM DB2 audit file up to the latest audit record that was collected by the Oracle Audit Vault DB2 collector. If you omit this value, then the default is `no`.
- **databasename:** Optional. Specify the name of the database that contains the audit records. This parameter enables you to collect categories of audit records such as object maintenance (`objmaint`) records, which capture the creation and dropping of tables. You can specify multiple databases. If you omit this parameter, then no database-specific audit records are extracted. Only all instance-wide audit records are extracted.

These two directory paths can be the same, or optionally, you can specify different directories for each location.

For example, to extract audit files and enable the audit trail cleanup for the databases `TOOLDB`, `TESTDB`, and `EMDB`:

```
DB295ExtractionUtil -archivepath /home/archive_dir -extractionpath  
/home/extract_dir -audittrailcleanup yes -databasename TOOLSDb TESTDB  
EMPDB
```

To schedule the script to run automatically, follow these guidelines:

- **UNIX:** Use the `crontab` UNIX utility. Provide the same information that you would provide using the parameters described previously when you normally run the script.
- **Microsoft Windows:** Use the Windows Scheduler. Provide the archive directory path (for release 9.5 databases only), extraction path, and source database name in the scheduled task.

This step completes the registration for the IBM DB2 source database and its collector. Next, you must start the collection agent and collector. See [Section 2.7](#) and [Section 2.8](#) for more information.

2.7 Starting the Collection Agents

This section contains:

- [Starting the Oracle Audit Vault Release 10.2.3.2 Collection Agents](#)
- [Starting the Oracle Audit Vault Release 10.2.3.1 or Earlier Collection Agents](#)

2.7.1 Starting the Oracle Audit Vault Release 10.2.3.2 Collection Agents

When you create a new Release 10.2.3.2 collection agent or upgrade an earlier one, by default it will be started. You can check the status of the collection agents by running the `avctl show_agent_status` command, described in [Section 7.4](#).

If the collection agent has not started, then follow these steps:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
2. Run the `avctl start_agent` command, which starts the collection agent.

For example:

```
avctl start_agent

Starting Agent...
Agent started successfully.
```

See [Section 7.9](#) for more information.

2.7.2 Starting the Oracle Audit Vault Release 10.2.3.1 or Earlier Collection Agents

To start the collection agents that were created in Oracle Audit Vault Release 10.2.3.1 or earlier but have not yet been upgraded:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
2. Run the `avctl start_oc4j` command, which starts the collection agent.

```
avctl start_oc4j

Starting OC4J...
OC4J started successfully.
```

See [Section 7.15.2](#) for additional `avctl start_oc4j` parameters.

2.8 Starting the Collectors

This section contains:

- [Starting the Collectors from the Audit Vault Console](#)
- [Starting the Collectors from the Audit Vault Server](#)

2.8.1 Starting the Collectors from the Audit Vault Console

To start the collectors from the Audit Vault Console:

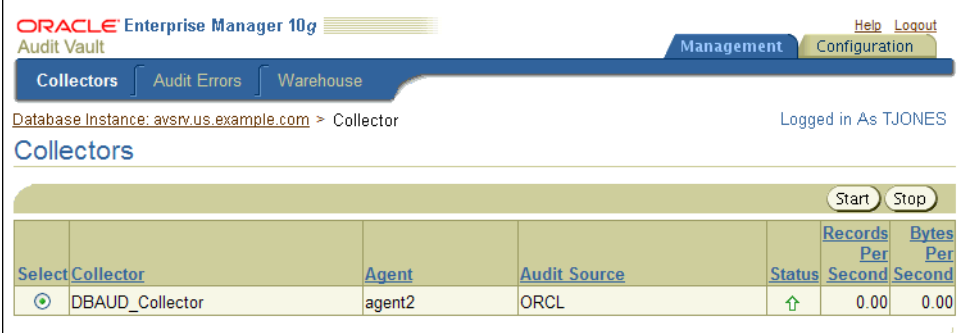
1. Log in to the Audit Vault Console as a user who has been granted the `AV_ADMIN` role.

See [Section 3.2.3](#) for login instructions.

2. Click the **Management** tab, then **Collectors** to display the **Collectors** page.

The Collectors page appears with a table containing the following columns.

- **Collector:** Name of the collector
- **Agent:** The name of the collection agent for this collector
- **Audit Source:** The name of the audit data source
- **Status:** The current running status of the collector: a green up arrow indicates that the collector is running, a red down arrow indicates that 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



Select	Collector	Agent	Audit Source	Status	Records Per Second	Bytes Per Second
<input checked="" type="radio"/>	DBAUD_Collector	agent2	ORCL	Running	0.00	0.00

3. Select the collector that you want to start.

This page also indicates whether the collector is running. A green up arrow indicates the collector is running; a red down arrow indicates it is not running.

4. Click **Start**.

In a moment, a message indicating that the collector has started should appear.

2.8.2 Starting the Collectors from the Audit Vault Server

To start the collectors from a shell:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avctl start_collector` command.

For example:

```
avctl start_collector -collname DBAUD_Collector -srcname hr_db
```

```
Starting collector...
Collector started successfully.
```

See [Section 7.11](#) for more information about the `avctl start_collector` command.

If the startup is successful, then Oracle Audit Vault moves the collector to a `RUNNING` state.

If the startup fails, then ensure that the collection agent is running:

- a. Open shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.

- b. Check the status of the collection agent.

For Release 10.2.3.2:

```
avctl show_agent_status
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl show_oc4j_status
```

- c. If the collection agent is not running, then enter the following command:

For Release 10.2.3.2:

```
avctl start_agent
```

```
Starting Agent...
Agent started successfully.
```

See [Section 7.9](#) for additional parameters `avctl start_agent` parameters.

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl start_oc4j
```

```
Starting OC4J...
OC4J started successfully.
```

See [Section 7.15.2](#) for additional parameters `avctl start_oc4j` parameters.

2.9 Checking the Status of the Collectors

This section contains:

- [Checking the Status of Collectors from the Audit Vault Console](#)
- [Checking the Status of Collectors from a Command Line](#)

2.9.1 Checking the Status of Collectors from the Audit Vault Console

1. Log in to the Audit Vault Console as a user who has been granted the `AV_ADMIN` role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Management** tab, and then select the **Collectors** tab.
3. In the Collectors page, check the list of collectors.

If the collector is running, its Status is set to an up arrow. If it is not, it is set to a red arrow pointing downward.

This page also lists the names of the agents associated with the collectors.

2.9.2 Checking the Status of Collectors from a Command Line

To check the status of collectors from the command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avctl show_collector_status` command.

For example:

```
avctl show_collector_status -collname DBAUD_Collector -srcname hr_db
```

```
Getting collector metrics...
```

```
-----
Collector is running
Records per second = 0.00
Bytes per second = 0.00
-----
```

See [Section 7.6](#) for detailed information about the `avctl show_collector_status` command.

2.10 Checking If the Collectors Are Collecting Audit Records

If the collection agents are not active (for example, they were disabled), then no audit data is lost, as long as the source database continues to collect the audit data. When you restart the collection agent, it captures the audit data that the source database had collected during the time the collection agent was inactive.

To ensure that audit records are being collected, inspect the contents of the log files in the Audit Vault collection agent `$ORACLE_HOME/av/log` directory. The log file names for command-line utilities are as follows:

- **Oracle Database AVORCLDB utility:** `collname_srcname_src_id.log` and `srcname-collname-#.log`
- **Microsoft SQL Server AVMSSQLDB utility:** `srcname-mssqldb-#.log`
- **Sybase ASE AVSYBDB:** `srcname-sybdb-#.log`
- **IBM DB2 AVDB2DB utility:** `srcname-db2db-#.log`

The 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 [Table A-2](#) on page A-3 for more information about these log files, and troubleshooting collector setup and collector startup operations.

Managing Oracle Audit Vault

This chapter contains:

- [About Managing Oracle Audit Vault](#)
- [Managing the Audit Vault Server](#)
- [Altering Collector Properties and Attributes](#)
- [Managing the Oracle Audit Vault Data Warehouse](#)
- [Altering Source Database Attributes](#)
- [Configuring E-Mail Notifications](#)
- [Configuring Oracle Audit Vault for the Remedy Trouble Ticket System](#)
- [Removing Source Databases from Oracle Audit Vault](#)

3.1 About Managing Oracle Audit Vault

This chapter describes common management activities that you need to perform after you have completed the configuration tasks in [Chapter 2](#). You can use the Audit Vault Console or the command-line tools described in this chapter to manage Oracle Audit Vault.

3.2 Managing the Audit Vault Server

This section contains:

- [About Managing the Audit Vault Console](#)
- [Checking the Audit Vault Console Status](#)
- [Starting and Logging into the Audit Vault Console](#)
- [Stopping the Audit Vault Server Console](#)
- [Globally Disabling and Enabling Alert Settings](#)
- [Viewing Audit Event Categories](#)
- [Viewing Operational Errors That Oracle Audit Vault Catches](#)

3.2.1 About Managing the Audit Vault Console

The Audit Vault Console is a graphical user interface that you can use to perform commonly used Oracle Audit Vault administration tasks. If you prefer to use a

command-line interface, you can use equivalent commands in the AVCA and AVCTL utilities.

3.2.2 Checking the Audit Vault Console Status

To check the status of the Audit Vault Console:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the following command:

```
avctl show_av_status
```

3.2.3 Starting and Logging into the Audit Vault Console

To start the Audit Vault Console:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Ensure that the Audit Vault Console is running.

```
avctl show_av_status
```

If the `avctl show_av_status` command indicates that the Audit Vault Console is not running, then enter the following command:

```
avctl start_av
```

At this stage, you can log in to the Audit Vault Console.

1. From a Web browser, enter the following URL:

```
http://host:port/av
```

In this specification:

- `host`: The host computer on which you installed the Audit Vault Server.
- `port`: The port number reserved for the Audit Vault Server.

If you are unsure of the host and port number values, then enter the `avctl show_av_status` command, which displays this information.

2. In the Login page, enter the following information:
 - **User Name:** Enter the name of a user who has been granted the `AV_ADMIN` role.
 - **Password:** Enter the user's password.
 - **Connect As:** From the list, select `AV_ADMIN`.
3. Click **Login**.

3.2.4 Stopping the Audit Vault Server Console

To stop the Audit Vault Server console:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the following command:

```
avctl stop_av
```

3.2.5 Globally Disabling and Enabling Alert Settings

If you must perform maintenance tasks or other similar activities that do not require alert settings to be active, then you can globally enable or disable the alert settings that Oracle Audit Vault auditors create. Do not disable alerts unless you are directed to do so by Oracle Support Services or if you encounter a problem with the alerts table. By default, alerts are enabled.

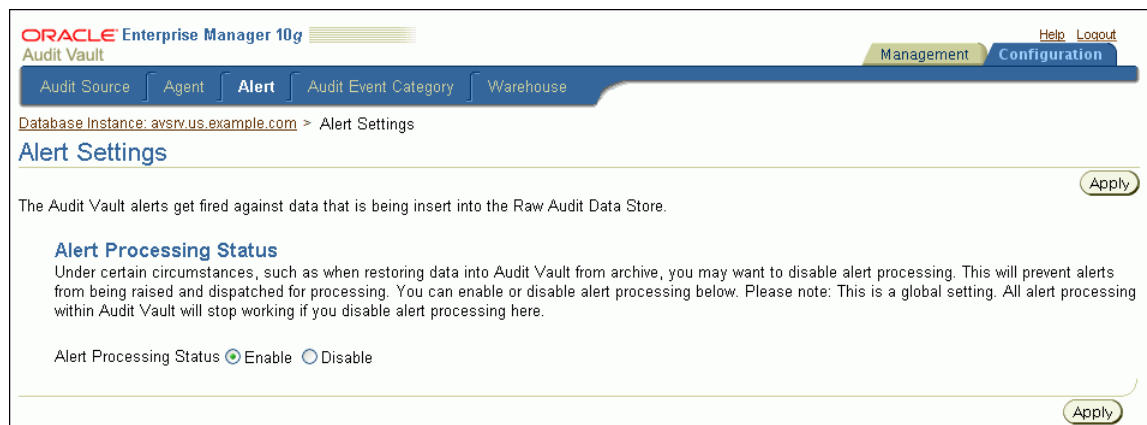
To globally disable and enable alerts:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Configuration** tab, and then select the **Alert** subpage.

The Alert Settings page appears.



3. At the Alert Processing Status label, select either **Disable** or **Enable**.
4. Click **Apply**.

3.2.6 Viewing Audit Event Categories

Audit event category management consists of viewing the Oracle Audit Vault audit event categories, their attributes, and their audited events. An audit event category defines how various types of events are organized. For example, invalid records are placed in the Invalid Record event category. See *Oracle Audit Vault Auditor's Guide* for more information about audit event categories.

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.
See [Section 3.2.3](#) for login instructions.
2. Select the **Configuration** tab, and then select the **Audit Event Category** subpage.
The Audit Event Category Management page appears.
3. Select an audit event category, and then click **View** to find detailed information about that category.
The View Audit Event Category page appears.
4. From the **Audit Source Type** list, select from the available source types: **ORCLDB**, **MSSQLDB**, **SYBDB**, and **DB2DB**.
5. Select the **Attributes** or **Audit Events** subpages to view detailed information about these categories.
6. Click **OK** when you complete viewing the audit event information for the category you selected.

[Figure 3–1](#) shows the Audit Event Category Management page.

Figure 3–1 Audit Event Category Management Page

Oracle Enterprise Manager 10g
Audit Vault

Management Configuration

Audit Source Agent Alert **Audit Event Category** Warehouse

Database Instance: avsrv.us.example.com > Audit Event Category Management

Logged in As TJONES

Audit Event Category Management

Audit Source Type: ORCLDB

View

Select	Audit Event Category	Audit Event Category Description	Format Name
<input checked="" type="radio"/>	ACCOUNT MANAGEMENT	Management of user and service accounts and profiles	AV_AUDIT_RECORD_ORCLDB
<input type="radio"/>	USER SESSION	Creation and use of user sessions on the system	AV_AUDIT_RECORD_ORCLDB_US
<input type="radio"/>	OBJECT MANAGEMENT	Creation and management of data items and resource elements	AV_AUDIT_RECORD_ORCLDB_OM
<input type="radio"/>	SYSTEM MANAGEMENT	Management of services which are system level	AV_AUDIT_RECORD_ORCLDB
<input type="radio"/>	APPLICATION MANAGEMENT	Management of applications or code on a system	AV_AUDIT_RECORD_ORCLDB_AM
<input type="radio"/>	ROLE AND PRIVILEGE MANAGEMENT	Management of roles and privileges granted to users or services	AV_AUDIT_RECORD_ORCLDB_RP
<input type="radio"/>	DATA ACCESS	Association with a data item or resource for its content or services	AV_AUDIT_RECORD_ORCLDB_DA
<input type="radio"/>	SERVICE AND APPLICATION UTILIZATION	Use of service or applications	AV_AUDIT_RECORD_ORCLDB
<input type="radio"/>	PEER ASSOCIATION	Management of association with peer systems	AV_AUDIT_RECORD_ORCLDB
<input type="radio"/>	AUDIT	Management of Audit service	AV_AUDIT_RECORD_ORCLDB_AUDIT

Previous 1-10 of 14 Next 4

View

On the **Audit Event Category Management** page, audit event categories appear in a table with the following columns:

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

3.2.7 Viewing Operational Errors That Oracle Audit Vault Catches

You can use the Audit Vault Console to view operational errors that Oracle Audit Vault catches, such as broken database connections and missing files.

To view errors using Oracle Audit Vault:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Management** tab, and then select the **Audit Errors** subpage.

The Audit Errors page appears.

3. After the Error Time label, specify a time range of errors to view.

Select from the **Last 24 Hours**, **Last One Week**, or **Last One Month** options to view errors from those times, or select **The Period** and then enter a start date in the **From** field and end date in the **To** field to specify a different time range.

4. Click **Go**.

[Figure 3–2](#) shows the Audit Errors page with audit errors from the last 24 hours.

Figure 3–2 Audit Errors Page

ORACLE Enterprise Manager 10g
Audit Vault

Management Configuration

Collectors Agents **Audit Errors** Warehouse

Database Instance: avsrus.example.com > Audit Error History

Logged in As TJONES

Audit Errors

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

☐ The Period From To

Error Time	Audit Source	Collector	Module	Message
2008-04-10 19:43:35	orcl1	DBAUD_Collector	zaac	Some rows may have been missed by Audit Vault or may be duplicated
2008-04-10 14:14:19	orcl1	DBAUD_Collector	zaac	On line 7521: ORA-12528: TNS:listener: all appropriate instances are blocking new connections
2008-04-10 14:14:17	orcl1	DBAUD_Collector	zaac	On line 2293: ORA-01089: immediate shutdown in progress - no operations are permitted
2008-04-10 14:14:17	orcl1	OSAUD_Collector	zaodrOCIError	OCI error encountered for source database orcl1 access, audit trail cleanup support disabled.

The **Audit Errors** page displays error information as a table with the following column headings:

- **Error Time:** Local time when the audit error was generated
- **Audit Source:** The audit source database 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

3.3 Altering Collector Properties and Attributes

This section contains:

- [About Collector Properties and Attributes](#)
- [Altering Collector Properties and Attributes Using the Audit Vault Console](#)
- [Altering Collector Properties and Attributes from a Command Line](#)

3.3.1 About Collector Properties and Attributes

After you add a collector to a database source, Oracle Audit Vault creates the collector with a set of default properties that are internal to Oracle Audit Vault. They have no effect on the source database. These properties control aspects such as the frequency of audit data collection from the source database, the name of the source database, and so on.

3.3.2 Altering Collector Properties and Attributes Using the Audit Vault Console

To alter collector properties and attributes using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Configuration** tab, and then select the **Audit Source** subpage.

The Source Configuration Management page appears.

3. Select the **Collector** subpage.

The Collector Configuration Management page appears, which displays the current settings for the available collectors.

4. Select the collector that you want to modify, and then click the **Edit** button.

The Edit Collector page appears.

5. Under Attributes, modify the attributes for the collectors by editing the values in the Value column.

For more information about these attributes, see the following sections:

- [Section 8.4](#) for the Oracle Database collector attributes
- [Section 9.4](#) for the SQL Server collector attributes
- [Section 10.4](#) for the Sybase ASE collector attributes
- [Section 11.4](#) for the IBM DB2 collector attributes

6. Click **OK**.

7. Restart the collector.

Return to the **Collectors** subpage, select the collector from the list, and click the **Stop** button. Then click **Start** to restart the collector.

3.3.3 Altering Collector Properties and Attributes from a Command Line

To alter collector properties from a command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).

- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
- 2. Run the `alter_collector` command for each collector type, as shown in the following examples:

For Oracle Database:

```
avorcldb alter_collector -srcname ORCL -collname DBAUD_Collector AUDAUDIT_
DELAY_TIME=60
```

See [Section 8.4](#) for more information about the `avorcldb alter_collector` command.

For Microsoft SQL Server:

```
avmssqldb alter_collector -srcname mssqlldb4 -collname MSSQLCollector NO_OF_
RECORDS=1500 DESCRIPTION="MSSQLDB collector 45" SERVERSIDE_TRACE_
FILEPATH="c:\SQLAuditFile*.trc"
```

See [Section 9.4](#) for more information about the `avmssqldb alter_collector` command.

For Sybase ASE:

```
avsybdb alter_collector -srcname sybdb4 -collname SybaseCollector
NO_OF_RECORDS=1500 DESCRIPTION="Sybase collector 45"
```

See [Section 10.4](#) for more information about the `avsybdb alter_collector` command.

For IBM DB2:

```
avdb2db alter_collector -srcname db2db4 -collname DB2Collector
NO_OF_RECORDS=1500 DESCRIPTION="IBM DB2 collector 95"
```

See [Section 11.4](#) for more information about the `avdb2db alter_collector` command.

- 3. Restart the collector.

In the Audit Vault Server shell, run commands similar to the following:

```
avctl stop_collector -collname DBAUD_Collector -srcname ORCL
avctl start_collector -collname DBAUD_Collector -srcname ORCL
```

See [Section 7.14](#) for more information about `avctl stop_collector` and [Section 7.11](#) for information about `avctl start_collector`.

3.4 Managing the Oracle Audit Vault Data Warehouse

This section contains:

- [About Managing the Oracle Audit Vault Data Warehouse](#)
- [Setting the Audit Vault Data Warehouse Retention Period](#)
- [Loading Data to the Oracle Audit Vault Data Warehouse](#)
- [Purging Data from the Oracle Audit Vault Data Warehouse](#)

3.4.1 About Managing the Oracle Audit Vault Data Warehouse

The collectors collect audit data from their source databases and send it to the Oracle Audit Vault repository. The repository stores the data in an internal format. This repository also contains a data warehouse, which is automatically refreshed with the latest audit records. Oracle Audit Vault provides predefined reports that display the data in the warehouse to the auditor.

You can perform the following activities with the Oracle Audit Vault data warehouse:

- **Set a retention period for the data that has been refreshed.** The data warehouse then contains the most recent data for that length of time.
- **Load older data from the raw audit data store into the data warehouse tables.** You can load older data into the data warehouse so that it can be available for analysis in the Oracle Audit Vault reports. However, you cannot load data from outside sources—just data that has been previously collected by the collectors but is too old to be loaded into the data warehouse as part of a normal refresh.
- **Purge audit data.** If you load older audit data into the warehouse, you can purge it from the data warehouse. Oracle Audit Vault still maintains this data in the Audit Vault repository but does not make it available for analysis in the warehouse.

3.4.2 Setting the Audit Vault Data Warehouse Retention Period

This section contains:

- [About Setting a Retention Period](#)
- [Creating a Retention Period Using the Audit Vault Console](#)
- [Creating a Retention Period from a Command Line](#)

3.4.2.1 About Setting a Retention Period

Oracle Audit Vault initially inserts audit data from the databases into a **raw audit data store** (that is, the internal format) as well as into the data warehouse so that it can be made available for the Oracle Audit Vault reports. As an AV_ADMIN user, you can specify how long the audit data should remain in the warehouse tables for online reporting. You can set a retention period that determines the content of an Audit Vault report.

For example, suppose on August 19, 2009, you set the warehouse retention period for 1 year. One month later, the retention period will have shifted forward: Now the data warehouse contains audit data from September 19, 2008 to September 19, 2009. Using a nightly job, Oracle Audit Vault then deletes the audit data from the warehouse tables used by the reports before September 19, 2008, because now it is older than the retention period. This way, you always have the most recent year of audit data, right up to the current time. The AV_AUDITOR user can specify the retention period for the raw audit data store. When audit records are deleted from the warehouse, a compressed copy of the audit data remains in the repository that may be reloaded in back into the warehouse for future reporting needed.

You can create a retention period from either the Audit Vault Console or at a shell or command prompt by using the AVCA utility.

See Also:

- *Oracle Audit Vault Auditor's Guide* for more information about the raw audit data store in the Audit Vault data warehouse schema
- [Section 3.4.3](#) for information about loading audit data to the Audit Vault data warehouse
- [Section 3.4.4](#) for information about purging audit data from the Audit Vault data warehouse

3.4.2.2 Creating a Retention Period Using the Audit Vault Console

To create the retention period using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Configuration** tab, and then select the **Warehouse** subpage.

The Warehouse Settings page appears.

ORACLE Enterprise Manager 10g

Audit Vault

Management Configuration

Audit Source Agent Alert Audit Event Category Warehouse

Database Instance: avsrv.us.example.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.

Revert Apply

Retention Time
Specify the size of the warehouse window.

Retention Time * Year * Months

Revert Apply

3. Set the retention window, that is, the period of time during which the data sent to the Oracle Audit Vault data warehouse remains in storage.

For example, suppose that you want to keep the audit data in storage for the next year and a half. To do so, you would enter 1 in the **Year** field and 6 in the **Months** field.

4. Click **Apply**.

3.4.2.3 Creating a Retention Period from a Command Line

To create a retention period from a command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avca set_warehouse_retention` command to set the retention period.

For example, to specify a period of 1 year and 6 months, enter the following command:

```
avca set_warehouse_retention -intrv +01-06
```

See [Section 6.24](#) for more information about the `avca set_warehouse_retention` command.

3.4.3 Loading Data to the Oracle Audit Vault Data Warehouse

This section contains:

- [About Loading Data into the Oracle Audit Vault Warehouse](#)
- [Loading Data Warehouse Data Using the Audit Vault Console](#)
- [Loading Data Warehouse Data from a Command Line](#)

3.4.3.1 About Loading Data into the Oracle Audit Vault Warehouse

You can load data that is older than the retention period from the [raw audit data store](#) into the Oracle Audit Vault data warehouse tables. After you load this data, it is available to auditors to generate reports or perform analysis.

To find the current retention period setting, view the Warehouse Settings page of the Audit Vault Console (see [Section 3.4.2](#)).

3.4.3.2 Loading Data Warehouse Data Using the Audit Vault Console

To load the data warehouse data using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.

See [Section 3.2.3](#) for login instructions.

2. Optionally, disable the alert settings.

See [Section 3.2.5](#) for more information.

3. Select the **Management** tab, and then select the **Warehouse** subpage.

The Warehouse Activity page appears.

4. Select the **Load Activity** subpage.

The Load Activity page appears.

ORACLE Enterprise Manager 10g
Audit Vault

Management Configuration

Collectors Agents Audit Errors Warehouse

Database Instance: avsvr.us.example.com > Load Activity

Logged in As TJONES

Warehouse Activity

Load raw audit data from any period of time into the Audit Vault Warehouse. You can then run reports against this data. If it is historical data needed mainly for ad-hoc reporting purposes, you will probably want to purge the data when done using it.

Refresh Activity Load Activity Purge Activity

* Start Date Specify the starting date from which to load data. * Number of Days Load Now

Scheduled	Start Time	Duration(Minutes)	CPU Used	Error Number	Message	Status
2008-08-06 11:20:10	2008-08-06 11:20:10	0 0 0:19.0	0 0 0:1.690000000	0		SUCCEEDED

5. In the **Start Date** field, enter the beginning date of the data that you want to load. For example, suppose the source database contains audit data that is 10 years old, and you want to load the last 5 years worth of audit data into the Oracle Audit Vault data warehouse. Assuming that today's date is August 8, 2008, you would specify August 8, 2003 as the start date.

6. In the **Number of Days** field, enter the number of days, starting from the start date, through which you want to load data.

7. Click the **Load Now** button.

Oracle Audit Vault schedules the data load operation, which is listed on this page the next time you access it.

8. Reenable the alert settings if you had disabled them.

See [Section 3.2.5](#) for more information.

3.4.3.3 Loading Data Warehouse Data from a Command Line

To load the data warehouse data from a command line:

1. Optionally, disable the alert settings.

See [Section 3.2.5](#) for more information.

2. Open a shell or command prompt for the Audit Vault Server.

- **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

3. Run the `avctl load_warehouse` command.

For example, to load 10 days of audit data that was recorded starting on August 8, 2003, enter the following command:

```
avctl load_warehouse -startdate 08-AUG-03 -numofdays 10
```

See [Section 7.2](#) for more information about the `avctl load_warehouse` command.

4. Reenable the alert settings if you had disabled them.

See [Section 3.2.5](#) for more information.

3.4.4 Purging Data from the Oracle Audit Vault Data Warehouse

This section contains:

- [About Purging the Oracle Audit Vault Data Warehouse](#)
- [Purging Data Warehouse Data Using the Audit Vault Console](#)
- [Purging Data Warehouse Data from a Command Line](#)

3.4.4.1 About Purging the Oracle Audit Vault Data Warehouse

When you no longer need the audit data that you have loaded into Audit Vault Server using the `avctl load_warehouse` command for reporting, you can remove it from the Oracle Audit Vault data warehouse. If in the future you decide that you need to run reports against this purged data, follow the instructions in [Section 3.4.3](#) to reload the necessary data into the data warehouse.

3.4.4.2 Purging Data Warehouse Data Using the Audit Vault Console

To purge the data warehouse data using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_ADMIN` role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Management** tab, and then select the **Warehouse** subpage.
The Warehouse Activity page appears.
3. Select the Purge Activity page.
The Purge Activity subpage appears.
4. In the **Start Date** field, enter the beginning date of the data that you want to purge.
5. In the **Number of Days** field, enter the number of days, starting from the start date, through which you want to purge data.
6. Click the **Purge Now** button.
Oracle Audit Vault schedules the data purge operation, which is listed on this page the next time you access it.

3.4.4.3 Purging Data Warehouse Data from a Command Line

To purge the data warehouse data from a command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avctl purge_warehouse` command.

For example, to purge 10 days of audit data that was recorded starting on January 1, 2004, and to specify that the operation wait until the previous purge job completes, enter the following command:

```
avctl purge_warehouse -startdate 01-JAN-04 -numofdays 10 -wait
```

See [Section 7.3](#) for more information about the `avctl purge_warehouse` command.

3.5 Altering Source Database Attributes

This section contains:

- [About Source Database Attributes](#)
- [Altering Source Database Attributes Using the Audit Vault Console](#)
- [Altering Source Database Attributes from a Command Line](#)

3.5.1 About Source Database Attributes

After you register a source database, Oracle Audit Vault creates a set of properties that reflect general aspects of the source database itself, such as its port number and IP address. These properties are internal to Oracle Audit Vault and have no effect on the source database.

3.5.2 Altering Source Database Attributes Using the Audit Vault Console

To alter the source database attributes using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_ADMIN` role.

See [Section 3.2.3](#) for login instructions.

2. Select the **Configuration** tab, and then select the **Audit Source** subpage.

The Source Configuration Management page appears.

3. Select the **Source** subpage.

The Source Configuration Management page displays the current settings for the available collectors.

ORACLE Enterprise Manager 10g
Audit Vault

Management Configuration

Audit Source Agent Alert Audit Event Category Warehouse

Database Instance: avsvr.us.example.com > Source Configuration Management

Logged in As TJONES

Source Configuration Management

Source Collector

Source Type

Source Go

View Edit Delete

Select	Audit Source Type	Source	Host	Host IP	Version	Audit Source Description
<input checked="" type="radio"/>	ORCLDB	orcl1	nemo.us.example.com	192.0.2.1	10.2.0.3.0	Oracle DB
<input type="radio"/>	SYBDB	sybasease1	binks.us.example.com	192.0.2.25	15.0.2	Sybase ASE DB
<input type="radio"/>	MSSQLDB	mssqlserver1	jules.us.example.com	192.0.2.21	2005	MS SQL Server DB

Source Collector

4. Select the source database that you want to modify, and then click the **Edit** button.

The Edit Source page appears.

5. Under Properties, optionally modify the description of the source database.
6. Under Attributes, modify the attributes for the source database by editing the values in the **Value** column.

For more information about these attributes, see the following sections:

- [Section 8.5](#) for the Oracle Database source database attributes
- [Section 9.5](#) for the SQL Server source database attributes
- [Section 10.5](#) for the Sybase ASE source database attributes
- [Section 11.5](#) for the IBM DB2 source database attributes

7. Click **OK**.

3.5.3 Altering Source Database Attributes from a Command Line

To alter source database attributes from a command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

2. Run the `alter_source` command for each source database type, as shown in the following examples.

For Oracle Database:

```
avorcldb alter_source -srcname ORCL PORT=1522
```

See [Section 8.5](#) for more information about the `avorcldb alter_source` command.

For Microsoft SQL Server:

```
avmssqldb alter_source -srcname mssqldb4 DESCRIPTION="HR Database"
```

See [Section 9.5](#) for more information about the `avmssqldb alter_source` command.

For Sybase ASE:

```
avsybdb alter_source -srcname sybdb4 DESCRIPTION="HR Database"
```

See [Section 10.5](#) for more information about the `avsybdb alter_source` command.

For IBM DB2:

```
avdb2db alter_source -srcname db2db4 DESCRIPTION="HR Database"
```

See [Section 11.5](#) for more information about the `avdb2db alter_source` command.

3.6 Configuring E-Mail Notifications

This section contains:

- [About E-Mail Notification Usage with Oracle Audit Vault](#)
- [Configuring the E-Mail Notification Service](#)

3.6.1 About E-Mail Notification Usage with Oracle Audit Vault

You can configure Oracle Audit Vault to send users e-mail notifications when Audit Vault alerts are generated. The e-mail notifications can be sent in text format to mobile devices, or routed through an SMS gateway if you already have one.

Note the following:

- You can configure one SMTP (or ESMTP) server for each Oracle Audit Vault installation.
- You can configure Oracle Audit Vault to work with both unsecured SMTP servers as well as secured and authenticated SMTP servers.

After you have configured the e-mail notification service, then an Oracle Audit Vault auditor can configure the Audit Vault to generate e-mail alerts.

See Also:

- [Chapter 6, "Audit Vault Configuration Assistant \(AVCA\) Reference"](#) for e-mail notification commands (search for `smtp`)
- [Section 7.8](#) (`avctl show_smtp_status` command)

3.6.2 Configuring the E-Mail Notification Service

To configure the e-mail notification service:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Register the SMTP server details that your e-mail server uses.

For example, to register an SMTP server that requires authentication:

```
avca register_smtp -server 192.0.2.8:2223 -sender_id ikuksa -sender_email
ima.kuksa@example.com -auth
```

```
Enter user: idaneau
Enter password: password
Re-enter password: password
```

In this example:

- `-server`: Enter either the IP address or host name of the server, and its port number.
- `-sender_id`: Enter the name of the user on whose behalf the Oracle Audit Vault e-mail alerts will be sent.
- `-sender_email`: Enter the e-mail ID of the user on whose behalf the e-mail alerts will be sent.
- `-auth`: Enter either `-auth` to indicate that the SMTP server requires authentication, or enter `-noauth` to indicate the SMTP needs no authentication.
- `Enter user`: Enter the name of the user with which to connect to SMTP Server.
- `Enter password` and `Re-enter password`: Enter the password of the user with which to connect to the SMTP server.

See [Section 6.17](#) for detailed information about the `avca register_smtp` command.

3. If the SMTP server is a secure server, then specify the type of protocol it uses and optionally, the truststore to validate the server certificate chain.

For example, to register an SMTP server that requires transport layer security (TLS) authentication:

```
avca secure_smtp -protocol tls -truststore $ORACLE_HOME/wallets/smtp_keystore
```

In this example:

- `-protocol`: Enter the protocol type. Acceptable values are SSL (Secure Sockets Layer) or TLS (Transport Layer Security). These values are case insensitive.
- `-truststore`: Enter the directory path to the truststore used to validate the server certificates.

See [Section 6.22](#) for detailed information about the `avca secure_smtp` command.

4. Optionally, test the configuration by trying to send an e-mail notification to a user in your network.

For example:

```
avca test_smtp -to idaneau@example.com
```

In this example, user Ida Neau should receive an e-mail similar to the following:

- **Subject header:** Oracle Audit Vault: Test Message
- **Body text:** This is a test message from Oracle Audit Vault

If the test fails, then check the configuration and status by running the `avca show_smtp_config` (Section 6.27) and `avctl show_smtp_status` (Section 7.8) commands. You can recreate the configuration by using the `avca alter_smtp` command (Section 6.3).

3.7 Configuring Oracle Audit Vault for the Remedy Trouble Ticket System

This section contains:

- [About Using the Remedy Trouble Ticket System with Oracle Audit Vault](#)
- [Configuring the Remedy Trouble Ticket Server Connection](#)

3.7.1 About Using the Remedy Trouble Ticket System with Oracle Audit Vault

You can configure Oracle Audit Vault to connect to BMC Remedy Action Request (AR) System Server 7.x. This connection enables Oracle Audit Vault auditors to raise trouble tickets in response to Audit Vault alerts. You can configure one Remedy server for each Oracle Audit Vault installation. After you have configured this connection, an Audit Vault auditor can create templates and the necessary configuration to handle the details of the alert.

See Also:

- [Chapter 6, "Audit Vault Configuration Assistant \(AVCA\) Reference"](#) for Remedy trouble ticket configuration commands (search for `remedy`)
- [Section 7.7](#) (`avctl show_remedy_status` command)

3.7.2 Configuring the Remedy Trouble Ticket Server Connection

To configure Oracle Audit Vault to connect to the Remedy trouble ticket server:

1. Make a copy of the `remedy.properties.tmpl` descriptor properties file, which by default is located in the `$ORACLE_HOME/av/conf` directory of the Audit Vault Server.
2. Modify the `remedy.properties.tmpl` descriptor properties file.

Follow the instructions in the file to change the appropriate settings, and then save the file. You can store the file in any location within the Audit Vault Server.

3. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

4. Run the `avca register_remedy` command to register the BMC Remedy Action Request System server with Oracle Audit Vault.

For example:

```
avca register_remedy -config $ORACLE_HOME/av/conf/remedy.properties
```

The change takes place right away. You do not need to restart the Audit Vault Server.

5. If the BMC Remedy Action Request System Server is on a secure server, then run the following command:

```
avca secure_remedy -truststore $ORACLE_HOME/wallets/remedy_keystore
```

See [Section 6.21](#) for more information.

6. Optionally, test the configuration by using an existing Remedy trouble ticket number.

You can use any trouble ticket number in the Remedy system.

For example:

```
avca test_remedy -ticket_id INC0000000000010
```

If the test is successful, then the `avca test_remedy` command displays a summary of the trouble ticket's fields. If the test fails, then check the configuration and status by running the `avca show_remedy_config` ([Section 6.25](#)) and `avctl show_remedy_status` ([Section 7.7](#)) commands. You can recreate the configuration by using the `avca alter_remedy` command ([Section 6.2](#)).

3.8 Removing Source Databases from Oracle Audit Vault

This section contains:

- [About Removing Source Databases from Oracle Audit Vault](#)
- [Removing a Source Database Using the Audit Vault Console](#)
- [Removing a Source Database from a Command Line](#)

3.8.1 About Removing Source Databases from Oracle Audit Vault

If you no longer need to have a source database registered with Oracle Audit Vault, you can use either the Audit Vault Console or the command-line utilities to remove the source database from Oracle Audit Vault. After you have removed the source database, its audit data still resides in the data warehouse within its retention period. To purge this audit data, see [Section 3.4.4](#). You can check the length of the retention period in the Audit Vault Console; see [Section 3.4.2](#).

Remember that after you have removed a source database, its identity data remains in Oracle Audit Vault so that there will be a record of source databases that have been dropped. Therefore, you cannot add a new source database with the name of a dropped source database. Remove the source database only if you no longer want to collect its data or if it has moved to a new host computer.

3.8.2 Removing a Source Database Using the Audit Vault Console

To remove a source database from Oracle Audit Vault using the Audit Vault Console:

1. Log in to the Audit Vault Console as a user who has been granted the AV_ADMIN role.
See [Section 3.2.3](#) for login instructions.
2. Select the **Configuration** tab, and then select the **Audit Source** subpage.
The Source Configuration Management subpage appears.
3. From the list of source databases, select the database that you want to remove, and then click **Delete**.
You can search for a source database by entering data in the **Source Type** and **Source** fields.
4. Click **Yes** in the Confirmation window.

3.8.3 Removing a Source Database from a Command Line

To remove a source database from Oracle Audit Vault from a command line:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `drop_source` command for the source database, as shown in the following examples:

For Oracle Database:

```
avorcldb drop_source -srcname ORCL
```

See [Section 8.7](#) for more information about the `avorcldb drop_source` command.

For Microsoft SQL Server:

```
avmssqldb drop_source -srcname mssql4
```

See [Section 9.7](#) for more information about the `avmssqldb drop_source` command.

For Sybase ASE:

```
avsybdb drop_source -srcname sybdb4
```

See [Section 10.7](#) for more information about the `avsybdb drop_source` command.

For IBM DB2:

```
avdb2db drop_source -srcname db2db4
```

See [Section 11.7](#) for more information about the `avdb2db drop_source` command.

Administering the Oracle Audit Vault Repository

This chapter contains:

- [About the Administrative Tasks in This Chapter](#)
- [Monitoring the Audit Vault Server SYSAUX Tablespace Space Usage](#)
- [Monitoring Audit Vault Server Archive Log Disk Space Usage](#)
- [Monitoring the Audit Vault Server Flash Recovery Area](#)
- [Managing Oracle Audit Vault Backup and Recovery Operations](#)
- [Managing the Audit Vault Console in an Oracle RAC Configuration](#)
- [Using a Collection Agent to Listen to Oracle RAC Nodes](#)
- [Configuring Collection Agent Connectivity for Oracle RAC](#)
- [Changing the Port Numbers Used by Oracle Audit Vault](#)
- [Purging the Oracle Source Database Audit Trail](#)
- [Purging the Oracle Audit Vault Repository Audit Trail](#)

4.1 About the Administrative Tasks in This Chapter

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

4.2 Monitoring the Audit Vault Server SYSAUX Tablespace Space Usage

The Oracle Audit Vault Server database contains the SYSAUX tablespace, which by default has one data file. The SYSAUX tablespace is a locally managed tablespace with automatic segment space management.

You should monitor the space usage for the SYSAUX tablespace and create additional data files for storage as needed. Remember that if you use the procedures in [Section 4.10](#) to clean up the audit trail, the SYSAUX tablespace by default will store the audit trail.

See *Oracle Database Administrator's Guide* for more information about the ALTER TABLESPACE SQL statement, which you can use to add more storage data files. For information about optimizing a tablespace, see *Oracle Database Performance Tuning Guide*.

4.3 Monitoring Audit Vault Server Archive Log Disk Space Usage

By default, ARCHIVELOG mode is enabled in the Audit Vault Server database. The ARCHIVELOG mode copies filled online redo logs to disk. This enables you to back up the database while it is open and being accessed by users, and to recover the database to any desired point in time. You should monitor the disk space usage for the redo logs.

See *Oracle Database Administrator's Guide* for more information about changing the LOG_ARCHIVE_DEST_# 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*.

4.4 Monitoring the Audit Vault Server Flash Recovery Area

By default, the Audit Vault Server database has the following initialization parameter settings:

- The DB_RECOVERY_FILE_DEST_SIZE initialization parameter is set to 2 GB.
- The DB_RECOVERY_FILE_DEST initialization parameter is set to the default flash recovery area, typically the `ORACLE_HOME/flash_recovery_area` directory.

Ensure that the size of the flash recovery area is large enough to hold a copy of all data files, all incremental backups, online redo logs, archived redo logs not yet backed up on tape, control files, and control file auto backups. This space can fill up quickly, depending on the number of collectors configured, the scope of the audit record collection being administered, and the backup and archive plans that you have in place.

You can use Oracle Enterprise Manager Database Control to monitor the available space in the flash recovery area. Monitor the percent space that is usable in the Usable Flash Recovery Area field under the High Availability section on the Home page. Check the alert log in the Database Console for messages. When the used space in the flash recovery area reaches 85 percent, a warning message is sent to the alert log. When the used space in the flash recovery area reaches 97 percent, a critical warning message is sent to the alert log.

You can manage space in the flash recovery area by adjusting the retention policy for data files to keep fewer copies or reduce the number of days these files stay in the recovery window. Alternatively, increase the value of the DB_RECOVERY_FILE_DEST_SIZE initialization parameter to accommodate these files and to set the DB_RECOVERY_FILE_DEST initialization parameter to a value where more disk space is available. See *Oracle Database Administrator's Guide* and *Oracle Database Backup and Recovery Basics* for more information.

4.5 Managing Oracle Audit Vault Backup and Recovery Operations

When you back up Oracle Audit Vault, you must back up the database, the Audit Vault Server home, and the Audit Vault collection agent home.

This section contains:

- [Backing Up the Database](#)
- [Backing Up Audit Vault Server Home and Audit Vault Collection Agent Home](#)

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

4.5.1 Backing Up the Database

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. Log in to Oracle Recovery Manager (RMAN):

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

2. Issue the following RMAN commands:

```
BACKUP DATABASE FORMAT 'some_backup_directory%U' TAG before_upgrade;
BACKUP CURRENT CONTROLFILE TO 'save_controlfile_location';
```

4.5.2 Backing Up Audit Vault Server Home and Audit Vault Collection Agent Home

Back up or copy the Audit Vault Server home and the Audit Vault collection agent home to separate directories.

4.6 Managing the Audit Vault Console in an Oracle RAC Configuration

When you can deploy the Oracle Audit Vault Server in an Oracle RAC configuration, the repository database can take advantage of the scalability and high availability features provided by Oracle RAC. However, the Audit Vault Console is not Oracle RAC-aware, and can only run on one node in the Oracle RAC environment. Usually, this is the node on which the first instance of Oracle Audit Vault was installed. In the event that this node becomes unavailable, the Console does not automatically fail over to another node as the repository database does. As a result, the Audit Vault Console application is no longer available to users. To remedy this problem, you must manually bring up the Audit Vault Console on another node in the Oracle RAC cluster.

To bring up the Audit Vault Console on another node in the Oracle RAC cluster:

1. Ensure that the Audit Vault Console is not running on the main node.

Because the node is inaccessible, this should be the case anyway. To check, run the `avctl show_av_status` command, described in [Section 7.5](#).

2. Open a shell or command prompt for the Audit Vault Server.

- **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

3. Run the `avca deploy_av` command to deploy the Audit Vault Console in the Oracle home.

For example:

```
avca deploy_av -sid av -dbalias av -avconsoleport 5700
```

See [Section 6.6](#) for more information about the `avca deploy_av` command.

4. Restore the wallet.

For each source database that has been registered with Oracle Audit Vault, Audit Vault uses a user name and password pair to connect to it. These user names and passwords are stored in an Oracle wallet on the Audit Vault Server. You can find the wallet in the `$ORACLE_HOME/network/admin/avwallet` directory. If you have the wallet from the original node backed up, restore it into this directory on the new node.

4.7 Using a Collection Agent to Listen to Oracle RAC Nodes

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

For the OSAUD and DBAUD collectors, you must update the `tnsnames.ora` file during installation of the Audit Vault collection agents.

After you configure the collection agent, the `tnsnames.ora` file located in `$ORACLE_HOME/network/admin` has an alias similar to the following:

```
AV =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = node01) (PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = avsrv.example.com)))
```

For high availability, you may need to edit the Audit Vault collection agent home `tnsnames.ora` file after you have configured the collection agent, and then 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 = avsrv.example.com)
    )
  )
```

For the REDO collector, you must log in using the source user account at the source database and then re-create the database link for `avsrv.example.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.

Follow these guidelines for OSAUD and DBAUD collectors:

- **Configuring OSAUD collectors.** You must create an OSAUD collector for each Oracle RAC node. If you have a shared file system, then ensure that files from one node be kept in a separate directory than those from another node.
- **Configuring DBAUD collectors.** You only need one DBAUD collector to manage all the Oracle RAC nodes. If the Oracle RAC source database is configured for failover and if one or more Oracle RAC nodes fails, then the collectors should continue to work without problems so long as at least one Oracle RAC node is working. However, if the computer where the DBAUD collector resides fails, then you can use the `avorcldb alter_collector` command ([Section 8.4](#)) to move the DBAUD collector to a different Oracle RAC node.

Be aware that this automatic failover configuration works only if you have added the source database with the host name or IP address of the virtual IP address, not of each individual database instance. Suppose you have host `hosta.example.com` at `192.0.2.100`, and host `hostb.example.com` at

192.0.2.101, and they are part of a cluster. The virtual IP address of the cluster is configured to 192.0.2.200, and the host name for that IP is `cluster.example.com`. In that case, you must run the `avorcldb add_source -src cluster.oracle.com:1521:..` command (See [Section 8.3](#)) to add the source database. With this method, failover is automatic. If, instead, you use `hosta.example.com` or `hostb.example.com`, then failover configuration will not work.

Another way to handle this configuration is to add the source database with `hosta.oracle.com`, but then you must change the `TNSNAMES.ORA` file on the Audit Vault Server and the agent managing your DBAUD collector. In addition, you must add `hostb.oracle.com` as another address for the same TNS alias as `hosta.oracle.com`. This method enables the collector to failover when one of the hosts is disabled.

4.8 Configuring Collection Agent Connectivity for Oracle RAC

When you add an Oracle source database to Oracle Audit Vault, you must provide the `host:port:service` information for the source database being added. This information is used for the following tasks from the collection 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 computer goes down, the connectivity to the source database from the Oracle Audit Vault collection agent is broken. Any attempt to perform these tasks is unsuccessful because this connection is not available:

You can do any or all of the following operations to make the connection between the source and the Audit Vault collection agent more highly available.

- **In the Audit Vault collection agent home, update the `tnsnames.ora` file to include additional host or port information for the service.** This file is located in the `$ORACLE_HOME/network/admin` directory. You can add options for load balancing and failure in the connect string. For additional information, see *Oracle Database Net Services Administrator's Guide*.
- **Configure a listener on the Oracle RAC nodes to support connecting to remote nodes and configuring the Oracle Database to communicate with remote listeners.** If 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*.
- **Provide host information using the virtual IP address of the node instead of the physical IP address.** If the host computer goes down, then all traffic to the host is redirected to a different node.

4.9 Changing the Port Numbers Used by Oracle Audit Vault

This section contains:

- [Changing Port Numbers for the Audit Vault Server](#)
- [Changing Port Numbers for the Audit Vault Collection Agents](#)
- [Changing Port Numbers for the Oracle Source Database](#)

4.9.1 Changing Port Numbers for the Audit Vault Server

This section contains:

- [Changing the Audit Vault Server Listener Port Number](#)
- [Changing the Audit Vault Console HTTP Port Number](#)
- [Changing the Oracle Enterprise Manager Database Control Port Number](#)
- [Changing the Audit Vault PL/SQL Gateway Port Number](#)

4.9.1.1 Changing the Audit Vault Server Listener Port Number

Changing the port numbers for the Audit Vault Server affects the agents, collectors, the Audit Vault Console Web application, and the Audit Vault command line utilities.

First, update and test the `listener.ora` and `tnsnames.ora` files for the Audit Vault Server, as follows:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.

2. Stop the collection agent.

For collection agents that were created in Release 10.2.3.2:

```
avctl stop_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl stop_oc4j
```

Leave this shell or command prompt open.

3. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
4. Stop the collector.

```
avctl stop_collector -collname collector_name -srcname source_name
```
5. Stop the Audit Vault Console.

```
avctl stop_av
```
6. Stop the listener on the server side.

```
lsnrctl stop listener_name
```
7. On the server side, manually edit the `listener.ora` and `tnsnames.ora` files in `$ORACLE_HOME/network/admin` on the server to use the new port number.

If the port number that you want to set is not 1521, then do the following:

- Verify that the `$ORACLE_HOME/network/admin/tnsnames.ora` file contains an entry for the listener. This entry is as follows; make a note of the `listener_name` value:

```
listener_name =  
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=hostname) (PORT=newport)))
```


- Verify that the `local_listener` parameter in the database is set to the listener name that is defined in your `tnsnames.ora` file. This step ensures that the database and related services are registered with the listener.
- 8. On the server side, restart the listener.


```
lsnrctl start listener_name
```
- 9. Edit the `emoms.properties` file in the `$ORACLE_HOME/hostname_sid/sysman/config` directory to use the listener port that Oracle Enterprise Manager connects to.

To do so, edit the `emdRepPort` and `emdRepConnectDescriptor` properties in the `emoms.properties` file.
- 10. Edit the `PORT` value in the `oracle_listener` and `oracle_database` entries in the `$ORACLE_HOME/hostname_sid/sysman/emd/targets.xml` file to use the new port number.
- 11. From the Audit Vault Server shell, restart the Audit Vault Console and collector, and then check their status to ensure that they can connect to the source database.


```
avctl start_av
avctl start_collector -collname collector_name -srcname source_name

avctl show_av_status
avctl show_collector_status -collname collector_name -srcname source_name
```
- 12. From the Audit Vault collection agent shell, restart the collection agent, and then ensure that it is running by checking its status.

For collection agents created in Release 10.2.3.2:

```
avctl start_agent
avctl show_agent_status
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl start_oc4j
avctl show_oc4j_status
```

Next, reconfigure each Audit Vault collection agent to connect to the database, as follows:

1. Access the shell or command prompt for the Audit Vault Server.
 - **UNIX:** If necessary, set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Stop each collector.


```
avctl stop_collector -collname collector_name -srcname source_name
```
3. Stop the collection agents.

For collection agents that were created in Release 10.2.3.2:

```
avctl stop_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl stop_oc4j
```

4. In the Audit Vault collection agent home, edit the entry for AV in the `$ORACLE_HOME/network/admin/tnsnames.ora` file to use the new port number.
5. Restart the collection agents.

For collection agents created in Release 10.2.3.2:

```
avctl start_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl start_oc4j
```

6. From the Audit Vault Server shell, start each collector for the agent.

```
avctl start_collector -collname collector_name -srcname source_name
```

4.9.1.2 Changing the Audit Vault Console HTTP Port Number

Changing the HTTP port for the Audit Vault Console affects the Audit Vault Console only.

To change the HTTP port for the Audit Vault Console:

1. In the `$ORACLE_HOME/oc4j/j2ee/OC4J_DBConsole_host_name_av/config/av-web-site.xml` file, edit the `web-site port` entry to use the new port number.
2. In the `$ORACLE_HOME/oc4j/j2ee/oc4j_applications/applications/av/av/WEB-INF/classes/av.properties` file, edit the `av.console.port` entry to match the port number you entered in Step 1.
3. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

4. Stop the Audit Vault Console.

```
avctl stop_av
```

5. Restart the Audit Vault Console.

```
avctl start_av
```

4.9.1.3 Changing the Oracle Enterprise Manager Database Control Port Number

Changing the Database Control port number affects only Database Control.

To change the Database Control port number:

1. From the Audit Vault Server shell, run the following `emca -reconfig ports` commands:

```
emca -reconfig ports -DBCONTROL_HTTP_PORT new_port_number
emca -reconfig ports -RMI_PORT new_port_number
emca -reconfig ports -JMS_PORT new_port_number
```

2. In the `$ORACLE_HOME/hostname_sid/sysman/config` directory, edit the `emoms.properties` file to use the new listener port that Database Control uses.

4.9.1.4 Changing the Audit Vault PL/SQL Gateway Port Number

Changing the Audit Vault PL/SQL gateway port affects the Audit Vault Console only.

1. In the Audit Vault Server shell or command prompt, ensure that the listener is running.

```
lsnrctl status
```

If the listener is not running, then start it.

```
lsnrctl start
```

2. Log in to SQL*Plus as a user who has been granted the AV_ADMIN role.

For example:

```
sqlplus tjones
Enter password: password
Connected.
```

3. Run the following statements:

```
SQL> EXEC DBMS_XDB.SETHTTPPORT(new_port_number);
SQL> COMMIT;
```

4.9.2 Changing Port Numbers for the Audit Vault Collection Agents

Changing the port numbers for the Audit Vault agent affects the agents and collectors.

This section contains:

- [Changing the Collection Agent HTTP Port Number](#)
- [Changing the Collection Agent RMI and JMS Port Numbers](#)

4.9.2.1 Changing the Collection Agent HTTP Port Number

Changing the HTTP port for the collection agent affects the agents and collectors only.

To change the port number for the agent HTTP connection:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.

2. Stop the collection agents.

For collection agents that were created in Release 10.2.3.2:

```
avctl stop_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl stop_oc4j
```

3. In the `$ORACLE_HOME/oc4j/j2ee/home/config/http-web-site.xml` file, edit the `web-site` port entry to use the new port number.

4. Restart the collection agents.

For collection agents created in Release 10.2.3.2:

```
avctl start_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl start_oc4j
```

5. Log in to Audit Vault Console as a user who has been granted the AV_ADMIN role.
6. Navigate to the Configuration page, then select the **Agent** tab.
7. Select the agent for which you changed the port.
8. Click the **Edit** button.
9. In the **Port Number** field, enter the new port number.
10. Click **OK** to update the port number for this agent in the Audit Vault Server.

4.9.2.2 Changing the Collection Agent RMI and JMS Port Numbers

Changing the collection agent RMI and JMS port numbers affects the agents only.

To change the collection agent RMI and JMS port numbers:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.

2. Stop the collection agents.

For collection agents that were created in Release 10.2.3.2:

```
avctl stop_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl stop_oc4j
```

3. In the `$ORACLE_HOME/oc4j/j2ee/home/config/rmi.xml` file, edit the `rmi-server` port setting to use the new port number for the RMI port.
4. In the `$ORACLE_HOME/oc4j/j2ee/home/config/jms.xml`, edit the `jms-server` port to use the new port number for the JMS port.
5. Restart the collection agents.

For collection agents created in Release 10.2.3.2:

```
avctl start_agent
```

For Release 10.2.3.1 or earlier collection agents that have not yet been upgraded:

```
avctl start_oc4j
```

4.9.3 Changing Port Numbers for the Oracle Source Database

Changing the port number for the Oracle source database affects the Audit Vault collectors.

First, change the port number for the source database listener:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Stop each collector that is running against this source database.

```
avctl stop_collector -collname collector_name -srcname source_name
```

3. Shut down the listener.

```
lsnrctl stop
```

4. Use Oracle Net Configuration Assistant to change the port number.

From `$ORACLE_HOME/bin`, enter the following command to start Net Configuration Assistant:

```
netac
```

5. Restart the listener.

```
lsnrctl start
```

6. Do not close this shell.

Next, follow these steps:

1. Update the source database port number.

From the Audit Vault Server, run the following command:

```
avorcldb alter_source -srcname source_name PORT=new_port_number
```

Alternatively, use the Audit Vault Console to change the source database port number.

2. From the collection agent shell, update the port number in the `tnsnames.ora` file.

```
avorcldb setup -srcname source_database
```

```
Enter Source user name: username
```

```
Enter Source password: password
```

Alternatively, edit the port number for the source database in the `tnsnames.ora` file in the `$ORACLE_HOME/network/admin` directory.

3. From the Audit Vault Server shell, start each collector the agent.

```
avctl start_collector -collname collector_name -srcname source_name
```

4. On the Audit Vault Server, update the port number in the file `$ORACLE_HOME/network/admin/tnsnames.ora` for the source database.

4.10 Purging the Oracle Source Database Audit Trail

This section contains:

- [About Purging the Oracle Source Database Audit Trail](#)
- [Scheduling an Automated Purge Job for an Oracle Audit Vault Environment](#)

4.10.1 About Purging the Oracle Source Database Audit Trail

When you add an Oracle source database from Releases 10.2.0.3 through 11.2 with Oracle Audit Vault, you can use the `DBMS_AUDIT_MGMT` PL/SQL package to purge the database audit trail. This feature does not apply to Oracle Database 9i Release 2 (9.2) source databases.

The `DBMS_AUDIT_MGMT` package enables you to perform audit trail cleanup tasks such as scheduling purge jobs, moving the audit trail to a different tablespace, setting

archive timestamps in the audit trail, and so on. You must have the EXECUTE privilege for DBMS_AUDIT_MGMT before you can use it.

By default, Oracle Database 11g Release 2 (11.2) has the DBMS_AUDIT_MGMT package and its associated data dictionary views installed. If your source database is from Release 10.2.0.3 through 11.1.0.7, then you can download the DBMS_AUDIT_MGMT package and data dictionary views from My Oracle Support, from the following Web site:

<https://support.oracle.com>

Search for Article ID 731908.1.

To create an automated purge job in an Oracle Audit Vault environment, see [Section 4.10.2](#).

For details about using the DBMS_AUDIT_MGMT PL/SQL package and views, refer to the following Oracle Database 11g Release 2 (11.2) documentation:

- The section "Purging Audit Trail Records" in *Oracle Database Security Guide* for conceptual and procedural information
- *Oracle Database PL/SQL Packages and Types Reference* for reference information about the DBMS_AUDIT_MGMT PL/SQL package
- *Oracle Database Reference* for information about the DBA_AUDIT_MGMT_* data dictionary views

4.10.2 Scheduling an Automated Purge Job for an Oracle Audit Vault Environment

Oracle Audit Vault is integrated with the DBMS_AUDIT_MGMT package on a source database. This integration automates the purging of audit records from the AUD\$ and FGA_LOG\$ files, and from the operating system .aud and .xml files after they have been successfully inserted into the Audit Vault repository by the Audit Vault collector. After the purge is completed, the collectors automatically set a timestamp on audit data that has been collected. Therefore, you must set the USE_LAST_ARCH_TIMESTAMP property to true to ensure that the right set of audit records are purged. You do not need to manually set a purge job interval.

To schedule an automated purge job for an Audit Vault source Oracle database:

1. Log in to SQL*Plus on the source database as a user who has been granted the EXECUTE privilege for the DBMS_AUDIT_MGMT PL/SQL package.

For example:

```
sqlplus tjones
Enter password: password
```

2. Initialize the audit trail cleanup operation.

In the following example, the DEFAULT_CLEANUP_INTERVAL setting runs the job every two hours:

```
BEGIN
  DBMS_AUDIT_MGMT.INIT_CLEANUP(
    AUDIT_TRAIL_TYPE      => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
    DEFAULT_CLEANUP_INTERVAL => 2 );
END;
/
```

3. Verify that the audit trail is initialized for cleanup.

For example:

```
SET SERVEROUTPUT ON
BEGIN
  IF
    DBMS_AUDIT_MGMT.IS_CLEANUP_INITIALIZED(DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL)
  THEN
    DBMS_OUTPUT.PUT_LINE('Database and OS audit are initialized for cleanup');
  ELSE
    DBMS_OUTPUT.PUT_LINE('Database and OS audit are not initialized for
cleanup. ');
  END IF;
END;
/
```

4. Use the DBMS_AUDIT_MGMT.CREATE_PURGE_JOB procedure to create and schedule the purge job.

In this procedure, ensure that you set the `USE_LAST_ARCH_TIMESTAMP` property to `TRUE`, so all records older than the timestamp can be deleted.

The following procedure creates a purge job called `CLEANUP_OS_DB_AUDIT_RECORDS` that will run every two hours to purge the audit records.

```
BEGIN
  DBMS_AUDIT_MGMT.CREATE_PURGE_JOB (
    AUDIT_TRAIL_TYPE           => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
    AUDIT_TRAIL_PURGE_INTERVAL => 2,
    AUDIT_TRAIL_PURGE_NAME     => 'CLEANUP_OS_DB_AUDIT_RECORDS',
    USE_LAST_ARCH_TIMESTAMP    => TRUE );
END;
/
```

See *Oracle Database PL/SQL Packages and Types Reference* for detailed information about the `DBMS_AUDIT_MGMT` PL/SQL package.

4.11 Purging the Oracle Audit Vault Repository Audit Trail

By default, the audit trail generated by the Oracle Audit Vault repository is purged every 24 hours. If you want, you can change these purge settings, or to disable purging altogether. (You may want to disable the purge settings if you are using a different purge utility.) For information about purging the audit trail, see the list of documentation references in [Section 4.11](#).

Note the following:

- The `AUDIT_TRAIL` initialization parameter in the Audit Vault Server database is set to `DB`, which means that the audit trail is written to the database `AUD$` system table. You can set the audit trail to any valid `AUDIT_TRAIL` initialization parameter setting. (However, you cannot modify the Oracle Database Vault audit trail setting, which is always `DB`.)
- Because Oracle Database Vault is enabled, the `AUD$` system table resides in the `SYSTEM` schema. The synonym `SYS.AUD$` is created to refer to the `SYSTEM.AUD$` table. (Oracle strongly recommends that you do not disable Oracle Database Vault.)

Managing Oracle Audit Vault Security

This chapter contains:

- [About Managing Oracle Audit Vault Security](#)
- [Managing Oracle Audit Vault User Accounts](#)
- [Managing Authentication Metadata Using Oracle Advanced Security](#)
- [Changing Oracle Audit Vault User Passwords on a Regular Basis](#)
- [Using Oracle Database Vault within Oracle Audit Vault](#)
- [Configuring HTTPS and SSL Communication for Oracle Audit Vault](#)
- [Updating XDB Certificates](#)

5.1 About Managing Oracle Audit Vault Security

This chapter explains how to manage Oracle Audit Vault security. You should perform Oracle Audit Vault security tasks in this order of importance:

1. Secure management communication between the Oracle Audit Vault Server and collection agent, described in [Section 5.6](#).
2. Manage user authentication metadata, described in [Section 5.3](#).

[Section 5.5](#) explains how Oracle Database Vault protects audit data and provides strong access control.

5.2 Managing Oracle Audit Vault User Accounts

During the Oracle Audit Vault installation process, you created the following two system-generated user accounts:

- **Audit Vault administrator account.** This user account is responsible for the administrative tasks described in this manual, and is granted the AV_ADMIN role.
- **Audit Vault auditor account.** This user account is responsible for the auditing tasks described in *Oracle Audit Vault Auditor's Guide*, and is granted the AV_AUDITOR role.

As a best practice, you should use these two user accounts only as back-up accounts, and grant the appropriate Audit Vault role to the users who are responsible for the day-to-day Oracle Audit Vault operations. Each user account must have its own user name and password. For example, if your site requires two Audit Vault administrators and six auditors, then grant the administrators the AV_ADMIN role and the auditors the AV_AUDITOR role. Or, for example, if all your administrators are granted SEC_ADMIN

role and everyone who has the SEC_ADMIN role must also administer Oracle Audit Vault, then grant the AV_ADMIN role to the SEC_ADMIN role.

This way, if an Audit Vault administrator or auditor leaves the department or your company, then you only need to revoke the role from this user. If all the users who have been granted a particular role leave your company, then you can use the back-up Audit Vault user account that you created during installation to grant the role to new users. The danger of relying on the default user accounts that you created during installation is that if multiple users use the account, then they all can log in using the same user account and password. Shared passwords make your system less secure.

Similarly, you should grant the DV_OWNER and DV_ACCTMGR roles to individual users, and only use the DV_OWNER and DV_ACCTMGR accounts that you created during installation as back-up accounts. This is particularly important in the case where a user must have his or her password reset, because only a user who has been granted the DV_ACCTMGR role or the ALTER USER privilege can set passwords.

In addition to the AV_ADMIN and AV_AUDITOR roles, a default Oracle Audit Vault installation provides a set of administrative roles that you can use to manage Oracle Audit Vault. These roles provide separation-of-duty tasks. See [Table 5–1](#) on page 5-4 for more information.

To create user accounts for use with Oracle Audit Vault:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. If you must create new user accounts, then log in to SQL*Plus as a user who has been granted the CREATE USER privilege or the DV_ACCTMGR role, and create the user accounts.

For example:

```
sqlplus avadmin/va
Enter password: password
Connected.
```

```
SQL> CREATE USER tjones IDENTIFIED BY password; -- The AV_ADMIN user
SQL> CREATE USER psmith IDENTIFIED BY password; -- The AV_AUDITOR user
```

3. Connect as a user who has been granted the AV_ADMIN role and then grant the AV_ADMIN and AV_AUDITOR roles to these users.

For example:

```
SQL> CONNECT avadmin
Enter password: password
Connected.
```

```
SQL> GRANT AV_ADMIN TO tjones; -- The AV_ADMIN user
SQL> GRANT AV_AUDITOR TO psmith; -- The AV_AUDITOR user
```

4. Repeat these steps to create individual accounts to be granted the DV_OWNER and DV_ACCTMGR roles.

For the role grants, do the following:

- When you are ready to grant the DV_OWNER role to the user, connect as a user who has been granted the DV_OWNER role.

- When you are ready to grant the DV_ACCTMGR role to the user, connect as a user who has been granted the DV_ACCTMGR role.

See [Table 1–7](#) on page 1-11 for more information about these roles.

5. Optionally, audit the actions of the user who has been granted the AV_ADMIN role.

5.3 Managing Authentication Metadata Using Oracle Advanced Security

As part of the Audit Vault Server and the Oracle Audit Vault collection agent installation, two wallets are created. One wallet resides on the Audit Vault Server and this one contains the credentials of the AV_ADMIN. The Audit Vault Console uses this wallet to communicate with the Oracle Audit Vault database. The Audit Vault Console provides the management service that initiates the communication with collection agents using HTTP. Audit Vault Configuration Assistant (AVCA) modifies the Database Control console `server.xml` file and other related files to enable Oracle 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 collection agent and contains the AV_AGENT credentials. The collection agent uses this wallet to get configuration data from Oracle Audit Vault. This wallet is located in the `$ORACLE_HOME/network/admin/avwallet` directory. This wallet also contains the credentials used by the collectors to communicate with the source database (Oracle Database, Microsoft SQL Server database, Sybase ASE, or IBM DB2 database). The three ORCLDB collectors, the MSSQLDB collector, the SYBDB collector, and the DB2 collector all use these credentials to connect to the source database and to:

- Open a connection to the source database to read, extract, and send audit records to the Audit Vault repository
- Obtain metadata and metrics for all the collectors
- Start and stop the collectors
- Obtain audit settings as part of Audit Settings management for ORCLDB collectors
- Obtain user entitlement information for ORCLDB collectors

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. You can manage Oracle wallets by using Oracle Wallet Manager. Oracle Wallet Manager can perform tasks such as wallet creation, certificate request generation, and importing certificates into the wallet.

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 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.

5.4 Changing Oracle Audit Vault User Passwords on a Regular Basis

This section contains:

- [About Oracle Audit Vault User Passwords](#)
- [Changing the AV_ADMIN User Password](#)
- [Changing the AVREPORTUSER Password](#)
- [Changing the AV_AGENT Password](#)
- [Changing the Source User Password](#)
- [Changing the AV_AUDITOR Password](#)
- [Ensuring That All Changed User Name Passwords Work Correctly](#)

5.4.1 About Oracle Audit Vault User Passwords

You should have a policy in place for changing passwords for the Oracle Audit Vault user accounts. For example, you may require that users change their passwords on a regular basis, such as every 120 days, and that they create passwords that are not easily guessed.

[Table 5–1](#) summarizes guidelines that you must follow when you change passwords for the Oracle Audit Vault user accounts.

Table 5–1 Storage Location of Audit Vault and Source User Name Passwords

Audit Vault Role	Is Password Stored in Wallet?	How Do I Change the Password?
AV_ADMIN	Yes	<ol style="list-style-type: none"> 1. If the system-generated AV_ADMIN user account password changes, then use the <code>ALTER USER SQL</code> statement to change the password of this user in the database. (You do not need to change the password for other users who have been granted the AV_ADMIN role.) 2. Use the <code>avca create_credential</code> command to change the password in the wallet in the Audit Vault Server home. <p>See Section 5.4.2.</p>
AVREPORTUSER user	Yes	<ol style="list-style-type: none"> 1. Use the <code>ALTER USER SQL</code> statement to change the password of this user in the database. 2. Use the <code>avca create_credential</code> command to change the password in the wallet in the Audit Vault Server home.
AV_AGENT	Yes	<ol style="list-style-type: none"> 1. Use the <code>ALTER USER SQL</code> statement to change the password of this user in the database. 2. Use the <code>avca create_credential</code> command to change the password in the wallet in the Audit Vault collection agent home. <p>See Section 5.4.4.</p>

Table 5–1 (Cont.) Storage Location of Audit Vault and Source User Name Passwords

Audit Vault Role	Is Password Stored in Wallet?	How Do I Change the Password?
Source user on source database	Yes	<ol style="list-style-type: none"> 1. For Oracle Database source user accounts, use the <code>ALTER USER SQL</code> statement in the source database to change the password. 2. Also for Oracle databases, run the <code>avca create_credential</code> command to change the password in the wallet in the Audit Vault Server. 3. For all source database types, run the <code>setup</code> command of the <code>AVORCLDB</code>, <code>AVMSSQLDB</code>, or <code>AVSYBDB</code> utility to change the password in the wallet in the Audit Vault collection agent home. (The <code>AVDB2DB</code> utility has no <code>setup</code> command. For IBM DB2 databases, you only need to change the password of the designated user account.) <p>See Section 5.4.4</p>
AV_AUDITOR	No	<p>Use the <code>ALTER USER SQL</code> statement in the Audit Vault Server home to change this user's password.</p> <p>See Section 5.4.6.</p>

5.4.2 Changing the AV_ADMIN User Password

After you have updated the AV_ADMIN user account using the `ALTER USER SQL` statement, you must update the password credentials of this user.

To change the password of a user who has been granted the AV_ADMIN role:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Log in to SQL*Plus as the user whose password you must change, another user who has been granted the `ALTER_USER` privilege, or a user with the `DV_ACCTMGR` role, and then change the password.

For example:

```
sqlplus dvsmith
Enter password: password
Connected.
```

```
SQL> ALTER USER avsmith IDENTIFIED BY password;
```

3. Exit SQL*Plus.

If this user was granted the AV_ADMIN role after the Oracle Audit Vault installation, then you have completed this procedure. Otherwise, if the AV_ADMIN user account had been created during the Audit Vault installation, then go to Step 4.

4. Run the `avca create_credential` command to change the password credentials of the AV_ADMIN user.

For example:

```
avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -dbalias orcl
AVCA started
```

```

Storing user credentials in wallet...
Enter source user username: avadminuser
Enter source user password: password
Re-enter source user password: password
Create credential Modify credential
Modify 2
done.

```

In this example, the `dbalias` parameter specifies the Audit Vault Server SID in the Audit Vault Server home. You can find this information by running the `lsnrctl status` command on the computer where you installed the source database. For detailed information about using the `avca create_credential` command, see [Section 6.4](#).

5.4.3 Changing the AVREPORTUSER Password

The AVREPORTUSER account is an internal account that is used to manage Audit Vault reports.

To update the AVREPORTUSER password:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Log in to SQL*Plus as the user whose password you must change, another user who has been granted the ALTER_USER privilege, or a user with the DV_ACCTMGR role, and then change the password.

For example:

```

sqlplus dvsmith
Enter password: password
Connected.

```

```
SQL> ALTER USER avreportuser IDENTIFIED BY password;
```

3. Run the `avca create_credential` command to change the password credentials of the AVREPORTUSER account.

For example:

```
avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -dbalias av_
auditor_user
```

```

AVCA started
Storing user credentials in wallet...
Enter source user username: AVREPORTUSER
Enter source user password: password
Re-enter source user password: password
Create credential Modify credential
Modify 2
done.

```

5.4.4 Changing the AV_AGENT Password

When you change the AV_AGENT user password, you must also update this user's credentials for each agent that connects to the Audit Vault Server as the AV_AGENT user account.

To change the password credentials for the AV_AGENT user account:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
2. Log in to SQL*Plus and use the `ALTER USER SQL` statement to change the password of the AV_AGENT user.

For example:

```
sqlplus dvsmith
Enter password: password
Connected.
SQL> ALTER USER avagent_usr IDENTIFIED BY password;
```

3. Access the shell or command prompt used for the Audit Vault collection agent.
4. For each agent that connects to the server as the AV_AGENT user account, run the `avca create_credential` command to update the locally cached credentials with the new password.

For example:

```
avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -dbalias av
AVCA started
Storing user credentials in wallet...
Enter source user username: avagentuser
Enter source user password: password
Re-enter source user password: password
Create credential Modify credential
Modify 2
done.
```

For detailed information about using the `avca create_credential` command, see [Section 6.4](#).

5.4.5 Changing the Source User Password

After you have updated the source database stored password credential, you must update the password credentials of this account.

To change the password credentials for the source user account:

1. In the source database, change the password for the source database user.

For an Oracle Database source, use the `ALTER USER SQL` statement to change the password.

For example:

```
sqlplus dvsmith
Enter password: password
Connected.
SQL> ALTER USER srcuser_ora IDENTIFIED BY password;
```

For source user accounts created for Microsoft Windows, Sybase ASE, and IBM DB2, log in to the appropriate source database and then change the password there.

2. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).

- **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.
3. Run the appropriate `setup` command to configure the source user password. (Ensure that you only run this command on the agent, not the server.)
 - **Oracle Database source databases:** Run the `avorcldb setup` command (see [Section 8.9](#)). For example:


```
avorcldb setup -srcname hrdb.example.com
Enter Source user name: srcuser_ora
Enter Source password: password
```
 - **SQL Server source databases:** Run the `avmssqldb setup` command ([Section 9.9](#)). For example:


```
avmssqldb setup -srcname mssqldb4
Enter a username : source_user_name
Enter a password : password
```
 - **Sybase ASE source databases:** Run the `avsybdb setup` command ([Section 10.9](#)). For example:


```
avsybdb setup -srcname sybdb4
Enter a username : source_user_name
Enter a password : password
```
 - **IBM DB2 databases:** The `avdb2db` utility has no `setup` command. For IBM DB2 databases, you only need to change the password of the designated user account.
 4. If the source database is an Oracle database, then open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
 5. For this Oracle source database, run the `avca create_credential` command to change the password credentials.
 - a. Find the value of the `dbalias` parameter for the Oracle source database. Query source ID from Audit Vault as follows, and appending it to the string `SRCDB` (for example, `SRCDB1`):


```
sqlplus /@AV_SID
SELECT SOURCE_ID FROM AVSYS.AV$SOURCE WHERE SOURCE_NAME = source_name
```
 - b. Use this value in the `avca create_credential` command. For example, assuming the `dbalias` is `avorcl`:


```
avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -dbalias
avorcl
AVCA started
Storing user credentials in wallet...
Enter source user username: avsource_user
Enter source user password: password
Re-enter source user password: password
Create credential Modify credential
Modify 2
done.
```


5.4.6 Changing the AV_AUDITOR Password

To change the password of a user who has been granted the AV_AUDITOR role, you must change the passwords in both the Audit Vault Server home in the Audit Vault database by using the SQL ALTER_USER command. Log in as the user with the role of Database Vault Account Manager.

For example:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Log in to SQL*Plus as the Database Vault Account Manager (that is, a user who has been granted the DV_ACCTMGR role).

For example:

```
sqlplus dvsmith
Enter password: password
Connected.
SQL>
```

3. Use the ALTER USER SQL statement to change the AV_AUDITOR user account.

For example:

```
SQL> ALTER USER avauditorusr-name IDENTIFIED BY password;
```

5.4.7 Ensuring That All Changed User Name Passwords Work Correctly

To test the changed passwords for users who have been granted the AV_ADMIN and AV_AUDITOR roles, log in to the Audit Vault Console as the Audit Vault administrator and then as the Audit Vault auditor. See [Section 3.2.3](#) for instructions on logging in to the Audit Vault Console. If the login is not successful, repeat the procedures described in this section to re-create the passwords, and then retest them.

For the AV_ADMIN role, you must also test that the credentials were stored correctly in the wallet.

Follow these steps:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. In SQL*Plus, log in to the Audit Vault Server.

For example, assuming the SID of the Audit Vault Server is av:

```
sqlplus /@av
```

To test the AV_AGENT and source database user account passwords, stop the collection agents, and then restart the collection agent and each collector. See [Chapter 7](#) for information about the commands you use to perform this test. If you are able to collect new audit records, then the AV_AGENT and source database user account passwords are working. If you cannot collect audit records, then check the log files (see [Appendix A](#) for more information) to determine which user name password might be the cause of the problem. If necessary, re-create the passwords and then retest them.

5.5 Using Oracle Database Vault within Oracle Audit Vault

By default, Oracle Database Vault is enabled in the Audit Vault Server. Oracle Database Vault restricts access to the data in the Audit Vault Server from any user, including users who have administrative access. For Oracle Audit Vault, Oracle Database Vault protects the Audit Vault Server by using a realm. To ensure that the data in the Audit Vault Server is protected, do not disable Oracle Database Vault.

The inclusion of Oracle Database Vault provides the DV_OWNER and DV_ACCTMGR roles. The DV_OWNER role manages the database roles and configuration, and the DV_ACCTMGR role manages user accounts. As with all Oracle Database roles, grant these roles only to those users who are responsible for the tasks associated with the role.

Be aware that Oracle Database Vault revokes some privileges from several roles supplied by the Oracle database roles, including SYS and SYSTEM. *Oracle Database Vault Administrator's Guide* describes roles and privileges that Oracle Database Vault affects. Remember that only the user who has been granted the DV_ACCTMGR role can create, alter, and drop users. However, the DV_ACCTMGR user cannot grant these roles to these users. Only the user who has been granted the AV_ADMIN role can grant the AV_ADMIN and AV_AUDITOR roles to another user.

Table 5–2 shows the roles and privileges an administrative user is granted when that user is granted and Oracle Audit Vault or Oracle Database Vault roles. For detailed information about the Oracle Audit Vault or Oracle Database Vault roles, see [Section 1.5](#).

Table 5–2 Roles and Privileges Granted to Audit Vault or Database Vault Administrators

Role Granted to User	Roles Granted to This Role	Privileges Granted
AV_ADMIN	SELECT_CATALOG_ROLE	CREATE SESSION
	AQ_ADMINISTRATOR_ROLE	GRANT ANY ROLE
	AV_AUDITOR ¹	
	AV_AGENT	
	XDBADMIN	
AV_AUDITOR	SELECT_CATALOG_ROLE	CREATE SESSION
AV_AGENT	No additional roles granted	CREATE SESSION
		CREATE ANY VIEW
DV_ACCTMGR	DV_PUBLIC	CREATE SESSION
	CONNECT	CREATE USER
		ALTER USER
		DROP USER
		CREATE PROFILE
		ALTER PROFILE
DV_OWNER		DROP PROFILE
	DV_PUBLIC	CREATE SESSION
	CONNECT	GRANT ANY ROLE
	DV_ADMIN	ALTER ANY TRIGGER
	DV_SECANALYST	ADMINISTER DATABASE TRIGGER

¹ The AV_ADMIN role is granted the AV_AUDITOR role only if you did not create the AV_AUDITOR user during installation.

[Table 5–3](#) shows other database core accounts that are created in the default Oracle Audit Vault installation. Oracle Audit Vault permits operating system authentication to the database. It disables remote authentication to the database if you try to use the SYSDBA privilege, but if it is needed, you can enable it by using a password file. See the sections that discuss postinstallation tasks in the *Oracle Audit Vault Installation Guide* for more information about unlocking and resetting user passwords and enabling or disabling connections with the SYSDBA privilege.

Table 5–3 Database Core Accounts Created and Privileges Use

Account	Privileges	Privilege In Use	Password to Use
SYS SYSTEM SYSMAN DBSNMP	Many ¹	Yes	Use same password as user granted AV_ ADMIN role for basic installation or password may be set separately in advanced installation
SYS AS or / AS	SYSDBA	Yes, allowed	Operating system authentication to the database is enabled by default.
SYS AS	SYSDBA	No, not allowed for remote connection	To use for remote connection, user must create a password file to enable its use. Password is set when password file is created.
SYS AS	SYSOPER	Yes, allowed	Use same password as user granted AV_ ADMIN role

¹ To find the privileges associated with the user account, log in to SQL*Plus as the user and then run the following query: `SELECT * FROM SESSION_ROLES;`

5.6 Configuring HTTPS and SSL Communication for Oracle Audit Vault

This section contains:

- [About Configuring HTTPS and SSL Communication for Oracle Audit Vault](#)
- [Step 1: Generate the Keystore](#)
- [Step 2: Create an Audit Vault Agent Keystore by Using the keytool Utility](#)
- [Step 3: Secure the XDB Services](#)
- [Step 4: Secure Audit Vault Server](#)
- [Step 5: Secure Audit Vault Agent](#)

5.6.1 About Configuring HTTPS and SSL Communication for Oracle Audit Vault

You can secure management communication between the Oracle Audit Vault Server and collection agent by using the [HTTPS](#) protocol to encrypt data. In this case, you provide [X.509 certificates](#) for authentication. This section explains how to configure Secure Sockets Layer (SSL) for the mutual authentication between Oracle Audit Vault on the server side and each collection agent over HTTPS. A certificate authority (CA) must provide these certificates to you, the Oracle Audit Vault administrator.

To accomplish this, you secure the following services on the Audit Vault Server side:

- Oracle Audit Vault Web application, which you secure by using the `avca secure_av` command.
- XDB services, which you secure by using the `avca generate_crs` and `avca import` commands.

For the Audit Vault agent side, you secure OC4J by using the `avca secure_agent` command.

After you secure the Audit Vault Server and Audit Vault collection agent communication to use HTTPS, you must enable the browser to use HTTPS to access the Audit Vault Console. At this stage, HTTP will no longer be available for the browser user because the browser to the Audit Vault Console communication is also made secure.

Before you follow the procedures described in this section, you must understand how to use keystores, which are in JKS (Java Keystore) format from Sun Microsystems. You can create and manage keystores by using the keystore application from Sun Microsystems. See the following URLs for more information:

<http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html>

<http://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html>

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

5.6.2 Step 1: Generate the Keystore

To generate the keystore:

1. Create a keystore to secure the Audit Vault Console.

The following example uses the name `avkeystore` to denote the Audit Vault Server keystore:

```
oracle:/home/oracle> $ORACLE_HOME/jdk/bin/keytool -genkey -v -alias avkey
-keyalg RSA -keysize 1024 -dname "CN=avserver, OU=st, O=example, L=nomadcity,
ST=ca, C=us" -validity 365 -keypass welcome -keystore /tmp/certs/avkeystore
-storepass password
```

Output similar to the following appears:

```
Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)
for: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
[Saving /tmp/certs/avkeystore]
```

2. List the contents, and ensure that the keystore has valid keys and components.

At this stage, you should have a new keystore with an Audit Vault Server private key/certificate pair.

For example:

```
oracle:/home/oracle> $ORACLE_HOME/jdk/bin/keytool -list -v -keystore
/tmp/certs/avkeystore
Enter keystore password: password
```

Output similar to the following appears:

```
Keystore type: jks
Keystore provider: SUN
```

Your keystore contains 1 entry

```
Alias name: avkey
Creation date: Feb 18, 2010
```

```

Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
Serial number: 4b7e19da

```

3. Generate the certificate request.

For example:

```

oracle:/home/oracle> $ORACLE_HOME/jdk/bin/keytool -certreq -alias avkey
-keystore /tmp/certs/avkeystore -file /tmp/mycsr.csr
Enter keystore password: password

```

4. Send this certificate request file to a CA to be signed and then returned to you.

In the preceding steps, this request file is called `mycsr.csr` and was created in the `tmp` directory.

5. Import the CA root certificate.

For example:

```

oracle:/home/oracle> $ORACLE_HOME/jdk/bin/keytool -keystore
/tmp/certs/avkeystore -import -alias CACert -trustcacerts -file /tmp/cacert.pem
Enter keystore password: password

```

Output similar to the following appears; answer the prompts as needed.

```

Owner: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Issuer: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleSC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 0
Valid from: Mon Feb 08 23:54:23 MST 2010 until: Tue Feb 08 23:54:23 MST 2011
Certificate fingerprints:
MD5: 1C:D7:51:31:81:14:39:F3:CC:E0:24:86:9C:8A:69:08
SHA1: 6C:A4:35:1F:82:57:BF:DB:DC:D9:2B:82:A2:AC:F6:15:BD:8C:A6:99
Trust this certificate? [no]: yes
Certificate was added to keystore

```

6. Import the signed certificate to keystore.

For example:

```

oracle:/tmp> $ORACLE_HOME/jdk/bin/keytool -keystore /tmp/certs/avkeystore
-import -file /tmp/mycert.cer
Enter keystore password: password

```

Certificate was added to keystore

7. Check the keystore to ensure that the certificate chain is complete.

For example:

```

oracle:/tmp> $ORACLE_HOME/jdk/bin/keytool -list -v -keystore
/tmp/certs/avkeystore
Enter keystore password: password

```

Output similar to the following appears:

```

Keystore type: jks
Keystore provider: SUN

```

```

Your keystore contains 3 entries

Alias name: avkey
Creation date: Feb 18, 2010
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
Serial number: 4b7e19da
Valid from: Thu Feb 18 21:55:54 MST 2010 until: Fri Feb 18 21:55:54 MST 2011
Certificate fingerprints:
MD5: 89:AF:A3:3E:3C:91:B6:41:9C:26:D3:95:6C:AF:24:17
SHA1: 69:04:B2:16:95:69:38:9D:0F:D1:7B:4F:1B:EE:F3:E4:FA:A2:72:78

*****
*****

Alias name: cacert
Creation date: Feb 18, 2010
Entry type: trustedCertEntry

Owner: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Issuer: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 0
Valid from: Mon Feb 08 23:54:23 MST 2010 until: Tue Feb 08 23:54:23 MST 2011
Certificate fingerprints:
MD5: 1C:D7:51:31:81:14:39:F3:CC:E0:24:86:9C:8A:69:08
SHA1: 6C:A4:35:1F:82:57:BF:DB:DC:D9:2B:82:A2:AC:F6:15:BD:8C:A6:99

*****
*****

Alias name: mykey
Creation date: Feb 18, 2010
Entry type: trustedCertEntry

Owner: CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: EMAILADDRESS=sunil.shetty@examplecom, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 4
Valid from: Thu Feb 18 21:37:12 MST 2010 until: Fri Feb 18 21:37:12 MST 2011
Certificate fingerprints:
MD5: 87:82:9F:09:11:40:62:9E:FA:63:68:92:E2:7C:AA:57
SHA1: 47:41:0E:BE:05:49:2C:A5:55:3A:3E:F5:14:47:04:6E:85:40:F0:9F

*****
*****

```

5.6.3 Step 2: Create an Audit Vault Agent Keystore by Using the keytool Utility

To create an Audit Vault Agent keystore using the `keytool` utility:

1. Create the keystore that you will use to secure the Audit Vault agent.

For example:

```

oracle:/tmp/certs> $ORACLE_HOME/jdk/bin/keytool -genkey -v -alias agkey -keyalg
RSA -keysize 1024 -dname "CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us"

```

```
-validity 365 -keypass password -keystore /tmp/certs/agkeystore -storepass
password
```

Specify the same password for the `keypass` and `storepass` parameters. Otherwise, OC4J will be unable to open the keystore during startup.

Output similar to the following appears:

```
Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)
for: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
[Saving /tmp/certs/agkeystore]
```

2. List the contents to ensure that the keystore has valid keys and components.

At this stage, you should have a new keystore with an Audit Vault agent private key/certificate pair.

For example:

```
oracle:/tmp/certs> $ORACLE_HOME/jdk/bin/keytool -list -v -keystore
/tmp/certs/agkeystore
Enter keystore password: password
```

Output similar to the following appears:

```
Keystore type: jks
Keystore provider: SUN
```

Your keystore contains 1 entry

```
Alias name: agkey
Creation date: Feb 18, 2010
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
Serial number: 4b7e211b
Valid from: Thu Feb 18 22:26:51 MST 2010 until: Fri Feb 18 22:26:51 MST 2011
Certificate fingerprints:
MD5: D4:EE:B1:EC:D2:DA:02:07:20:8C:01:C8:36:FE:2C:0B
SHA1: CF:1F:9D:BF:6C:65:FD:4D:15:54:0C:27:F3:5F:63:E8:39:90:D4:EA
```

```
*****
*****
```

3. Generate the certificate request.

For example:

```
oracle:/tmp/certs> $ORACLE_HOME/jdk/bin/keytool -certreq -alias agkey -keystore
/tmp/certs/agkeystore -file /tmp/mycsr_agent.csr
Enter keystore password: password
```

4. Send this certificate request file to a CA to be signed and then returned to you.

5. Import the CA root certificate to the agent keystore.

For example:

```
oracle:/tmp> $ORACLE_HOME/jdk/bin/keytool -keystore /tmp/certs/agkeystore
-import -alias CAcert_agent -trustcacerts -file /tmp/cacert.pem
Enter keystore password: password
```

Output similar to the following appears; answer the prompts as needed.

```
Owner: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Issuer: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 0
Valid from: Mon Feb 08 23:54:23 MST 2010 until: Tue Feb 08 23:54:23 MST 2011
Certificate fingerprints:
MD5: 1C:D7:51:31:81:14:39:F3:CC:E0:24:86:9C:8A:69:08
SHA1: 6C:A4:35:1F:82:57:BF:DB:DC:D9:2B:82:A2:AC:F6:15:BD:8C:A6:99
Trust this certificate? [no]: yes

Certificate was added to keystore
```

6. Import the signed certificate of the Audit Vault agent to keystore.

For example:

```
oracle:/tmp> $ORACLE_HOME/jdk/bin/keytool -keystore /tmp/certs/agkeystore
-import -trustcacerts -file /tmp/mycert_agent.cer
Enter keystore password: password

Certificate was added to keystore
```

7. Ensure that the Audit Vault agent keystore has proper certificate chain.

For example:

```
oracle:/tmp> $ORACLE_HOME/jdk/bin/keytool -list -v -keystore
/tmp/certs/agkeystore
Enter keystore password: password
```

Output similar to the following appears:

```
Keystore type: jks
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: agkey
Creation date: Feb 18, 2010
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
Serial number: 4b7e211b
Valid from: Thu Feb 18 22:26:51 MST 2010 until: Fri Feb 18 22:26:51 MST 2011
Certificate fingerprints:
MD5: D4:EE:B1:EC:D2:DA:02:07:20:8C:01:C8:36:FE:2C:0B
SHA1: CF:1F:9D:BF:6C:65:FD:4D:15:54:0C:27:F3:5F:63:E8:39:90:D4:EA

*****
*****

Alias name: cacert_agent
Creation date: Feb 18, 2010
Entry type: trustedCertEntry

Owner: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
```



```

Issuer: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=Example eISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 0
Valid from: Mon Feb 08 23:54:23 MST 2010 until: Tue Feb 08 23:54:23 MST 2011
Certificate fingerprints:
MD5: 1C:D7:51:31:81:14:39:F3:CC:E0:24:86:9C:8A:69:08
SHA1: 6C:A4:35:1F:82:57:BF:DB:DC:D9:2B:82:A2:AC:F6:15:BD:8C:A6:99

```

```

*****
*****

```

```

Alias name: mykey
Creation date: Feb 18, 2010
Entry type: trustedCertEntry

```

```

Owner: CN=agent, OU=st, O=example, L=nomadcity, ST=ca, C=us
Issuer: EMAILADDRESS=sunil.shetty@example.com, CN=Sathya, OU=ExampleISC,
O=Support, L=Bangalore, ST=Karnataka, C=IN
Serial number: 5
Valid from: Thu Feb 18 21:57:09 MST 2010 until: Fri Feb 18 21:57:09 MST 2011
Certificate fingerprints:
MD5: E5:19:D5:F8:95:37:C5:F3:91:AB:CB:F1:C9:26:E1:30
SHA1: 16:4A:63:6A:84:9A:CC:2A:8E:6D:28:46:65:48:CA:31:D0:80:DA:3D

```

```

*****
*****

```

5.6.4 Step 3: Secure the XDB Services

To secure the XDB services:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

2. Create a certificate request that will be stored in the Oracle wallet.

```

oracle:/tmp> avca generate_csr -certdn
\"cn=oe15upd1,OU=DBSEC,O=Example,ST=CA,C=US\" -out /tmp/cert.out

```

```

Generating Certificate request...
Certificate request generated successfully.

```

See [Section 6.12](#) for detailed information about the `avca generate_csr` command.

3. Send this certificate request file to a CA to be signed and then returned to you.
4. Import the CA certificate into the Oracle wallet as a trusted CA.

For example:

```

oracle:/tmp> avca import_cert -cert /tmp/cacert.pem -trusted

```

```

Importing Certificate...
Certificate imported successfully.

```

See [Section 6.14](#) for detailed information about the `avca import_cert` command.

5. Import the user certificate.

For example:

```
oracle:/tmp> avca import_cert -cert /tmp/newcert.pem
```

```
Importing Certificate...
Certificate imported successfully.
```

5.6.5 Step 4: Secure Audit Vault Server

To secure Audit Vault Server:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avca secure_av` command.

For example:

```
oracle:/tmp> avca secure_av -avkeystore /tmp/certs/avkeystore -avtruststore
/tmp/certs/avkeystore
```

See [Section 6.20](#) for detailed information about the `avca secure_av` command.

Output similar to the following appears:

```
Checking for SSL Certificate...
done.
Enter Audit Vault Server keystore password:
Stopping OC4J...
OC4J stopped successfully.
Securing XDB services...
Identified XDB http(s) Port...
Stopping Listeners...
done.
Starting Listeners...
done.
done.
Starting OC4J...
OC4J started successfully.
TZ set to US/MountainOracle Audit Vault 10g Database Control Release 10.2.3.2.0
Copyright (c) 2006, 2009 Oracle Corporation. All rights reserved.
https://oel5updl:5700/av
Oracle Audit Vault 10g is running.
```

Logs are generated in directory `/home/oracle/product/10.2.3/av_1/av/log`

5.6.6 Step 5: Secure Audit Vault Agent

To secure the Audit Vault agent:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
2. Run the `avca secure_agent` command.

For example:

```
oracle:/tmp> avca secure_agent -agentkeystore /tmp/certs/agkeystore -avdn
\"CN=avserver, OU=st, O=example, L=nomadcity, ST=ca, C=us\" -agentdn
\"CN=agent, OU=st, O=example,L=nomadcity, ST=ca, C=us\"
```

See [Section 6.19](#) for detailed information about the `avca secure_agent` command.

Output similar to the following appears; answer the prompts as needed.

```
Enter Audit Vault Agent keystore password: password
Stopping agent...
Agent stopped successfully.
Starting agent...
Agent started successfully.
```

5.7 Updating XDB Certificates

If you need to update the XDB certificate that you obtained from running the `avca generate_csr` command, then follow these steps to ensure that the Oracle wallet uses the updated XDB certificate:

1. Open a shell or command prompt for the Audit Vault Server.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.2](#).
 - **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.
2. Run the `avca remove_certificate` command with the `-certdn` parameter set to the DN of the XDB certificate.

For example:

```
avca remove_cert -certdn -hrdb.example.com \"CN=AV_Server_host_
DN,OU=DBSEC,O=Oracle,ST=CA,C=US\"
```

3. Shut down the Audit Vault Web application.


```
avctl stop_av
```
4. Stop the listener for the Audit Vault database.


```
lsnrctl stop
```
5. Log in to SQL*Plus and then shut down the Audit Vault database.

For example:

```
sqlplus sys as sysoper
Enter password: password
Connected.
```

```
SQL> SHUTDOWN IMMEDIATE
```

6. Restart the Audit Vault database listener.


```
lsnrctl start
```
7. Restart the Audit Vault database.


```
SQL> STARTUP
```
8. Start the Audit Vault Web application

```
avctl start_av
```

9. Generate a new certificate.

For example:

```
avca generate_csr -certdn \"CN=AV_Server_host_DN, OU=DBSEC, O=Oracle, ST=CA, C=US\"  
-out user_certificate.cer
```

10. Import the new certificate.

For example:

```
avca import_cert -cert user_certificate.cer
```

Audit Vault Configuration Assistant (AVCA) Reference

Audit Vault Configuration Assistant (AVCA) is a command-line utility you use to manage various Audit Vault components (for example, adding or dropping collection agents). When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVCA command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 6–1](#) describes the Audit Vault Configuration Assistant commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

Table 6–1 Audit Vault Configuration Assistant Commands

Command	Used Where?	Description
add_agent	Server	Adds a collection agent to Oracle Audit Vault
alter_remedy	Server	Reconfigures the Remedy ticket service to use the settings in the deployment descriptor properties file
alter_smtp	Server	Reconfigures the ticket notification service to use different SMTP server settings
create_credential	Both	Creates or updates a credential to be stored in the wallet
create_wallet	Collection agent	Creates a wallet to hold credentials
deploy_av	Server	Deploys the <code>av.ear</code> file to another node in an Oracle RAC environment
disable_remedy	Server	Disables the Remedy ticket service
disable_smtp	Server	Disables the SMTP configuration
drop_agent	Server	Drops a collection agent from Oracle Audit Vault
enable_remedy	Server	Enables the Remedy ticket service

Table 6–1 (Cont.) Audit Vault Configuration Assistant Commands

Command	Used Where?	Description
<code>enable_smtp</code>	Server	Enables an existing SMTP configuration for the e-mail notification service
<code>generate_csr</code>	Server	Generates a certificate request
<code>-help</code>	Both	Displays help information for the AVCA commands
<code>import_cert</code>	Server	Imports the specified certificate into the wallet
<code>redeploy</code>	Both	Redeploys the <code>av.ear</code> file on the Audit Vault Server system or the <code>AVAgent.ear</code> file on the Audit Vault collection agent system
<code>register_remedy</code>	Server	Registers the Remedy ticket service with Oracle Audit Vault
<code>register_smtp</code>	Server	Registers or removes the Oracle Audit Vault e-mail notification service to use an SMTP server
<code>remove_cert</code>	Server	Removes the specified certificate from the wallet
<code>secure_agent</code>	Collection agent	Secures the Audit Vault collection agent by enabling mutual authentication with Oracle Audit Vault
<code>secure_av</code>	Server	Secures Audit Vault Server by enabling mutual authentication with the Audit Vault collection agent
<code>secure_remedy</code>	Server	Enables the Remedy ticket service to use a secure configuration
<code>secure_smtp</code>	Server	Enables the e-mail notification service to work with a secure SMTP server by specifying the type of connection protocol used to communicate to the SMTP server
<code>set_server_tz</code>	Server	Sets the time zone based on the UTC (GMC) time zone for use in generated reports
<code>set_warehouse_retention</code>	Server	Controls the amount of data kept online in the data warehouse fact table
<code>show_remedy_config</code>	Server	Shows the configuration details of the Remedy ticket service
<code>show_server_tz</code>	Server	Shows the configuration details for the <code>avca set_server_tz</code> command
<code>show_smtp_config</code>	Server	Displays the current SMTP configuration details used by the e-mail notification service
<code>test_remedy</code>	Server	Tests the connection of the Remedy ticket service
<code>test_smtp</code>	Server	Tests the connection of the ticket notification services with the SMTP server

Note: In an Oracle RAC environment, you must run AVCA commands 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.

6.1 add_agent

The `avca add_agent` command adds or registers a collection agent to Oracle Audit Vault. The collection agent is installed on the server that contains the source databases that you plan to audit.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca add_agent -agentname agent_name [-agentdesc desc] -agenthost host
```

Arguments

Argument	Description
<code>-agentname agent_name</code>	Enter a unique name for the collection agent that you want to create.
<code>-agentdesc desc</code>	Enter a description of the collection agent. Optional.
<code>-agenthost host</code>	Enter the name of an agent host name where this collection agent is to be installed.

Usage Notes

- The type of collector that you plan to use determines where you must create the agent. See *Oracle Audit Vault Collection Agent Installation Guide* for more information about deploying the collection agents.
- To find the names and source database locations of existing agents, log in to Audit Vault Console, click the **Configuration** tab, and then click **Agent** to display the Agent page. This page lists the agent, host (source database), port, and user.
- You will be prompted to create an agent user name and password. Oracle Audit Vault grants this user the `AV_AGENT` role and uses this account to start and stop the collectors. It is for internal use only. See the example that follows these usage notes.
- You may want to create one agent user for each agent, in the event that an agent user account is removed in the future. Alternatively, you can create one agent user for all the agents.
- After you create an agent, it is not running. You can start the agent by using the following commands: `avctl start_agent` command, described in [Section 7.9](#).

Example

```
avca add_agent -agentname agent3 -agenthost turbokuksa.us.example.com
```

Adding agent...

Enter agent user name: `agent_user_name`

Enter agent user password: `agent_user_pwd`

Re-enter agent user password: `agent_user_pwd`

Agent added successfully.

6.2 alter_remedy

The `avca alter_remedy` command reconfigures the Remedy trouble ticket service connection to Oracle Audit Vault. The settings are based on the settings in the deployment descriptor properties file, described in [Section 3.7.2](#). In other words, if you want to modify the Remedy trouble ticket service connection to Audit Vault, modify the deployment descriptor properties file and then run this command in the Audit Vault Server. Run this command after each time you modify or move the deployment descriptor properties file. For the full procedure, see [Section 3.7](#).

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca alter_remedy -conf deploymentDescriptor.properties
```

Arguments

Argument	Description
<code>-conf deploymentDescriptor.properties</code>	Enter the path to the deployment descriptor properties file. By default, this file is located in the <code>\$ORACLE_HOME/av/conf</code> directory.

Usage Notes

- Right after you complete the Remedy trouble ticket service configuration, it is enabled and ready to use.
- If the Remedy trouble ticket service is on a secure server, then run the `avca secure_remedy` command ([Section 6.21](#)) after you run `avca register_remedy`.
- To test the configuration, run the `avca test_remedy` command ([Section 6.28](#)).

Example

```
avca alter_remedy -conf $ORACLE_HOME/av/conf/remedy.properties
```

Remedy configuration altered successfully.

6.3 alter_smtp

The `avca alter_smtp` command reconfigures the Oracle Audit Vault e-mail notification service.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca alter_smtp -server IP:port|host:port -sender_id string -sender_email e-mail
-auth|-noauth
```

Arguments

Argument	Description
<code>-server IP:port host:port</code>	Enter the server connection information, either using the IP address or the server name, and the outgoing server port number.
<code>-sender_id string</code>	Enter the user ID of the person responsible for sending the e-mail (that is, the e-mail address that appears after From).
<code>-sender_email e-mail</code>	Enter the e-mail address of the person whose ID you entered for the <code>-sender_email</code> argument, in Request For Comments (RFC) 822 format.
<code>-auth -noauth</code>	Enter one of the following settings: <ul style="list-style-type: none"> ■ <code>-auth</code>: Enables authentication for the recipient user. After you enter the <code>avca alter_smtp</code> command, you are prompted for this user's user name and password. See the example in this section. ■ <code>-noauth</code>: Oracle Audit Vault assumes that the SMTP server needs no authentication. In that case, the command does not prompt for the user name and password interactively. It also ignores any settings for the <code>AVCA_SMTPUSR</code> variable.

Usage Notes

- After you complete the SMTP server connection, it is enabled and ready to use.
- If the SMTP server is a secure server, then run the `avca secure_smtp` command ([Section 6.22](#)) after you run `avca register_smtp`.
- The `AVCA_SMTPUSR` variable is an alternative way that you can use to set the username and password without having the command interactively prompt for the username and password. You can use this variable for scripts that run `AVCA` and do not want manual intervention. Ensure that you set this variable on the Audit Vault Server. For example:

```
setenv AVCA_SMTPUSR user/password
```
- To test the configuration, run the `avca test_smtp` command ([Section 6.29](#)).

Example

```
avca register_smtp kuksanest:3924 -sender rmcmurphy -sender_email
rmcmurphy@example.com -auth
```

```
Enter SMTP server username: dharding
Enter SMTP server password: password
Re-enter SMTP server: password
Credential stored successfully.
SMTP configuration altered successfully.
```

6.4 create_credential

The `avca create_credential` command creates or updates a credential to be stored in an Oracle wallet. Run this command on both the Audit Vault Server and Audit Vault collection agent during collector development.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avca create_credential -wrl wallet_location -dbalias db_alias
```

Arguments

Argument	Description
<code>-wrl wallet_location</code>	Enter the location of the Oracle Audit Vault wallet. Locations are as follows: <ul style="list-style-type: none">■ UNIX and Linux-based systems: <code>\$ORACLE_HOME/network/admin/avwallet</code>■ Microsoft Windows systems: <code>ORACLE_HOME\network\ADMIN\avwallet</code>
<code>-dbalias db_alias</code>	Enter the database alias. In the Audit Vault Server home, the database alias is the SID or Oracle instance identifier. You can find this SID by running the <code>lsnrctl status</code> command on the computer where you installed the source database.

Usage Notes

- Use this command to create a new certificate if another user changes the source user password on the source database, thus eventually breaking the connection between the collector and the source.
- If you installed the collection agent on a Microsoft Windows computer and want to run the `avca create_credential` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.

Example

```
avca create_credential -wrl $ORACLE_HOME/network/admin/avwallet -dbalias av
```

```
AVCA started
Storing user credentials in wallet...
Enter source user username: srcuser1
Enter source user password: password
Re-enter source user password: password
Credential stored successfully.
```

6.5 create_wallet

The `avca create_wallet` command creates a wallet to hold credentials.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avca create_wallet -wrl wallet_location
```

Arguments

Argument	Description
<code>-wrl wallet_location</code>	Enter the directory location for the wallet. Ensure that this directory already exists. Locations are as follows: <ul style="list-style-type: none"> ■ Linux and UNIX-based systems: <code>\$ORACLE_HOME/network/admin/avwallet</code> ■ Microsoft Windows systems: <code>ORACLE_HOME\network\ADMIN\avwallet</code>

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avca create_wallet` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- After you execute this command, then the `.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`:

```
avca create_wallet -wrl $T_WORK/tt_1
Enter wallet password: password
Wallet created successfully.
```

6.6 deploy_av

The `avca deploy_av` command deploys the `av.ear` file to another node in an Oracle Real Application Clusters (Oracle RAC) environment. This command also modifies the `server.xml` file and other related files to enable Oracle Audit Vault management through the Oracle Enterprise Manager Database Control console.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca deploy_av -sid sid -dbalias db_alias -avconsoleport av_console_port
```

Arguments

Argument	Description
<code>-sid <i>sid</i></code>	<p>Enter the Oracle Database system identifier (SID) for the instance. You can verify the SID by running the <code>lsnrctl status</code> command on the computer where you installed the source database.</p> <p>Enter the Oracle Database system identifier (SID) for the Audit Vault Server instance. You can verify the SID by running the <code>lsnrctl status</code> command on the computer where you installed the source database. If you installed the Audit Vault Server in an Oracle RAC configuration, then use the <code>svrctl status listener</code> command.</p>
<code>-dbalias <i>db_alias</i></code>	Enter the database alias for Oracle Audit Vault. The database alias is the value that you provided in the Audit Vault Name field during installation.
<code>-avconsoleport <i>av_console_port</i></code>	<p>Enter the port number for the Audit Vault Console. You can find this number by entering the following command in the Audit Vault Server shell or command prompt:</p> <pre>avctl show_av_status</pre>

Usage Notes

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

If the host on which Oracle Enterprise Manager resides becomes unavailable, you can migrate the Audit Vault Web application file, `av.ear`, to a different node by using the `avca deploy_av` command. After you migrate the Web application, you must recreate the wallet entries for all the source databases managed by Oracle Audit Vault on this new node by using the `avca create_credential` command.

To use the Audit Vault Console from this other node, enter its host name or IP address (*host*) and port number (*port*) as you did previously in the **Address** field of the browser window (`http://host:port/av`), but replace the original host name or IP address with that for the other node.

Example

```
avca deploy_av -sid av -dbalias av -avconsoleport 5700
```

6.7 disable_remedy

The `avca disable_remedy` command disables the Remedy trouble ticket service configuration.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca disable_remedy
```

Arguments

None.

Usage Notes

- After you disable the configuration, Oracle Audit Vault preserves the most recent configuration. So, when you re-enable the configuration, this configuration is made active again.
- To find details about the current Remedy service configuration, issue the `avca show_remedy_config` command, described in [Section 6.25](#).

Example

```
avca disable_remedy
```

```
Remedy integration is disabled.
```

6.8 disable_smtp

The `avca disable_smtp` command disables the SMTP configuration for the e-mail notification service.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca disable_smtp
```

Arguments

None.

Usage Notes

- After you disable the configuration, Oracle Audit Vault preserves the most recent configuration. So, when you re-enable the configuration, this configuration is made active again.
- To find details about the current SMTP configuration, issue the `avca show_smtp_config` command, described in [Section 6.27](#).

Example

```
avca disable_smtp
```

SMTP integration is disabled.

6.9 drop_agent

The `avca drop_agent` disables (but does not remove) a collection agent from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca drop_agent -agentname agent_name
```

Arguments

Argument	Description
<code>-agentname agent_name</code>	Enter the name of the collection agent to be dropped from Oracle Audit Vault.

Usage Notes

- The `drop_agent` command does not delete the collection agent from Oracle Audit Vault. It only disables the collection agent. The collection agent metadata is still in the database after you run the `drop_agent` command. If you want to re-create the collection agent, create it with a different name.
- Oracle Audit Vault displays an error if active collectors are still running in the collection agent.

Example

The following example shows how to drop a collection agent named `sales_agt` from Oracle Audit Vault:

```
avca drop_agent -agentname uberkuksa
```

Agent dropped successfully.

6.10 enable_remedy

The `avca enable_remedy` enables the Remedy trouble ticket service configuration that was registered with the `avca register_remedy` or `avca alter_remedy` command.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca enable_remedy
```

Arguments

None.

Usage Notes

- When you enable the Remedy registration, Oracle Audit Vault uses the configuration that was in place when you last disabled the Remedy trouble ticket service.
- To find details about the most recent Remedy service configuration, issue the `avca show_remedy_config` command, described in [Section 6.25](#).

Example

```
avca enable_remedy
```

Remedy integration is enabled.

6.11 enable_smtp

The `avca enable_smtp` command enables the SMTP configuration for the e-mail notification service that was created with the `avca register_smtp` command.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca enable_smtp
```

Arguments

None.

Usage Notes

- When you enable the configuration, Oracle Audit Vault uses the configuration that was in place when you last disabled the SMTP configuration.
- To find details about the most recent service configuration, issue the `avca show_smtp_config` command, described in [Section 6.27](#).

Example

```
avca enable_smtp
```

SMTP integration is enabled.

6.12 generate_csr

The `avca generate_csr` command generates a certificate request in the format of a text file.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca generate_csr -certdn Audit_Vault_Server_host_DN [-keysize size]
                  -out certificate_request_output_file
```

Arguments

Argument	Description
<code>-certdn Audit_Vault_Server_host_DN</code>	Enter the distinguished name (DN) of the Audit Vault Server host
<code>keysize size</code>	Enter the certificate key size (in bits). Optional. Possible values are: <ul style="list-style-type: none"> ■ 512 ■ 1024 (default) ■ 2048
<code>-out certificate_request_output_file</code>	Enter the path and name of the certificate request output file. Ensure that you have write permissions for this directory.

Usage Notes

- You must use this command to generate a certificate request. After generating the certificate request, send it to your certificate authority (CA) and get it signed and then returned as a signed certificate.

The DN of the Audit Vault Server is typically of the following form:

```
CN=fully_qualified_hostname,OU=Org_Unit,O=Organization,ST=State,C=Country
```

- On Microsoft Windows, enclose the DN in double quotation marks and a backslash (\) character. For example:

```
avca generate_csr -certdn
\"CN=kuksagruvin,OU=DBSEC,O=RisingDoughCo,ST=CA,C=US\" -out user_
c:\oracle\product\10.2.3\avserver\certs\certificate.txt
```

- For detailed information about generating certificate requests when setting up the HTTPS protocol for Oracle Audit Vault, see [Section 5.6](#).
- If you need to update the XDB certificate that you obtained from running the `avca generate_csr` command, see [Section 5.7](#).

Example

The following example shows how to generate a certificate request for UNIX platforms:

```
avca generate_csr -certdn CN=kuksagruvin,OU=DBSEC,O=RisingDoughCo,ST=CA,C=US -out user_certificate.cer
```

```
Generating Certificate request...
```

```
Certificate request generated successfully
```

6.13 -help

The `avca -help` command displays help information for the AVCA commands.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avca -help
```

```
avca command -help
```

Arguments

Argument	Description
<i>command</i>	Enter the name of an AVCA command for which you want help messages to appear

Usage Notes

If you installed the collection agent on a Microsoft Windows computer and want to run the `avca help` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, ensure that you have set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.

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 Configuration commands - AV Server:
```

```
avca deploy_av -sid <sid> -dbalias <db alias> -avconsoleport <av console port>
```

```
avca generate_csr -certdn <Audit Vault Server host DN> [-keysize 512|1024|2048] -out
```

```
<certificate request output file>
```

```
avca import_cert -cert <User/Trusted certificate> [-trusted]
```

```
avca remove_cert -certdn <Audit Vault Server host DN>
```

```
avca secure_av -avkeystore <keystore location> -avtruststore <truststore location>
avca secure_av -remove
avca set_server_tz -offset <[+/-]hh:mm>
avca show_server_tz
```

Oracle Audit Vault Configuration commands - Agent:

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

Oracle Audit Vault Configuration commands - Warehouse:

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

Oracle Audit Vault Configuration commands - SMTP:

```
avca register_smtp -server <host:port> -sender_id <sender id> -sender_email <sender email>
-auth|-noauth
avca register_smtp -remove
avca alter_smtp [-server <host:port>] [-sender_id <sender id>] [-sender_email <sender email>]
[-auth|-noauth]
avca secure_smtp -protocol ssl|tls [-truststore <truststore location>]
avca secure_smtp -remove
avca show_smtp_config
avca enable_smtp
avca disable_smtp
avca test_smtp -to <recipient email>
```

Oracle Audit Vault Configuration commands - Remedy:

```
avca register_remedy -config <remedy config file>
avca register_remedy -remove
avca alter_remedy -config <remedy config file> [-auth]
avca secure_remedy [-truststore <truststore location>]
avca secure_remedy -remove
avca show_remedy_config
avca enable_remedy
avca disable_remedy
avca test_remedy -ticket_id <remedy ticket id>
```

Oracle Audit Vault Configuration commands - Authentication:

```
avca create_wallet -wrl <wallet_location>
avca create_credential -wrl <wallet_location> -wpwd <wallet_pwd> -dbalias <db alias> -usr
<usr>/<pwd>
```

```
avca -help
```

From the Audit Vault collection agent home, the avca -help output is as follows:

```
avca -help

-----
AVCA Usage
-----

Oracle Audit Vault Agent Installation commands
    avca secure_agent -agentkeystore <keystore location> -avdn <DN of Audit
Vault> -agentdn <DN of agent>
    avca secure_agent -remove

Oracle Audit Vault Configuration commands - Authentication:
    avca create_wallet -wrl <wallet_location>
    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>
-----
-agentname <agent name>
[-agentdesc <agent description>]
-agenthost <agent host>
-----
```

6.14 import_cert

The `avca import_cert` command imports the specified user or trusted certificate into the wallet.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca import_cert -cert User/Trusted_certificate [-trusted]
```

Arguments

Argument	Description
<code>-cert User/Trusted_certificate</code>	Enter the path and file name of the certificate to be imported into the wallet. See the usage notes.
<code>-trusted</code>	Include this argument if you want to indicate that the certificate is trusted. If it is a user certificate, then omit the <code>trusted</code> argument. Optional.

Usage Notes

- To obtain the certificate, contact the certificate authority. Place the certificate in a directory that you can easily access, for the `-cert` argument. Ensure that the certificate matches a pending certificate request in the wallet. You must import the trusted certificate for this certificate first.
- For detailed information about configuring wallets when setting up the HTTPS protocol for Oracle Audit Vault, see [Section 5.6](#).

Example

The following example shows how to import a certificate into the wallet.

```
avca import_cert -cert user_certificate.cer
```

```
Importing Certificate...
Certificate imported successfully.
```

This example shows how to import a trusted certificate into the wallet.

```
avca import_cert -cert ca_certificate.cer -trusted
```

```
Importing Certificate...  
Certificate imported successfully.
```

6.15 redeploy

The `avca redeploy` command redeploys the `av.ear` file on the Audit Vault Server system or the `AVAgent.ear` file on the Audit Vault collection agent system.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avca redeploy
```

Arguments

None.

Usage Notes

If you installed the collection agent on a Microsoft Windows computer and want to run the `avca redeploy` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, ensure that you have set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.

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 collection agent system.

```
avca redeploy  
  
Deploying AV web application...  
Getting EM home = stapp03.us.oracle.com_sx4  
Stopping OC4J...  
OC4J stopped successfully.  
Expanding av.ear  
Looking for directory /oracle/work/sx4/oc4j/j2ee/oc4j_applications/applications/av  
Deleting directory /oracle/work/sx4/oc4j/j2ee/oc4j_applications/applications/av  
Creating directory /oracle/work/sx4/oc4j/j2ee/oc4j_applications/applications/av  
Looking for directory /oracle/work/sx4/oc4j/j2ee/oc4j_applications/applications/av/av  
Creating directory /oracle/work/sx4/oc4j/j2ee/oc4j_applications/applications/av/av  
Deploying pre-compiled jsps  
Starting OC4J...  
OC4J started successfully.
```

6.16 register_remedy

The `avca register_remedy` command registers or removes the BMC Remedy Action Request (AR) System Server 7.x trouble ticket service from Oracle Audit Vault. The registration is based on the settings in the deployment descriptor properties file, described in [Section 3.7.2](#). For the full procedure, see [Section 3.7](#). You can register only one Remedy trouble ticket with each Oracle Audit Vault installation.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca register_remedy -config deploymentDescriptor.properties
```

```
avca register_remedy -remove
```

Arguments

Argument	Description
<code>-config deploymentDescriptor.properties</code>	Enter the path to the deployment descriptor properties file. By default, a template for this file is located in the <code>\$ORACLE_HOME/av/conf</code> directory.
<code>-remove</code>	Include this keyword to remove the Remedy trouble ticket service from Oracle Audit Vault.

Usage Notes

- Right after you register the Remedy trouble ticket service configuration, it is enabled and ready to use.
- If the Remedy trouble ticket service is on a secure server, then run the `avca secure_remedy` command ([Section 6.21](#)) after you run `avca register_remedy`.
- To test the configuration, run the `avca test_remedy` command ([Section 6.28](#)).

Examples

The following example demonstrates how to register the Remedy trouble ticket service:

```
avca register_remedy -config $ORACLE_HOME/av/conf/remedy.properties
```

```
Enter Remedy server username: Remedy_server_username
Enter Remedy server password: password
Re-enter Remedy server password: password
Credential stored successfully.
Remedy server registered successfully.
```

The command does not create any users; it just stores the user input in the Oracle wallet.

This example shows how to unregister the Remedy trouble ticket service:

```
avca register_remedy -remove
```

Remedy server unregistered successfully.

6.17 register_smtp

The `avca register_smtp` command registers or unregisters the Oracle Audit Vault e-mail notification service to use an SMTP server. For the full procedure required to complete this type of registration, see [Section 3.6](#).

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca register_smtp -server IP:port|host:port -sender_id string -sender_email  
e-mail -auth|-noauth
```

```
avca register_smtp -remove
```

Arguments

Argument	Description
<code>-server IP:port host:port</code>	Enter the server connection information, either using the IP address or server name, and the outgoing server port number.
<code>-sender string</code>	Enter the user ID of the person responsible for sending the e-mail (that is, the e-mail address that appears after From).
<code>-sender_email e-mail</code>	Enter the e-mail address of the person whose ID you entered for the <code>-sender</code> argument, in Request For Comments (RFC) 822 format.
<code>-auth -noauth</code>	Enter one of the following settings: <ul style="list-style-type: none">■ <code>-auth</code>: Enables authentication for the recipient user. After you enter the <code>avca alter_smtp</code> command, you are prompted for this user's user name and password. See the example in this section.■ <code>-noauth</code>: Oracle Audit Vault assumes that the SMTP server needs no authentication. In that case, the command does not prompt for the username and password interactively. It also ignores any settings for the <code>AVCA_SMTPUSR</code> variable.
<code>-remove</code>	Include this keyword to remove the SMTP service from Oracle Audit Vault.

Usage Notes

- Right after you create the SMTP server connection, it is enabled and ready to use.
- If the SMTP server is a secure server, then run the `avca secure_smtp` command ([Section 6.22](#)) after you run `avca register_smtp`.
- To test the configuration, run the `avca test_smtp` command ([Section 6.29](#)).

Example

```
avca register_smtp -server kuksanest:3924 -sender imanoyd -sender_email
inoydt@example.com -auth
```

Enter SMTP server username: *idaneau*

Enter SMTP server password: *password*

Re-enter SMTP server: *password*

Credential stored successfully.

SMTP configuration registered successfully.

The following example removes the SMTP registration:

```
avca register_smtp -remove
```

SMTP server unregistered successfully.

6.18 remove_cert

The `avca remove_cert` command removes the specified certificate from the wallet.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca remove_cert -certdn Audit_Vault_Server_host_DN
```

Arguments

Argument	Description
<code>-certdn Audit_Vault_Server_host_DN</code>	Enter the distinguished name (DN) of the Audit Vault Server host that was used for the <code>avca generate_csr</code> command.

Usage Notes

- Oracle Audit Vault removes the certificate or key pair for the DN matching the given DN from the wallet. For example, you can use this command to remove a certificate that expires or is revoked by the CA, and replace it with a renewed certificate.

You, the Oracle Audit Vault administrator, provide the DN of the Audit Vault Server is typically of the form:

```
CN=hostname_fully_qualified,OU=Org_Unit,O=Organization,ST=State,C=Country
```

- On Microsoft Windows, enclose the DN in double quotation marks and a backslash (\) character. For example:

```
avca remove_cert -certdn -hrdb.example.com
\"CN=kuksagruvin,OU=DBSEC,O=RisingDoughCo,ST=CA,C=US\"
```

Example

The following example shows how to remove a certificate from the wallet.

```
avca remove_cert -certdn -hrdb.example.com
CN=kuksagruvin,OU=DBSEC,O=RisingDoughCo,ST=CA,C=US
```

```
Removing Certificate...
Certificate removed successfully.
```

6.19 secure_agent

The `avca secure_agent` command secures the Audit Vault collection agent by enabling mutual authentication with the Audit Vault Server. If you specify the `remove` argument, this command removes mutual authentication with the Audit Vault Server.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avca secure_agent -agentkeystore keystore_location
                  -avdn Audit_Vault_Server_host_DN
                  -agentdn agent_DN [-agentkeystore_pwd keystore_pwd]
```

```
avca secure_agent -remove
```

Arguments

Argument	Description
<code>-agentkeystore keystore_location</code>	Enter the keystore file location for this collection agent. See Section 5.6 for more information about the keystore file.
<code>-avdn Audit_Vault_Server_host_DN</code>	Enter the distinguished name (DN) of the Audit Vault Server.
<code>-agentdn agent_DN</code>	Enter the DN of this Audit Vault collection agent.
<code>-remove</code>	Include this keyword to remove mutual authentication with the Audit Vault Server.

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avca secure_agent` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avca secure_agent` command prompts for the agent key password. You can bypass this prompt if the corresponding environment variable, `AVCA_AGENTKEYSTOREPWD` is set. If you enter the password, then it overrides the environment variable. This argument is provided for backward compatibility.

- On Microsoft Windows, enclose the DN in double quotation marks with a backslash (\) character, as shown in the examples following these notes.
- The keystore and certificate must be in place at the collection agent site before you execute this command.
- Use the following command to generate a keystore:
`$ORACLE_HOME/jdk/bin/keytool`
- When you issue the `secure_agent` command for the specified collection agent with both the collection agent and its collectors in a running state, the collection agent and all its collectors will shut down when the agent OC4J shuts down and then restarts. You must manually restart the collection agent and its collectors.
- For detailed information about configuring mutual authentication when setting up the HTTPS protocol for Oracle Audit Vault, see [Section 5.6](#).

Example

The following example shows how to secure the Audit Vault collection agent by enabling mutual authentication with the Audit Vault Server.

```
avca secure_agent -agentkeystore /tmp/agentkeystore
-agentdn \"CN=agent1, OU=sales, O=example, L=nomadcity, ST=ca, C=us\"
-avdn \"CN=av1, OU=sales, O=example, L=nomadcity, ST=ca, C=us\"
```

```
Enter Audit Vault Agent keystore password: password
Stopping agent...
Agent stopped successfully.
Starting agent...
Agent started successfully.
```

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

```
avca secure_agent -remove

Stopping agent...
Agent stopped successfully.
Starting agent...
Agent started successfully.
```

6.20 secure_av

The `avca secure_av` command secures the Audit Vault Server by enabling mutual authentication with the Audit Vault collection agent. If you specify the `remove` argument, this command removes mutual authentication with Audit Vault collection agent.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca secure_av -avkeystore keystore_location -avtruststore truststore_location
[-avkeystorepwd keystore_pwd>]
```

```
avca secure_av -remove
```

Arguments

Argument	Description
<code>-avkeystore <i>keystore_location</i></code>	Enter the keystore file location for the Audit Vault Server. By default, this file is located in the Audit Vault Server home directory. It has the file extension of <code>.keystore</code> . See Section 5.6 for more information about the keystore file.
<code>-avtruststore <i>truststore_location</i></code>	Enter the trust store location for the Audit Vault Server. This file can be the same file as the <code>avkesytore</code> file. Ensure that this file has the CA certificates imported into it.
<code>-remove</code>	Include this keyword to remove mutual authentication with the Audit Vault collection agent

Usage Notes

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

```
$ORACLE_HOME/jdk/bin/keytool
```
- When you issue the `avca secure_av` command, the Audit Vault Console agent OC4J restarts, which requires you to log in to Audit Vault Console again.
- The `avca secure_av` command prompts for the keystore password for the Audit Vault Server. If the corresponding environment variable, `AVCA_AVKEYSTOREPWD`, is set, then you can bypass this prompt. If you enter the password anyway, it overrides the environment variable. This argument is provided for backward compatibility.
- For detailed information about configuring mutual authentication when setting up the HTTPS protocol for Oracle Audit Vault, see [Section 5.6](#).

Example

The following example shows how to secure the Audit Vault Server by enabling mutual authentication with the Oracle Audit Vault collection agent.

```
avca secure_av -avkeystore /tmp/avkeystore -avtruststore /tmp/avkeystore
Enter keystore password: password
```

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

```
avca secure_av -remove

Stopping OC4J...
OC4J stopped successfully.
Starting OC4J...
OC4J started successfully.
Oracle Audit Vault 10g Database Control Release 10.2.3.2.0 Copyright (c)
1996,2008 Oracle Corporation. All rights reserved.
http://av_srv.us.example.com:5700/av
```

Oracle Audit Vault 10g is running.

Logs are generated in directory \$ORACLE_HOME/10.2.3/av_1/av/log

6.21 secure_remedy

The `avca secure_remedy` command enables or disables a secure configuration for the Remedy ticket service. Run this command if the BMC Remedy Action Request System Server is on a secure server.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca secure_remedy -truststore truststore
```

```
avca secure_remedy -remove
```

Arguments

Argument	Description
<code>-truststore truststore</code>	Enter the path to the truststore file used to validate the server certificates. Optional.
<code>-remove</code>	Include this keyword to disable the Remedy ticket service from being a secure configuration.

Usage Notes

- Run this command after you run either the `avca register_remedy` ([Section 6.16](#)) or `avca alter_remedy` ([Section 6.2](#)) command.

Example

```
avca secure_remedy -truststore ca_cert.ce
```

```
Setting Truststore to ca_cert.cer
Updated Remedy server configuration to not use secure protocol.
```

6.22 secure_smtp

The `avca secure_smtp` command enables the e-mail notification service to work with a secure SMTP server by specifying the type of connection protocol used to communicate to the SMTP server. Only run this command if the SMTP server that you are configuring is a secure server.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca secure_smtp -protocol ssl_type -truststore truststore
```

```
avca secure_smtp -remove
```

Arguments

Argument	Description
-protocol <i>ssl_type</i>	Specify one of the following types of protocol: <ul style="list-style-type: none"> ■ SSL: Secure Sockets Layer (default) ■ TLS: Transport Layer Security
-truststore <i>truststore</i>	Enter the path to the truststore file used to validate the server certificates. Optional.
-remove	Include this keyword to disable the e-mail notification service from being a secure configuration.

Usage Notes

Run this command after you run either the `avca register_smtp` (Section 6.17) or `avca alter_smtp` (Section 6.3) command.

Examples

The following example shows how to configure the truststore to use the TLS protocol:

```
avca secure_smtp -protocol tls -truststore $ORACLE_HOME/wallets/smtp_keystore
```

Updated SMTP server configuration to use secure protocol.

These example demonstrates how to disable the e-mail configuration service:

```
avca secure_smtp -remove
```

Updated SMTP server configuration to not use secure protocol.

6.23 set_server_tz

The `avca set_server_tz` command sets the time zone format for Oracle Audit Vault reports and alerts, using an offset of the UTC time zone. It takes effect the next time you generate a report or an alert. Use this command if the time stamps in the generated Audit Vault reports and alerts must be in a time zone other than UTC. (The Audit Vault Server itself always uses the UTC time zone.)

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in Section 2.2.2.
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca set_server_tz -offset offset_value
```

Arguments

Argument	Description
<code>-offset <i>offset_value</i></code>	Enter the offset value in the following format: +/-HH:MM

Usage Notes

To find the current UTC time zone setting, run the `avca show_server_tz` command, described in [Section 6.26](#).

Example

The following example shows how to set the offset value for U.S. Pacific Daylight Time (PDT):

```
avca set_server_tz -offset +07:00
```

Updated timezone offset successfully.

6.24 set_warehouse_retention

The `avca set_warehouse_retention` command controls the amount of data kept online in the data warehouse fact table.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca set_warehouse_retention -intrv year_month_interval
```

Arguments

Argument	Description
<code>-intrv <i>year_month_interval</i></code>	Enter the year-month interval in the following format: +YY-MM

Usage Notes

- The interval setting must be a positive value.
- As the retention period shifts forward in time, Oracle Audit Vault removes the data that was loaded before the retention period. For example, if you set the retention period for 1 year, any data before that year is discarded.
- See [Section 3.4](#) for detailed information about creating a retention period.

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 1 year and 6 months is specified.

```
avca set_warehouse_retention -intrv +01-06
```

```
AVCA started
Setting warehouse retention period...
done.
```

6.25 show_remedy_config

The `avca show_remedy_config` command displays the configuration for the Remedy trouble ticket service connection with Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca show_remedy_config
```

Arguments

None.

Usage Notes

To reconfigure the Remedy trouble ticket service connection, run the `avca alter_remedy` ([Section 6.2](#)) command.

Examples

In the following example, the Remedy trouble ticket service has not been registered:

```
avca show_remedy_config

Error executing command show_remedy_config
OAV-46856: no remedy server registered
```

In this example, the Remedy trouble ticket service has been successfully registered:

```
avca show_remedy_config

Remedy server configuration details:
-----
Action Request host: kuksavoid.com
Mid-tier host: kuksavoid.com
Mid-tier port: 3128
Version: 7.5
Helpdesk Form name: HPD:IncidentInterface
Create Ticket URL:
http://kuksavoid.com:3128/arsys/services/ARService?server=kuksavoid&webService=HPD_IncidentInterface_Create_WS
Get Ticket URL:
http://kuksavoid.example.com:3128/arsys/services/ARService?kuksavoid=shobeen&webService=HPD_IncidentInterface_WS
Auth String: None
Locale: en_US
Locale: UTC
Security protocol: None
User name: Remedy_server_username
Password: *****
State: Enabled
```

6.26 show_server_tz

The `avca show_server_tz` shows the configuration details for the `avca set_server_tz` command.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca show_server_tz
```

Arguments

None.

Usage Notes

To set the UTC time zone for reports and alerts, run the `avca set_server_tz` command, described in [Section 6.23](#).

Example

```
avca show_server_tz
```

```
Server Timezone UTC07:00
```

6.27 show_smtp_config

The `avca show_smtp_config` command displays the current SMTP configuration details used by Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca show_smtp_config
```

Arguments

None.

Usage Notes

To reconfigure the SMTP service connection, run the `avca alter_smtp` ([Section 6.3](#)) command.

Example

```
avca show_smtp_config
```

```
SMTP server configuration details:
-----
Host: kuksanest.example.com
Port: 465
Sender name: ida.neau@example.com "<ida.neau@example.com>"
Security protocol: SSL
Truststore: Default
Authentication required: No
State: Enabled
-----
```

6.28 test_remedy

The `avca test_remedy` command tests the Remedy ticket service connection for the provided ticket ID. You can enter any Remedy ticket number, not just Oracle Audit Vault-related Remedy ticket numbers.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca test_remedy -ticket_id
```

Arguments

Argument	Description
<code>-ticket_id id</code>	Enter the ID of any Remedy ticket in your system.

Usage Notes

- If the test fails, then check the configuration by running the `avca show_remedy_config` ([Section 6.25](#)) and `avctl show_remedy_status` ([Section 7.7](#)) commands.
- You can recreate the configuration by running the `avca alter_remedy` command ([Section 6.2](#)).

Example

```
avca test_remedy -ticket_id INC0000000000005
```

```
Querying Remedy Server for ticket ID "INC0000000000005"...
Assigned Group: Backoffice Support
Assigned Support Company: Calbro Services
Assigned Support Organization: IT Support
Assignee: Allen Allbrook
Summary: Test Ticket manually
Priority: Low
Service Type: Infrastructure Event
Status: Assigned
Urgency: 4-Low
```


6.29 test_smtp

The `avca test_smtp` command tests the Oracle Audit Vault e-mail notification service.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avca test_smtp -to e-mail
```

Arguments

Argument	Description
<code>-to e-mail</code>	Recipient to whom to send the test e-mail notification.

Usage Notes

- If the test fails, then check the configuration by running the `avca show_smtp_config` ([Section 6.27](#)) and `avctl show_smtp_status` ([Section 7.8](#)) commands.
- You can recreate the configuration by running the `avca alter_smtp` command ([Section 6.3](#)).

Example

```
avca test_smtp -to ida.kuksa@example.com
```

Sending Test e-mail to "ida.kuksa@example.com"...

Test e-mail sent successfully. Please check the recipients mailbox to see if the e-mail has been delivered.

In this example, user Ida Kuksa should receive an e-mail similar to the following:

- **Subject header:** Oracle Audit Vault: Test Message
- **Body text:** This is a test message from Oracle Audit Vault

If the test fails, then an error message similar to the following appears:

Sending Test e-mail to "ida.kuksa@example.com"...

Error: SEND_EMAIL_ERROR. Message is: Sending failed;

nested exception is:

 javax.mail.MessagingException: Unknown SMTP host: shobeen.example.com;

nested exception is:

 java.net.UnknownHostException: shobeen.example.com.

See the Usage Notes for advice on handling this situation.

Audit Vault Control (AVCTL) Reference

Use the Audit Vault Control (AVCTL) command-line utility to manage various Oracle Audit Vault components (for example, checking the status of collector agents or managing the Audit Vault Data Warehouse). When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVCTL command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 7–1](#) describes the Audit Vault Control commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

[Section 7.15](#) describes the commands you must use if you must start, stop, or check the status of collection agents that were that have not been upgraded to this release.

Table 7–1 Audit Vault Control Commands for Release 10.2.3.2

Command	Where Used	Description
-help	Both	Displays help information 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 audit data that was reloaded into the warehouse
show_agent_status	Collection agent	Shows the status (metric) of a collection 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_remedy_status	Server	Shows the status of the Remedy ticket service
show_smtp_status	Server	Indicates whether the SMTP service that you configured is running or not running
start_agent	Collection agent	Starts the collection agent

Table 7–1 (Cont.) Audit Vault Control Commands for Release 10.2.3.2

Command	Where Used	Description
start_av	Server	Starts the Audit Vault Console
start_collector	Server	Starts the collector
stop_agent	Collection agent	Stops the collection agent
stop_av	Server	Stops the Audit Vault Console
stop_collector	Server	Stops the collector

Note: In an Oracle RAC environment, you must issue the AVCTL commands 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, described in [Section 6.6](#).

7.1 -help

The `avctl -help` command displays help information for the AVCTL commands.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avctl -help
```

```
avctl command -help
```

Arguments

Argument	Description
<i>command</i>	Enter the name of an AVCTL command for which you want help to appear

Usage Notes

If you installed the collection agent on a Microsoft Windows computer and want to run the `avctl help` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.

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 - 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 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]

Oracle Audit Vault Control commands - SMTP:
    avctl show_smtp_status

Oracle Audit Vault Control commands - Remedy:
    avctl show_remedy_status

avctl -help
```

From the Audit Vault collection agent home, the `avctl -help` output is as follows:

```
avctl -help

-----
AVCTL Usage
-----
Oracle Audit Vault Control commands - Agent:
    avctl start_agent [-loglevel error|warning|info|debug] [-maxheapsize
<maximum heap memory>]
    avctl stop_agent
    avctl show_agent_status

avctl -help
```

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

```
avctl load_warehouse -help

    avctl load_warehouse -startdate <start date> -numofdays <num of days>
[-dateformat <date format>] [-wait]
-----
-startdate <start date>
-numofdays <num of days>
-dateformat <date format>
-wait : Wait till load job finishes
-----
```

7.2 load_warehouse

The `avctl load_warehouse` command loads audit trail data from the raw audit data store after it has been removed from the warehouse repository due to the retention period that was set.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl load_warehouse -startdate start_date -numofdays num_of_days
                        [-dateformat date_format] [-wait]
```

Arguments

Argument	Description
<code>-startdate start_date</code>	Enter the start date for the audit trail data to be loaded into the data warehouse repository using the default format DD-MON-YY. To use a different format, specify the <code>-dateformat</code> argument. Use any supported Oracle Database date format. See <i>Oracle Database Globalization Support Guide</i> for more information about date formats.
<code>-numofdays num_of_days</code>	Enter the number of days' worth of audit trail data to be loaded.
<code>-dateformat date_format</code>	Enter the date format for the <code>-startdate</code> argument. Optional. Ensure that the date argument used for <code>startdate</code> matches the date format you choose. For Oracle Database supported date formats, see <i>Oracle Database Globalization Support Guide</i> .
<code>-wait</code>	Enter the command wait for the load job to complete. If you do not specify this argument, a DBMS job is started, and the command returns immediately. Optional.

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.
- See [Section 3.4](#) for more information about managing the Oracle Audit Vault 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
```

```
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 using the DD/MM/YYYY date format, and to specify that the operation wait until the previous load job completes.

```
avctl load_warehouse -startdate 01/01/2004 -numofdays 10 -dateformat DD/MM/YYYY -wait
```

```
Loading older audit records into warehouse...
```

```
Waiting for load to complete...
```

```
done.
```

7.3 purge_warehouse

The `avctl purge_warehouse` command purges audit trail data from the warehouse repository that was previously loaded into the warehouse using the `avctl load_warehouse` command.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl purge_warehouse -startdate start_date -numofdays num_of_days
                        [-dateformat date_format] [-wait]
```

Arguments

Argument	Description
<code>-startdate start_date</code>	Enter 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 <code>-dateformat</code> argument. Use any supported Oracle Database date format. See <i>Oracle Database Globalization Support Guide</i> for more information about date formats.
<code>-numofdays num_of_days</code>	Enter the number of days' worth of data to be removed.
<code>-dateformat date_format</code>	Specify the date format for the <code>-startdate</code> argument. Optional.
<code>-wait</code>	Optionally, enter this keyword to have the command wait for the purge job to complete. If you omit this argument, then Oracle Audit Vault starts the job and then returns to the command prompt immediately. Optional.

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 `avctl purge_warehouse` command. The data that was loaded before the retention period set by the `avca set_warehouse_retention` command is automatically discarded.

- See [Section 3.4](#) for more information about managing the Oracle Audit Vault data warehouse.

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
```

```
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
```

```
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
```

```
Purging older audit records from warehouse...  
done.
```

7.4 show_agent_status

The `avctl show_agent_status` command shows the status (metric) of an Oracle Release 10.2.3.2 collection agent.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avctl show_agent_status
```

Arguments

None

Usage Notes

This command applies only to collection agents that were created in Oracle Audit Vault Release 10.2.3.2. For collection agents that were created in earlier releases but not yet upgraded, use the `avctl show_oc4j_status` command, described in [Section 7.15.1](#).

Example

The following example shows the collection agent status for the `sales_agt` agent:

```
avctl show_agent_status

-----
Agent is running
-----
```

7.5 show_av_status

The `avctl show_av_status` command shows the Audit Vault Console status or the metric of the Audit Vault Server.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

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

Oracle Audit Vault 10g Database Control Release 10.2.3.2.0 Copyright (c) 1996,
 2009 Oracle Corporation. All rights reserved.
http://hrdb.us.example.com:5700/av
Oracle Audit Vault 10g is running.
-----
Logs are generated in directory /oracle/product/10.2.3/av_1/av/log
```

7.6 show_collector_status

The `avctl show_collector_status` command shows the status (metric) of a collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl show_collector_status -collname collector_name -srcname source_name
```

Arguments

Argument	Description
-collname <i>collector_name</i>	Enter the target collector (by collector name).
-srcname <i>source_name</i>	Enter the name of the source database 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 hr_db
```

```
Getting collector metrics...
-----
Collector is running
Records per second = 0.00
Bytes per second = 0.00
-----
```

7.7 show_remedy_status

The `avctl show_remedy_status` command shows the status of the Remedy trouble ticket service, that is, whether it is active or inactive.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl show_remedy_status
```

Arguments

None

Usage Notes

To enable or disable the Remedy trouble ticket service connection with Oracle Audit Vault, run the `avca enable_remedy` ([Section 6.10](#)) or `avca disable_remedy` ([Section 6.7](#)) command.

Example

```
avctl show_remedy_status
```

```
Remedy Server is up and reachable
```

7.8 show_smtp_status

The `avca show_smtp_status` command indicates whether the SMTP service that you configured is running or not running.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl show_smtp_status
```

Arguments

None.

Usage Notes

To enable or disable the SMTP connection with Oracle Audit Vault, run the `avca enable_smtp` ([Section 6.11](#)) or `avca disable_smtp` ([Section 6.8](#)) command.

Examples

In this example, the SMTP server is available:

```
avctl show_smtp_status
```

```
SMTP Server is up and reachable
```

In the following example, the SMTP server is unavailable:

```
avctl show_smtp_status
```

```
SMTP Server is down
```

7.9 start_agent

The `avctl start_agent` command starts the specified Oracle Audit Vault Release 10.2.3.2 collection agent.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avctl start_agent [-loglevel level] [-maxheapsize maximum_heap_memory]
```

Arguments

Argument	Description
<code>-loglevel <i>level</i></code>	<p>Optionally, enter the desired level of logging from the following options:</p> <ul style="list-style-type: none"> ■ <code>error</code>: Logs only error messages ■ <code>warning</code>: Logs both warning and error messages ■ <code>info</code>: Logs informational and error messages (default) ■ <code>debug</code>: Logs debug, error, warning, and informational messages
<code>-maxheapsize <i>maximum_heap_memory</i></code>	<p>Optionally, enter the maximum amount of heap memory allocated for the Java OC4J process that is used to start the agent. The default value is 1000 MB.</p> <p>This setting enables you to fine-tune the agent performance based on the size of your Oracle Audit Vault installation. Check the size of the physical memory of the computer on which the Audit Vault collection agents are installed before setting this value.</p>

Usage Notes

- On successful completion of this command, the collection agent is moved to a RUNNING state. If an error is encountered, the collection agent is moved to an ERROR state.
- Oracle Audit Vault accepts audit records only from collection agents in the RUNNING state.
- If you set the `NLS_LANG` environment value before running the `avctl start_agent` command in the Audit Vault collection agent shell or command prompt, then the `avctl start_collector` command can accept a multibyte source name or collector name.
- This command applies only to collection agents that were created in Oracle Audit Vault Release 10.2.3.2. For collection agents that were created in earlier releases, use the `avctl start_oc4j` command, described in [Section 7.15.2](#).

Example

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

```
avctl start_agent -maxheapsize 500M
```

```
Starting Agent...
Agent started successfully.
```

7.10 start_av

The `avctl start_av` command starts the Audit Vault Console.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl start_av [-loglevel level]
```

Arguments

Argument	Description
-loglevel <i>level</i>	Optionally, enter the desired level of logging from the following options. <ul style="list-style-type: none"> ■ error: Logs only error messages ■ warning: Logs both warning and error messages ■ info: Logs informational and error messages (default) ■ debug: Logs debug, error, warning, and informational messages

Usage Notes

This command executes the `emctl start dbconsole` command.

Example

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

```
avctl start_av
```

```
Starting OC4J...
OC4J started successfully.
Oracle Audit Vault 10g Database Control Release 10.2.3.2.0 Copyright (c)
1996,2009 Oracle Corporation. All rights reserved.
http://kksaland.us.example.com:5700/av
Oracle Audit Vault 10g is running.
-----
Logs are generated in directory /oracle/product/10.2.3/av_1/av/log
```

7.11 start_collector

The `avctl start_collector` command starts the collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl start_collector -collname collector_name -srcname source_name
```

Arguments

Argument	Description
-collname <i>collector_name</i>	Enter the name of the collector to be started.
-srcname <i>source_name</i>	Enter the name of the source database to which the collector (specified in the -collname argument) belongs.

Usage Notes

- On successful completion of this command, Oracle Audit Vault sets the collector to a `RUNNING` state. If an error is encountered, the collector is set to an `ERROR` state.

If you receive a message saying that the collector is not in a `RUNNING` state, ensure that the agent has been started. Run the `avctl start_agent` command to start the agent, as described in [Section 7.9](#).

- Oracle Audit Vault accepts audit records only from collectors in the `RUNNING` state.
- If you set the `NLS_LANG` environment value before running the `avctl start_agent` command in the Audit Vault Agent shell or command prompt, or `avctl start_collector` command in the Audit Vault Server shell or command prompt, then the `avctl start_collector` command can accept a multibyte source name or collector name.

Example

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

```
avctl start_collector -collname DBAUD_Collector -srcname hr_db
```

```
Starting Collector...  
Collector started successfully.
```

7.12 stop_agent

The `avctl stop_agent` command stops the Oracle Audit Vault Release 10.2.3.2 collection agent and OC4J.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avctl stop_agent
```

Arguments

None.

Usage Notes

- Before you stop a collection agent, you must stop the collectors that are associated with the collection agent. See [Section 7.14](#) for information about the `avctl stop_collector` command. To find the status of a collector, run the `avctl show_collector_status` ([Section 7.6](#)).
- On successful completion of this command, the collection agent and its collectors are moved to a `STOPPED` state.
- If an error is encountered, Oracle Audit Vault sets the collection agent to an `ERROR` state. Oracle Audit Vault accepts audit records only from collection agents in the `RUNNING` state.

- This command applies only to collection agents that were created in Oracle Audit Vault Release 10.2.3.2. For collection agents that were created in earlier releases but have not yet been upgraded, use the `avctl stop_oc4j` command, described in [Section 7.15.3](#).

Example

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

```
avctl stop_agent

Stopping agent...
Agent stopped successfully.
```

7.13 stop_av

The `avctl stop_av` command stops the Audit Vault Console.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl stop_av
```

Arguments

None

Usage Notes

Oracle Audit Vault includes Enterprise Management Database Control as part of the user interfaces. When you issue the `stop_av` command, it not only shuts down the Audit Vault Console, but it also stops Enterprise Management Database Control by executing the `emctl stop dbconsole` command. You do not need to issue the `emctl` command separately.

Example

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

```
avctl stop_av

Stopping OC4J...
OC4J stopped successfully.
```

7.14 stop_collector

The `avctl stop_collector` command stops the collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avctl stop_collector -collname collector_name -srcname source_name
```

Arguments

Argument	Description
-collname <i>collector_name</i>	Enter the name of the collector to be stopped.
-srcname <i>source_name</i>	Enter the name of the source database to which the collector (specified in the -collname argument) belongs.

Usage Notes

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

Example

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

```
avctl stop_collector -collname DBAUD_Collector -srcname hr_db
```

```
Stopping Collector...
Collector stopped successfully.
```

7.15 AVCTL Commands Used for Release 10.2.3.1 Collection Agents

If you have upgraded from an earlier release of Oracle Audit Vault and have upgraded the collection agents from that release as well, then you can use the `avctl show_agent_status`, `avctl start_agent`, and `avctl stop_agent` commands on these collection agents.

Table 7–2 lists commands that you must use if you have upgraded from a previous release of Oracle Audit Vault but have not yet upgraded the collection agents from that release.

Table 7–2 Audit Vault Control Commands for Release 10.2.3.1

Command	Where Used	Description
show_oc4j_status	Collection agent	Shows the status of the agent OC4J
start_oc4j	Collection agent	Starts OC4J and collection agents
stop_oc4j	Collection agent	Stops OC4J and collection agents

7.15.1 show_oc4j_status

The `avctl show_oc4j_status` command shows the status of agent OC4J for collection agents that were created in Release 10.2.3.1 or earlier. For collection agents created in Release 10.2.3.2, it shows the status of the collection agent.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent *ORACLE_HOME\bin* directory.

Syntax

```
avctl show_oc4j_status
```

Arguments

None

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avctl show_oc4j_status` command from the *ORACLE_HOME\bin* directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avctl show_oc4j_status` command is deprecated, but you can use it to find the status of collection agents that were created in Release 10.2.3.1 or earlier. If the agent was created in Release 10.2.3.2, then use the `avctl show_agent_status` command instead.

Example

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

```
avctl show_oc4j_status
```

```
-----
OC4J is running
-----
```

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

```
avctl show_oc4j_status
```

```
-----
OC4J is not running
-----
```

7.15.2 start_oc4j

The `avctl start_oc4j` command starts the collection agents that were created in Release 10.2.3.1 or earlier.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent *ORACLE_HOME\bin* directory.

Syntax

```
avctl start_oc4j [-loglevel level] [-maxheapsize maximum_heap_memory]
```

Arguments

Argument	Description
<code>-loglevel <i>level</i></code>	<p>Optionally, enter the desired level of logging from the following options:</p> <ul style="list-style-type: none"> ■ <code>error</code>: Logs only error messages ■ <code>warning</code>: Logs both warning and error messages ■ <code>info</code>: Logs informational and error messages (default) ■ <code>debug</code>: Logs debug, error, warning, and informational messages
<code>-maxheapsize <i>maximum_heap_memory</i></code>	<p>Enter the maximum amount of heap memory allocated for the Java OC4J process. The default value is 1000 MB. Optional.</p> <p>This setting enables you to fine-tune the OC4J performance based on the size of your Oracle Audit Vault installation. Check the size of the physical memory of the computer on which the Audit Vault collection agents are installed before setting this value.</p>

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avctl start_oc4j` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- If you set the `NLS_LANG` environment value before running the `avctl start_oc4j` command in the Audit Vault Agent shell or command prompt, or `avctl start_collector` command in the Audit Vault Server shell or command prompt, it will ensure that the `avctl start_collector` command can accept with a multibyte source name or collector name.
- For collection agents that were created for Oracle Audit Vault Release 10.2.3.2, OC4J is automatically started when you run the `avctl start_agent` command.
- The `avctl start_oc4j` command is deprecated, but you can use it to start collection agents that were created in Release 10.2.3.1 or earlier. If the agent is was created in Release 10.2.3.2, then use the `avctl start_agent` command instead.

Example

The following example shows how to start OC4J. For the `-maxheapsize` setting, include `M` (for megabytes) as shown below. You can set it for other sizes, such as `G` for gigabyte, but in most cases, you should set it in megabytes.

```
avctl start_oc4j -maxheapsize 500M
```

```
Starting OC4J...
OC4J started successfully.
```

7.15.3 stop_oc4j

The `avctl stop_oc4j` command stops the agent OC4J and the collection agent.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avctl stop_oc4j
```

Arguments

None

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avctl stop_oc4j` command from the `ORACLE_HOME\bin` directory. For UNIX installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avctl stop_oc4j` command is deprecated, but you can use it to stop collection agents that were created in Release 10.2.3.1 or earlier. If the agent is was created in Release 10.2.3.2, then use the `avctl stop_agent` command instead.

Example

The following example shows how to stop OC4J and the Audit Vault agent:

```
avctl stop_oc4j
```

```
Stopping OC4J...  
OC4J stopped successfully.
```


Audit Vault Oracle Database (AVORCLDB) Utility Commands

Use the Audit Vault Oracle Database (AVORCLDB) command-line utility to manage the relationship between Oracle Audit Vault and an Oracle source database and collector. When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVORCLDB command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 8–1](#) describes the AVORCLDB commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

Table 8–1 AVORCLDB Commands

Command	Where Used?	Description
add_collector	Server	Adds a collector to Oracle Audit Vault
add_source	Server	Registers an audit source with Oracle 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 Oracle Audit Vault
drop_source	Server	Drops a source database from Oracle Audit Vault
-help	Both	Displays help information for the AVORCLDB commands
setup	Collection agent	Adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, verifies the connection to the source using the wallet, and updates the <code>tnsnames.ora</code> file
verify	Both	Verifies that the source is compatible with the collectors that are specified for setup

8.1 avorcldb

The AVORCLDB command-line utility, which you use to configure an Oracle database with Oracle Audit Vault.

Syntax

```
avorcldb command -help
```

```
avorcldb command [options] arguments
```

Arguments

Argument	Description
<i>command</i>	Enter one of the commands listed in Table 8-1 on page 8-1.
<i>arguments</i>	Enter one or more of the AVORCLDB command arguments.
-help	Displays help information for the AVORCLDB commands.

Usage Notes

Issuing an AVORCLDB command generates the following log file: \$ORACLE_HOME/av/log/avorcldb.log.

8.2 add_collector

The avorcldb add_collector command adds a collector for the given Oracle source database to Audit Vault. Oracle Audit Vault verifies the source database for the collector requirements.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server *ORACLE_HOME\bin* directory.

Syntax

```
avorcldb add_collector -srcname srcname
-agentname agentname -colltype [OSAUD,DBAUD,REDO]
[-collname collname] [-desc desc]
[-av host:port:service] [-instname instname] [-orclhome orclhome]
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the source database name for which the collector is to be added. This source name was displayed after you ran the avorcldb add_source command. Remember that the source database name is case-sensitive.

Argument	Description
<code>-agentname agentname</code>	<p>Enter the name of the collection agent that was created when you ran the <code>avca add_agent</code> command. (In most cases, this is the agent that you created when you installed the Audit Vault collection agent, as described in <i>Oracle Audit Vault Collection Agent Installation Guide</i>.)</p> <p>If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the Configuration tab, and then click the Agent tab to display the Agents page. The name of the agent is displayed in the Agent column.</p>
<code>-colltype colltype</code>	<p>Enter the collector type to be added.</p> <ul style="list-style-type: none"> ■ DBAUD ■ OSAUD ■ REDO <p>See Table 1-5 on page 1-8 for more information about the collector types.</p>
<code>-collname collname</code>	Create a name for the collector. Optional. If you do not create a name, Oracle Audit Vault names the collector <code>colltype_Collector</code> (for example, <code>OSAUD_Collector</code> for the OSAUD collector type).
<code>-desc desc</code>	Enter a brief description of the collector. Optional.
<code>-av host:port:service</code>	Enter the connection information for Oracle Audit Vault used for the database link from the source database to Oracle Audit Vault. You must include this argument if the <code>-colltype</code> argument is REDO; otherwise, this argument is optional.
<code>-instname instname</code>	Enter the instance name of Audit Vault Oracle RAC installation. You must include this argument if you are adding multiple OSAUD collectors, that is, one collector for each database instance.
<code>-orclhome orclhome</code>	Enter the Oracle home of the source database. You must include this argument if the <code>-colltype</code> argument is OSAUD; otherwise, this argument is optional. See the usage notes.

Usage Notes

- Run any collector-specific preparation scripts before you run the `avca add_collector` command.
- On Microsoft Windows systems, specifying the OSAUD collector type automatically includes the event log and XML audit trails.
- When specifying the value for the `-orclhome` argument, enter the value as either a quoted string using a backslash. For example:


```
-orclhome "c:\app\oracle\product\10.2.3\av_1"
```

Alternatively, enter it as a nonquoted string using a slash. For example:

```
-orclhome c:/app/oracle/product/10.2.3/av_1
```
- There is a 2 gigabyte audit file size limit for the OSAUD collector to be able to collect audit records from audit trails stored in files, which includes the SYSLOG,

.AUD, and .XML files. If the file size is greater than 2 gigabytes, then the OSAUD collector ignores all audit records beyond 2 gigabytes. To control the size of the operating system audit trail and select the audit trail type to set, set the DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE property and the DBMS_AUDIT_MGMT.AUDIT_TRAIL_TYPE type by using the DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY PL/SQL procedure. See *Oracle Database Security Guide* for more information.

- You can create a collection agent to remotely collect from a source database on a different server, but this collection agent cannot collect audit data from users who have logged in with the SYSDBA or SYSOPER privilege.
- To configure collection agents to listen to Oracle Real Application Clusters (Oracle RAC) nodes, see [Section 4.7](#).
- To modify the collector, use the `avorcldb alter_collector` command ([Section 8.4](#)).

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.

```
avorcldb add_collector -srcname orcl
-agentname kuksagruvin_os -colltype OSAUD -collname OSAUD_Collector -instname av01
-orclhome /u01/app/oracle/product/10.2.0/db_1
```

```
source hr_db 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
```

This example shows how to add a DBAUD collector to Oracle Audit Vault:

```
avorcldb add_collector -srcname source1db.example.com

-agentname kuksagruvin_dbuaud -colltype DBAUD
source hr_db 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 next example shows how to add a REDO collector to Oracle Audit Vault.

```
avorcldb add_collector -srcname source1db.example.com
-agentname kuksagruvin_redo -colltype REDO
-av system1.example.com:1521:av

source hr_db 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

```

8.3 add_source

The `avorcldb add_source` command registers an Oracle source database with Oracle Audit Vault for audit data consolidation. Run this command on the Audit Vault Server.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```

avorcldb add_source -src host:port:service
                    [-srcname srcname] [-desc desc] [-agentname agentname]

```

Arguments

Argument	Description
<code>-src host:port:service</code>	Enter the source database connection information: host name, port number, and service ID (SID), separated by a colon. If you are unsure of this connection information, run the <code>lsnrctl status</code> command on the computer where you installed the source database.
<code>-srcname srcname</code>	Enter the name of the source database. Remember that the source database name is case-sensitive. Optional. If you do not specify this argument, then Oracle Audit Vault uses the global database name. You can check this name by querying the <code>GLOBAL_NAME</code> data dictionary view in SQL*Plus. For example: <code>SQL> SELECT * FROM GLOBAL_NAME;</code>
<code>-desc desc</code>	Enter a brief description of the source database. Optional.
<code>-agentname agentname</code>	Enter the name of the agent. If you omit this name, then Oracle Audit Vault uses the name of the agent that you created during the agent installation process. Optional.

Usage Notes

- The global database name of the source database is used as the default source name in Oracle Audit Vault. You can provide a different name if you want.
- The `avorcldb add_source` command prompts for the source user name and password. This user account must exist on the source database.

To find this user, query the `SESSION_PRIVS` and `SESSION_ROLES` data dictionary views. The source user should have the privileges and roles that are listed in the `zarsspriv.sql` file, such as the `CREATE DATABASE LINK` privilege and `DBA` role.

If the AVORCLDB_SRCUSR environment variable is set to this user account and password, then you can bypass the Enter Source user name and Enter Source password prompts. If you do specify these values, they override the environment variable.

- You must specify the `-agentname agentname` parameter so that auditors can configure policy management using the Audit Vault Console.

Example

The following example shows how to register a source database with Oracle Audit Vault.

```
avorcldb add_source -src hrdb.example.com:1521:orcl -srcname hr_db -agentname
agent1
Enter Source user name: username
Enter Source password: password
```

```
Adding source...
Source added successfully.
source successfully added to Audit Vault
```

```
remember the following information for use in avctl
Source name (srcname): hr_db
Credential stored successfully
Mapping Source to Agent...
```

8.4 alter_collector

The `avorcldb alter_collector` command modifies the attributes of an Oracle Database collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb alter_collector -srcname srcname -collname collname
[attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database to which this collector belongs. Remember that the source database name is case-sensitive.
<code>-collname collname</code>	Enter the name of the collector to be modified.
<code>attrname=attrvalue</code>	Enter the attribute pair (attribute name, new attribute value) for mutable collector attributes for this collector type. This argument is optional. Enclose the attribute value in double quotation marks. For multiple values, enclose the entire set in double quotation marks and separate each value with a space. For example: ...="value1 value2 value3"

Usage Notes

- You can modify one or more collector attributes at a time. The following tables list the collector attributes (parameters) by collector type, whether the parameter is mutable, and its default value. See [Section 3.3](#) for a description of these attributes.
- Note the following case-sensitivity guidelines for specifying attributes:
 - Except for the AGENTNAME attribute, the attribute names are case sensitive. Enter them in upper-case letters.
 - All the attribute values, including the AGENTNAME attribute value, are case sensitive. Enter them in the case shown the following tables.
- To configure collection agents to listen to Oracle Real Application Clusters (Oracle RAC) nodes, see [Section 4.7](#).
- See also the Usage Notes for the avorcldb add_collector command ([Section 8.2](#)).

[Table 8–2](#) describes the DBAUD collector attributes.

Table 8–2 DBAUD Collector Attributes

Attribute	Description	Mutable	Default Value
AGENTNAME	Name of an agent to replace the agent that was specified by the avorcldb add_collector command that was used for this source database. This feature enables you to move a collector from one agent to another. It is useful for failover recovery if the host computer running the original agent fails. This attribute only applies to the DBAUD collector. When you enter a value for AGENTNAME, enter it using the same case that you used when you ran the avca add_agent command. After you replace the agent, you must run the avorcldb setup command and avctl start_collector command. See "Examples" on page 8-9 for more information.	Yes	NULL
AUDAUDIT_ACTIVE_SLEEP_TIME	The amount of active sleep time (in milliseconds) for the DBAUD process when the last retrieval actually did retrieve records.	Yes	1000 milliseconds
AUDAUDIT_AUDIT_VAULT_ALIAS	The alias name for the Audit Vault Server. The value you enter is not case sensitive.	No	NULL
AUDAUDIT_DELAY_TIME	The amount of delay time (in seconds) for the DBAUD process.	Yes	20 seconds
AUDAUDIT_MAX_PROCESS_RECORDS	The maximum number of records after which the collector commits records to the raw audit data store and generates minor recovery context. In fine-grained auditing (FGA_LOG\$) and 9.x sources, the collector might need to delay this until the record with the higher timestamp is retrieved. A valid value is an integer value from 10 to 10000.	Yes	1000 records

Table 8–2 (Cont.) DBAUD Collector Attributes

Attribute	Description	Mutable	Default Value
AUDAUDIT_SLEEP_TIME	The amount of sleep time (in milliseconds) for the DBAUD process. For example, if it is now 10:00:00 AM, the collector will retrieve the records with the timestamps that are less than 9:59:40. However, the next time the collector will only retrieve records with the timestamps of 9:59:40 or higher. The assumption is that within 20 seconds after the timestamp is assigned to the record, the record would be visible (retrievable). This attribute is used only for time-based retrieval in fine-grained auditing (FGA_LOG\$) on 9.x source databases. In Oracle Audit Vault, time-based retrieval is used for all retrievals.	Yes	5000 milliseconds
AUDAUDIT_SORT_POLICY	The audit data sort policy. This attribute is not implemented. It was deprecated for Oracle Audit Vault Release 10.2.3.	Yes	NULL
AUDAUDIT_SOURCE_ALIAS	The alias name for the audit data source. The value you enter is not case sensitive.	No	NULL

Table 8–3 describes the OSAUD collector attributes.

Table 8–3 OSAUD Collector Attributes

Attribute	Description	Mutable	Default Value
OSAUDIT_AUDIT_VALUE_ALIAS	The alias name for the Audit Vault Server. The value you enter is not case sensitive.	No	NULL
OSAUDIT_CHANNEL_TYPE	The channel type being used by the collector This attribute is not implemented. It was deprecated in Oracle Audit Vault Release 10.2.3.	No	NULL
OSAUDIT_DEFAULT_FILE_DEST ¹	The default directory for Oracle Database operating system audit files. This directory contains mandatory audit record files. The value you enter is not case sensitive.	Yes	\$ORACLE_HOME/rdbms/audit
OSAUDIT_FILE_DEST	The directory for the Oracle Database operating system audit files. This directory contains SYS and regular audit record files.	Yes	\$ORACLE_HOME/admin/DB_UNIQUE_NAME/adump
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.	Yes	10000
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.	Yes	600 centiseconds
OSAUDIT_NLS_CHARSET	The NLS character set of the data source. The value you enter is not case sensitive.	Yes	WE8ISO8859P1
OSAUDIT_NLS_LANGUAGE	The NLS language of the data source. The value you enter is not case sensitive.	Yes	AMERICAN
OSAUDIT_NLS_TERRITORY	The NLS territory of the data source. The value you enter is not case sensitive.	Yes	AMERICA
OSAUDIT_NT_ORACLE_SID	The Oracle SID name on Microsoft Windows systems. The value you enter is not case sensitive.	Yes	NULL

Table 8–3 (Cont.) OSAUD Collector Attributes

Attribute	Description	Mutable	Default Value
OSAUDIT_RAC_INSTANCE_ID	The instance ID in an Oracle RAC environment	Yes	1.0
OSAUDIT_SOURCE_ALIAS	The alias or connection string to the source database. The value you enter is not case sensitive.	Yes	NULL
OSAUDIT_SYSLOG_FILE	The syslog file name and location, if other than the default as indicated in the <code>etc/syslog.conf</code> file. Setting this parameter to a valid syslog file name overrides the default setting. The value you enter is not case sensitive.	Yes	NULL

¹ To avoid collecting duplicate operating system audit trail records, do not set the attribute value for the OSAUDIT_DEFAULT_FILE_DEST attribute and the OSAUDIT_FILE_DEST attribute such that the values, although different, resolves to the same directory.

Table 8–4 describes the REDO collector attributes.

Table 8–4 REDO Collector Attributes

Attribute	Description	Mutable	Default Value
AV.DATABASE.NAME	The Oracle Audit Vault database name. The value you enter is not case sensitive.	No	NULL
STRCOLL_DBPORT	The port number of the audit data Oracle source database	Yes	NULL
STRCOLL_DBSERVICE	The service name of the audit data Oracle source database. The value you enter is not case sensitive.	No	NULL
STRCOLL_HEARTBEAT_TIME	The time, in seconds, between events for monitoring the status of the Audit Vault REDO collection system	Yes	60 seconds
STRCOLL_SRCADM_ALIAS	The alias name for the audit data source. The value you enter is not case sensitive.	No	NULL
STRCOLL_SRCADM_NAME	The name of the audit data source database. The value you enter is not case sensitive.	No	NULL

On Microsoft Windows systems, if the path value for the OSAUDIT_DEFAULT_FILE_DEST attribute is set incorrectly using backslashes, use the Audit Vault Console to log in as the Audit Vault administrator and connect as AV_ADMIN, click **Configuration**, click **Collector**, select the **OSAUD_Collector** name, then click **Edit** and edit the value for this attribute using slashes instead of backslashes. When finished, click **OK** to save your changes.

Examples

The following example shows how to alter the AUDAUDIT_DELAY_TIME attribute for the DBAUD_Collector collector in Oracle Audit Vault:

```
avorcldb alter_collector -srcname hrdb.example.com -collname DBAUD_Collector
AUDAUDIT_DELAY_TIME="60"
```

Collector altered successfully.

The following sequence of commands demonstrate how to move a collector from one collection agent to another agent:

1. From the Audit Vault Server, configure two agents, A and B, on two separate hosts.

For example:

```
avca add_agent -agentname A -agenthost host1.example.com
```

Adding agent...

Enter agent user name: *agent_user_name*

Enter agent user password: *agent_user_pwd*

Re-enter agent user password: *agent_user_pwd*

```
avca add_agent -agentname B -agenthost host2.example.com
```

...

2. Configure collector L to run under agent A and collect from source S.

For example:

```
avorcldb add_collector -collname L -srcname S -agentname A
```

3. The node that runs agent A fails.
4. Move the collector L from agent A to agent B.

For example:

```
avorcldb alter_collector -collname L -srcname S agentname=B
```

5. From the Audit Vault collection agent home, configure agent B to connect to source S.

For example:

```
avorcldb setup -srcname S
```

Enter Source user name: *source_user_name*

Enter Source password: *password*

...

6. From the Audit Vault Server, restart the collector.

For example:

```
avctl start_collector -collname L -srcname S
```

Starting Collector...

Collector started successfully.

8.5 alter_source

The `avorcldb alter_source` command modifies the attributes of an Oracle source database.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb alter_source -srcname srcname  
[attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database to be modified. Remember that the source database name is case-sensitive.
<code>attrname=attrvalue</code>	Enter the pair (attribute name, new attribute value) for the mutable source attributes of this source to be modified. Optional. Separate multiple pairs by a space on the command line.

Usage Notes

[Table 8–5](#) lists source attributes that you can specify for the `attrname=attrvalue` argument.

Table 8–5 Source Attributes

Parameter	Description	Mutable	Default Value
HOST_IP	The Internet protocol address of the host system on which the source database resides	Yes	NULL
SOURCE_VERSION	The source database version	Yes	NULL
DESCRIPTION	The description for this source database	Yes	NULL
DB_SERVICE	A new audit data source database service name	Yes	NULL
PORT	A new port number for this system where the source database audit data resides	Yes	NULL
GLOBAL_DATABASE_NAME	The new global database name	Yes	NULL

Example

The following example shows how to alter the `PORT` attribute for the source database named `hr_db` in Oracle Audit Vault:

```
avorcldb alter_source -srcname hr_db PORT=1522
```

```
Altering source...
Source altered successfully.
```

8.6 drop_collector

The `avorcldb drop_collector` command disables (but does not remove) a collector from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb drop_collector -srcname srcname -collname collname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database to which the collector (specified in the <code>-collname</code> argument) belongs. Remember that the source database name is case-sensitive.
<code>-collname <i>collname</i></code>	Enter the name of the collector to be dropped from Oracle Audit Vault.

Usage Notes

The `drop_collector` command does not delete the collector from Oracle Audit Vault. It only disables the collector. The collector metadata is still in the database after you run the `drop_collector` command. If you want to recreate the collector, create it with a different name.

Example

```
avorcldb drop_collector -srcname hrdb.example.com -collname DBAUD_Collector
```

```
Dropping collector...
Collector dropped successfully.
```

8.7 drop_source

The `avorcldb drop_source` command disables (but does not remove) a source database from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb drop_source -srcname srcname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database to be dropped from Oracle Audit Vault. Remember that the source database name is case-sensitive.

Usage Notes

- The `drop_source` command does not delete the source database from Oracle Audit Vault. It only disables the source database definition in Oracle Audit Vault. The source database metadata is still in the database after you run the `drop_source` command. If you want to re-create the source database definition, create it with a different name.
- You cannot drop a source database if there are any active collectors for this source. You must drop all collectors associated with the source database before you can run the `drop_source` command on it.

Example

The following example shows how to drop the source named `hrdb.example.com` from Oracle Audit Vault:

```
avorcldb drop_source -srcname hrdb.example.com
```

```
Dropping source...
Source dropped successfully.
```

8.8 -help

The `avorcldb -help` command displays help information for the AVORCLDB commands. Run this command on either the Audit Vault Server and the Audit Vault collection agent.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb -help
```

```
avorcldb command -help
```

Arguments

Argument	Description
<i>command</i>	Enter 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 Oracle 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.

```
avorcldb add_source -help
```

```
avorcldb add_source command
```

```
add_source
  -src <host:port:service>
  [-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

Arguments:

```
-src          : Source DB connection information
-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
                  -desc 'HR Database'
```

8.9 setup

The `avorcldb setup` command adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, verifies the connection to the source using the wallet, and updates the `tnsnames.ora` file. You also can use this command to change the source user credentials in the wallet after these credentials have been changed in the source database.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avorcldb setup -srcname srcname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database. Remember that the source database name is case-sensitive.

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avorcldb setup` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avorcldb setup` command prompts for the source user name and password. This user account must exist on the source database.

To find the privileges and roles granted to this user, query the `SESSION_PRIVS` and `SESSION_ROLES` data dictionary views. The source user should have the privileges and roles that are listed in the `zarsspriv.sql` file, such as the `CREATE DATABASE LINK` privilege and `DBA` role.

If the `AVORCLDB_SRCUSR` environment variable is set to this user account and password, then you can bypass the `Enter Source user name` and `Enter Source password` prompts. If you do specify these values, they override the environment variable.

Example

The following example configures the REDO and OSAUD collectors.

```

avorcldb setup -srcname hrdb.example.com
Enter Source user name: srcuser_ora
Enter Source password: password

adding credentials for user srcuser_ora for connection [SRCDB1]
Credential stored successfully.
updated tnsnames.ora with alias [SRCDB1] to source database
verifying SRCDB1 connection using wallet

```

To change the source user name password in the wallet in the Audit Vault collection agent home, use the following setup command, where the source name is `orcl1` and the source user name is `srcuser_ora`.

```

avorcldb setup -srcname orcl
Enter Source user name: srcuser_ora
Enter Source password: password

adding credentials for user srcuser_ora for connection [SRCDB1]
Credential stored successfully.
updated tnsnames.ora with alias [SRCDB1] to source database
verifying SRCDB1 connection using wallet

```

8.10 verify

The `avorcldb verify` command verifies that the source is compatible for setting up the specified collectors.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```

avorcldb verify -src host:port:service
                -colltype [OSAUD,DBAUD,REDO,ALL]

```

Arguments

Argument	Description
<code>-src host:port:service</code>	<p>Enter the source database connection information: host name, port number, and service name, separated by a colon.</p> <p>Typically, the host is the fully qualified domain name or IP address of the server on which the source database is running, and the port number is 1521.</p> <p>If you are unsure of the host and port number, run the <code>lsnrctl status</code> command on the computer where you installed the source database.</p>

Argument	Description
<code>-colltype colltype</code>	<p>Enter one of the following collector types:</p> <ul style="list-style-type: none"> ■ ALL ■ DBAUD ■ OSAUD ■ REDO <p>See Table 1-5 on page 1-8 for more information about the collector types.</p>

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer and want to run the `avorcldb verify` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avorcldb verify` command prompts for the source user name and password. This user account must exist on the source database. To find this user, query the `SESSION_PRIVS` and `SESSION_ROLES` data dictionary views. The source user should have the privileges and roles that are listed in the `zarsspriv.sql` file, such as the `CREATE DATABASE LINK` privilege and `DBA` role.
- If the `AVORCLDB_SRCUSR` environment variable is set to this user account, then you can bypass the `Enter Source user name` and `Enter Source password` prompts. If you do specify these values, they override the environment variable.

Example

The following example verifies that the source is compatible with the OSAUD, DBAUD, and REDO collectors on a Linux or UNIX system.

```
avorcldb verify -src hrdb.example.com:1521:orcl -colltype ALL
Enter Source user name: username
Enter Source password: password
```

```
source HRDB.EXAMPLE.COM verified for OS File Audit Collector collector
source HRDB.EXAMPLE.COM verified for Aud$/FGA_LOG$ Audit Collector collector
source HRDB.EXAMPLE.COM verified for REDO Log Audit Collector collector
```

Audit Vault SQL Server (AVMSSQLDB) Utility Commands

Use the Audit Vault SQL Server Database (AVMSSQLDB) command-line utility to manage the relationship between Oracle Audit Vault and a Microsoft SQL Server source database instance and collector. When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVMSSQLDB command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 9–1](#) describes the AVMSSQLDB commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

Table 9–1 AVMSSQLDB Commands

Command	Where Used?	Description
add_collector	Server	Adds a collector to Oracle Audit Vault
add_source	Server	Registers an audit source with Oracle 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 Oracle Audit Vault
drop_source	Server	Drops a source from Oracle Audit Vault
-help	Both	Displays help information for the AVMSSQLDB commands
setup	Collection agent	Adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet
verify	Both	Verifies that the source is compatible with the collectors

9.1 avmssqldb

The AVMSSQLDB command-line utility, which you use to configure a Microsoft SQL Server database instance with Oracle Audit Vault.

Syntax

```
avmssqldb command -help
```

```
avmssqldb command [options] arguments
```

Arguments

Argument	Description
<i>command</i>	Enter one of the commands listed in Table 9-1 on page 9-1.
<i>arguments</i>	Enter one or more of the AVMSSQLDB command arguments.
-help	Displays help information for the AVMSSQLDB commands.

Usage Notes

Issuing an AVMSSQLDB command generates the following log file: \$ORACLE_HOME/av/log/srcname-mssqldb-#.log. The # is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit.

9.2 add_collector

The avmssqldb add_collector command adds a collector for the given SQL Server source database instance to Oracle Audit Vault. Oracle Audit Vault verifies the source database instance for the collector requirements.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb add_collector -srcname srcname -agentname agentname  
                        [-collname collname] [-desc desc]
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database instance for which the collector is to be added. Remember that the source database instance name is case-sensitive.

Argument	Description
-agentname <i>agentname</i>	Enter the name of the collection agent that was created when you ran the <code>avca add_agent</code> command. (In most cases, this is the agent that you created when you installed the Audit Vault collection agent, as described in <i>Oracle Audit Vault Collection Agent Installation Guide</i> .) If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the Configuration tab, and then click the Agent tab to display the Agents page. The name of the agent is displayed in the Agent column.
-collname <i>collname</i>	Create a name for the MSSQLDB collector. Optional. If you do not create a name, Oracle Audit Vault names the collector <code>MSSQLCollector</code> .
-desc <i>desc</i>	Enter a brief description of the collector. Optional.

Usage Notes

- Run any collector-specific preparation scripts before you execute the `avmssqldb add_collector` command.
- The `avmssqldb add_collector` command prompts for the source user name and password. This user account must exist on the source database instance.

Example

The following example shows how to add the MSSQLDB collector to Oracle Audit Vault.

```
avmssqldb add_collector -srcname mssqldb4 -agentname agent1
Enter a username :source_user_name
Enter a password : password

***** Collector Added Successfully*****
```

9.3 add_source

The `avmssqldb add_source` command registers a SQL Server source database instance with Oracle Audit Vault for audit data consolidation.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb add_source -src host:port|host\instance_name -srcname srcname
[-desc desc]
```

Arguments

Argument	Description
<code>-src host:port host\instance_name</code>	<p>Enter the source database instance connection information. Typically, the host is the fully qualified domain name or IP address of the server on which the SQL Server source database instance is running.</p> <p>The syntax you use depends on your configuration. Use the following syntax for single-instance configurations where the port number is different from 1433. Separate the host and port number with a colon.</p> <pre>-src host:port</pre> <p>Use the following syntax if the instance is not on the default port or does not have a default name. For configurations with multiple instances on one server, you must only use this syntax. Separate the host name and instance name with a backslash, and then enclose them single quotation marks.</p> <pre>-src 'host\instance_name'</pre>
<code>-srcname srcname</code>	<p>Create a name for the source database instance connection. Remember that the database instance name is case-sensitive. Oracle Audit Vault uses this name to connect to the Microsoft SQL Server source database instance.</p>
<code>-desc desc</code>	<p>Enter a brief description for the source database instance. Optional.</p>

Usage Notes

The `avmssqldb add_source` command prompts for the source user name and password. This user account must exist on the source database instance. See the example.

Example

The following example shows how to register a source with Oracle Audit Vault.

```
avmssqldb add_source -src mssqlserver\hr_db -srcname mssqldb4 -desc 'HR Database'
Enter a username :source_user_name
Enter a password : password

***** Source Verified *****
***** Source Added Successfully *****
```

9.4 alter_collector

The `avmssqldb alter_collector` command modifies the attributes of an MSSQLDB collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb alter_collector -srcname srcname -collname collname
[attrname=attrvalue...attrname=attrvalue]
```


Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database instance to which this collector belongs. Remember that the database instance name is case-sensitive.
<code>-collname collname</code>	Enter the name of the collector to be modified.
<code>attrname=attrvalue</code>	<p>Enter the attribute pair (attribute name, new attribute value) for mutable collector property and attributes for this collector type. This argument is optional.</p> <p>Enclose the attribute value in double quotation marks. For multiple values, enclose the entire set in double quotation marks and separate each value with a space. For example:</p> <pre>...="value1 value2 value3"</pre>

Usage Notes

- For SQL Server 2000 source databases only, the trace file (.trc) audit trail is not released to the collector until either the file reaches its maximum file size and another trace file is created, or the source database instance is shut down and restarted.
- You can specify the `SERVERSIDE_TRACE_FILEPATH` or `C2_TRACE_FILEPATH` attributes in the following ways:
 - The value for the path can be of the form *Drive:\Directory...\File Prefix.trc*, enclosed in double quotation marks. For example:


```
"c:\tracefiles\SQLAudit.trc"
```
 - Enter `#DYNAMIC` (but not enclosed in quotation marks) to enable the collector to query the SQL Server database to find the trace file paths. For example:


```
... SERVERSIDE_TRACE_FILEPATH=#DYNAMIC
```
 - You can include the asterisk (*) wildcard character to select multiple files. For example:


```
... SERVERSIDE_TRACE_FILEPATH="c:\SQLAuditFile*.trc"
```

Be aware that if you include the asterisk (*) wildcard character in the file path, then the collector reads from all files that are affected by the wildcard. For example, if you enter `c:\SQLAuditFile*.trc`, then the collector reads from `SQLAuditFile1.trc`, `SQLAuditFile2.trc`, `SQLAuditFile3.trc`, and so on.
 - Specify the path by providing the complete file path name. For example:


```
... SERVERSIDE_TRACE_FILEPATH="c:\SQLAuditFile1.trc"
```
 - Specify the multiple trace file paths by separating each path with a semicolon (;). For example:


```
... SERVERSIDE_TRACE_FILEPATH="c:\SQLAuditFile1.trc;SQLAuditFile2.trc;
c:\tracefi*.trc"
```
- If the `SERVERSIDE_TRACE_FILEPATH` attribute or the `C2_TRACE_FILEPATH` attribute is set to null, then the SQL Server collector does not retrieve audit data from the source database instance.

- If `AUDIT_SERVERSIDE_TRACES_FLAG` is not set, then collector does not check the value of `SERVERSIDE_TRACE_FILEPATH`. In this case, no data is collected from the server side traces, even if the value of `SERVERSIDE_TRACE_FILEPATH` is set. This behavior also applies to the `AUDIT_C2_FLAG` and `C2_TRACE_FILEPATH` settings, which control record collection from C2 traces.
- For server side traces, if `AUDIT_SERVERSIDE_TRACES_FLAG` is set, then the collector retrieves the value of the `SERVERSIDE_TRACE_FILEPATH` setting. If this parameter contains the value `#DYNAMIC`, then the collector collects audit data from the SQL Server source database instance. This behavior also applies to the `AUDIT_C2_FLAG` and `C2_TRACE_FILEPATH` settings.
- You can modify the collector `DESCRIPTION` property and one or more attributes at a time. [Table 9–2](#) lists the collector attributes (parameters), whether the parameter is mutable, the default value, and a brief description of the attribute.
- Note the following case-sensitivity guidelines for specifying attributes:
 - Except for the `AGENTNAME` attribute, the attribute names are case sensitive. Enter them in upper-case letters.
 - All the attribute values, including the `AGENTNAME` attribute value, are case sensitive. Enter them in the case shown the following tables.

Table 9–2 MSSQLDB Collector Attributes

Attribute	Description	Mutable	Default Value
AGENTNAME	Name of an agent to replace the agent that was specified by the <code>avmssqldb add_collector</code> command that was used for this source database instance. This feature enables you to move a collector from one agent to another. It is useful for failover recovery if the host computer running the original agent fails. This attribute only applies to collectors that collect from the server-side trace logs. When you enter a value for <code>AGENTNAME</code> , enter it using the same case that you used when you ran the <code>avca add_agent</code> command. After you replace the agent, you must run the <code>avmssqldb setup</code> command and <code>avctl start_collector</code> command. See "Examples" on page 9-7 for more information.	Yes	NULL
DESCRIPTION	The description for this collector. The value you enter is not case sensitive.	Yes	NULL
DBCONNECTION	Number of connections to the database	No	1
AUDIT_C2_FLAG	Whether C2 logs can be collected by the MSSQLDB collector. Values can be 0 or 1.	Yes	1
AUDIT_SERVERSIDE_TRACES_FLAG	Whether server-side trace logs can be collected by the MSSQLDB collector. Values can be 0 or 1. See the usage notes.	Yes	1
AUDIT_EVENT_LOG_FLAG	Whether events logs can be collected by the MSSQLDB collector. Values can be 0 or 1. For SQL Server 2000, set this parameter to 0, because in that release, there are no auditable events written to the Windows Eventlog.	Yes	1
C2_TRACE_FILEPATH	The C2 trace file path. The value you enter is not case sensitive. See the usage notes.	Yes	NULL

Table 9–2 (Cont.) MSSQLDB Collector Attributes

Attribute	Description	Mutable	Default Value
SERVERSIDE_TRACE_FILEPATH	The value for server-side trace file path The value you enter is not case sensitive. See the usage notes.	Yes	NULL
DELAY_TIME	The delay time (in milliseconds) of the collector	Yes	20000
NO_OF_RECORDS	The maximum number of records to be fetched by the collector. This attribute is mutable.	Yes	1000

Examples

The following example shows how to alter the NO_OF_RECORDS attribute and the collector description for the MSSQLCollector collector in Oracle Audit Vault:

```
avmssqldb alter_collector -srcname mssqldb4 -collname MSSQLCollector NO_OF_
RECORDS=1500 DESCRIPTION="MSSQLDB collector 45" SERVERSIDE_TRACE_
FILEPATH="c:\SQLAuditFile*.trc"
```

```
***** Collector Altered Successfully *****
```

The following sequence of commands demonstrate how to move a collector from one collection agent to another agent:

1. From the Audit Vault Server, configure two agents, A and B, on two separate hosts.

For example:

```
avca add_agent -agentname A -agenthost host1.example.com
```

Adding agent...

Enter agent user name: *agent_user_name*

Enter agent user password: *agent_user_pwd*

Re-enter agent user password: *agent_user_pwd*

```
avca add_agent -agentname B -agenthost host2.example.com
```

...

2. Configure collector L to run under agent A and collect from source S.

For example:

```
avorcldb add_collector -collname L -srcname S -agentname A
```

3. The node that runs agent A fails.
4. Move the collector L from agent A to agent B.

For example:

```
avorcldb alter_collector -collname L -srcname S agentname=B
```

5. From the Audit Vault collection agent home, configure agent B to connect to source S.

For example:

```
avorcldb setup -srcname S
```

Enter Source user name: *source_user_name*

Enter Source password: *password*

...

6. From the Audit Vault Server, restart the collector.

For example:

```
avctl start_collector -collname L -srcname S
```

```
Starting Collector...
```

```
Collector started successfully.
```

9.5 alter_source

The `avmssqldb alter_source` command modifies the attributes of a SQL Server source database instance.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb alter_source -srcname sourcename  
[attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
<code>-srcname <i>sourcename</i></code>	Enter the name of the source database instance to be modified. Remember that the database instance name is case-sensitive.
<code><i>attrname=attrvalue</i></code>	Enter the attribute pair (attribute name, new attribute value) for mutable source properties and attributes for this source type. This argument is optional. Separate multiple pairs by a space on the command line.

Usage Notes

[Table 9–3](#) lists the source attributes, a brief description of the attribute, whether the attribute is mutable, and the default value. You can modify one or more source attributes at a time.

Table 9–3 Source Attributes

Attribute	Description	Mutable	Default Value
SOURCETYPE	The source type name for this source database instance. The default name is MSSQLDB.	No	NULL
NAME	The name for this source database instance	No	NULL
HOST	The source database instance host name	No	NULL
HOST_IP	The source database instance host IP address	No	NULL
VERSION	The source database instance version	Yes	NULL

Table 9–3 (Cont.) Source Attributes

Attribute	Description	Mutable	Default Value
DESCRIPTION	The description for this source database instance	Yes	NULL
PORT	A new port number for this system where the source database instance audit data resides	Yes	None

Example

The following example shows how to alter the DESCRIPTION attribute for the source database instance named mssqlldb4 in Oracle Audit Vault:

```
avmssqldb alter_source -srcname mssqldb4 DESCRIPTION="HR Database"
```

```
***** Source Altered Successfully *****
```

9.6 drop_collector

The `avmssqldb drop_collector` command disables (but does not remove) an MSSQLDB collector from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb drop_collector -srcname srcname -collname collname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database instance to which the collector (specified in the <code>-collname</code> argument) belongs. Remember that the database instance name is case-sensitive.
<code>-collname <i>collname</i></code>	Enter the name of the collector to be dropped from Oracle Audit Vault.

Usage Notes

The `drop_collector` command does not delete the collector from Oracle Audit Vault. It only disables the collector. The collector metadata is still in the database after you run the `drop_collector` command. If you want to recreate the collector, create it with a different name.

Example

The following example shows how to drop a collector named MSSQLCollector from Oracle Audit Vault:

```
avmssqldb drop_collector -srcname mssqldb4 -collname MSSQLCollector
```

```
***** Collector Dropped Successfully *****
```

9.7 drop_source

The `avmssqldb drop_source` command disables (but does not remove) a SQL Server source database instance from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb drop_source -srcname srcname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the source database instance to be dropped from Oracle Audit Vault. Remember that the database instance name is case-sensitive.

Usage Notes

- The `drop_source` command does not delete the source database instance from Oracle Audit Vault. It only disables the source database instance definition in Oracle Audit Vault. The source database instance metadata is still in the database after you run the `drop_source` command. If you want to re-create the source database instance definition, create it with a different name.
- You cannot drop a source database instance if it has any active collectors for this source database instance. You must drop all collectors associated with the source database instance before you can run the `drop_source` command on it.

Example

The following example shows how to drop the source named `mssqldb4` from Oracle Audit Vault:

```
avmssqldb drop_source -srcname mssqldb4
```

```
***** Drop Source Successfully *****
```

9.8 -help

The `avmssqldb -help` command displays help information for the `AVMSSQLDB` commands.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb -help
```

```
avmssqldb command -help
```

Arguments

Argument	Description
<i>command</i>	Enter the name of an AVMSSQLDB command for which you want help to appear.

Usage Notes

None

Example

The following example shows how to display general AVMSSQLDB utility help in Oracle Audit Vault:

```
avmssqldb -help
```

The following example shows how to display specific AVMSSQLDB help for the `add_source` command in the Audit Vault Server home.

```
avmssqldb add_source -help
```

```
add_source
  -src <host>[:<port>|\\<instancename>] -srcname
  <srcname> [-desc <desc>]
```

Purpose: The source is added to Audit Vault.

Arguments:

```
-src      : Source DB connection information
-srcname  : Name of a source
-desc     : Optional description of the source
```

Examples:

```
avmssqldb add_source -src 'server\instancename'
-desc 'source for admin databases' -srcname mssource
```

9.9 setup

The `avmssqldb setup` command adds the SQL Server source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet. You also can use this command to change the source user credentials in the wallet after these credentials have been changed in the source database instance.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb setup -srcname srcname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database instance. Remember that the database instance name is case-sensitive.

Usage Notes

- You cannot run this command in a UNIX environment.
- The `avmssqldb setup` command prompts for the source user name and password. This user account must exist on the source database instance.

Example

```
avmssqldb setup -srcname mssqldb4
Enter a username : source_user_name
Enter a password : password

***** Credentials Successfully added *****
```

9.10 verify

The `avmssqldb verify` command verifies that a SQL Server source database instance is compatible for setting up the specified collector.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avmssqldb verify -src host:port|host\instance_name
```


Arguments

Argument	Description
<code>-src host:port host\instance_name</code>	<p>Enter the source database instance connection information. Typically, the host is the fully qualified domain name or IP address of the server on which the SQL Server database instance is running.</p> <p>The syntax you use depends on your configuration. Use the following syntax for single-instance configurations where the port number is different from 1433. Separate the host and port number with a colon.</p> <p><code>-src host:port</code></p> <p>Use the following syntax if the instance is not on the default port or does not have a default name. For configurations with multiple instances on one server, you must only use this syntax. Separate the host name and instance name with a backslash, and then enclose them single quotation marks.</p> <p><code>-src 'host\instance_name'</code></p>

Usage Notes

- The `avmssqldb verify` command checks the following:
 - Whether the version of the SQL Server database is supported: SQL Server 2000 or SQL Server 2005
 - Whether the source user has the required privileges in the source database instance that is to be registered with Oracle Audit Vault
 - Whether auditing (C2 auditing and server-side trace auditing) is enabled in the source database instance
- If you installed the collection agent on a Microsoft Windows computer, then run the `avmssqldb verify` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avmssqldb verify` command prompts for the source user name and password. This user account must exist on the source database instance.

Example

The following example verifies that the source is compatible with the MSSQLDB collector on Windows.

```
avmssqldb verify -src 192.0.2.1:4523
Enter a username : source_user_name
Enter a password : password

***** Source Verified *****
```


Audit Vault Sybase ASE (AVSYBDB) Utility Commands

Use the Audit Vault Sybase Database (AVSYBDB) command-line utility to manage the relationship between Oracle Audit Vault and a Sybase ASE source database and collector. When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVSYBDB command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 10–1](#) describes the AVSYBDB commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

Table 10–1 AVSYBDB Commands

Command	Where Used?	Description
add_collector	Server	Adds a collector to Oracle Audit Vault
add_source	Server	Registers an audit source with Oracle 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 Oracle Audit Vault
drop_source	Server	Drops a source from Oracle Audit Vault
-help	Both	Displays help information for the AVSYBDB commands
setup	Collection agent	Adds the source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet
verify	Both	Verifies that the source is compatible with the collectors

10.1 avsybdb

The AVSYBDB command-line utility, which you use to configure a Sybase ASE database with Oracle Audit Vault.

Syntax

```
avsybdb command -help
```

```
avsybdb command [options] arguments
```

Arguments

Argument	Description
<i>command</i>	Enter one of the commands listed in Table 10-1 on page 10-1.
<i>arguments</i>	Enter one or more of the AVSYBDB command arguments.
-help	Displays help information for the AVSYBDB commands.

Usage Notes

Issuing an AVSYBDB command generates the following log file: \$ORACLE_HOME/av/log/srcname-sybdb-#.log. The # is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit.

10.2 add_collector

The avsybdb add_collector command adds a SYBDB collector for a Sybase ASE source database to Oracle Audit Vault. Oracle Audit Vault verifies the source database for the collector requirements.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb add_collector -srcname srcname -agentname agentname  
[-collname collname] [-desc desc]
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database for which the collector is to be added. Remember that the source database name is case-sensitive. Typically, the host is the fully qualified domain name or IP address of the server on which the Sybase ASE source database is running, and the port number is 5000.

Argument	Description
-agentname <i>agentname</i>	Enter the name of the collection agent that was created when you ran the <code>avca add_agent</code> command. (In most cases, this is the agent that you created when you installed the Audit Vault collection agent, as described in <i>Oracle Audit Vault Collection Agent Installation Guide</i> .) If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the Configuration tab, and then click the Agent tab to display the Agents page. The name of the agent is displayed in the Agent column.
-collname <i>collname</i>	Create a name for the SYBDB collector. Optional. If you do not create a name, Oracle Audit Vault names the collector <code>SybaseCollector</code> .
-desc <i>desc</i>	Enter a brief description of the collector. Optional.

Usage Notes

- Run any collector-specific preparation scripts before you execute the `avsybdb add_collector` command.
- The `avsybdb add_collector` command prompts for the source user name and password. This user account must exist on the source database.

Example

The following example shows how to add a SYBDB collector to Oracle Audit Vault on Linux and UNIX platforms.

```
avsybdb add_collector -srcname sybdb4 -agentname agent1
Enter a username : source_user_name
Enter a password : password

***** Collector Added Successfully*****
```

10.3 add_source

The `avsybdb add_source` command registers a Sybase ASE source database with Oracle Audit Vault for audit data consolidation.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb add_source -src host:port -srcname srcname [-desc desc]
```

Arguments

Argument	Description
<code>-src host:port</code>	Enter the source database connection information: host name and port number, separated by a colon. Typically, the host is the fully qualified domain name or IP address of the server on which the Sybase ASE source database is running, and the port number is 5000.
<code>-srcname srcname</code>	Create a name to associate with this source database. Remember that the source database name is case-sensitive. Oracle Audit Vault uses this name to connect to the Sybase ASE source database.
<code>-desc desc</code>	Enter a brief description of the source database. Optional.

Usage Notes

The `avsybdb add_source` command prompts for the source user name and password. This user account must exist on the source database.

Example

The following example shows how to register a source with Oracle Audit Vault.

```
avsybdb add_source -src lnxserver:5000 -srcname sybdb4 -desc 'HR Database'
Enter a username : source_user_name
Enter a password : password
```

```
***** Source Verified *****
***** Source Added Successfully *****
```

10.4 alter_collector

The `avsybdb alter_collector` command modifies the attributes of a SYBDB collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb alter_collector -srcname srcname -collname collname
[attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database to which this collector belongs. Remember that the source database name is case-sensitive.
<code>-collname collname</code>	Enter the name of the collector to be modified.

Argument	Description
<i>attrname=attrvalue</i>	<p>Enter the attribute pair (attribute name, new attribute value) for mutable collector property and attributes for this collector type. This argument is optional.</p> <p>Enclose the attribute value in double quotation marks. For multiple values, enclose the entire set in double quotation marks and separate each value with a space. For example:</p> <p>...="value1 value2 value3"</p>

Usage Notes

- You can modify one or more collector attributes at a time. [Table 10–2](#) lists the collector attributes, whether the attribute is mutable, its default value, and a brief description.
- Note the following case-sensitivity guidelines for specifying attributes:
 - Except for the AGENTNAME attribute, the attribute names are case sensitive. Enter them in upper-case letters.
 - All the attribute values, including the AGENTNAME attribute value, are case sensitive. Enter them in the case shown the following tables.

Table 10–2 SYBDB Collector Attributes

Attribute	Description	Mutable	Default Value
AGENTNAME	<p>Name of an agent to replace the agent that was specified by the <code>avsybdb add_collector</code> command that was used for this source database. This feature enables you to move a collector from one agent to another. It is useful for failover recovery if the host computer running the original agent fails. When you enter a value for AGENTNAME, enter it using the same case that you used when you ran the <code>avca add_agent</code> command.</p> <p>After you replace the agent, you must run the <code>avsybdb setup</code> command and <code>avctl start_collector</code> command. See "Examples" on page 10-5 for more information.</p>	Yes	NULL
DESCRIPTION	The description for this collector. The value you enter is not case sensitive.	Yes	NULL
DBCONNECTION	Number of connections to the database	No	1
DELAY_TIME	The delay time (in milliseconds) of the collector	Yes	20000
NO_OF_RECORDS	The maximum number of records to be fetched by the collector	Yes	1000

Examples

The following example shows how to alter the NO_OF_RECORDS attribute and the collector description for the SybaseCollector collector in Oracle Audit Vault:

```
avsybdb alter_collector -srcname sybdb4 -collname SybaseCollector
NO_OF_RECORDS=1500 DESCRIPTION="Sybase collector 45"
```

```
***** Collector Altered Successfully *****
```

The following sequence of commands demonstrate how to move a collector from one collection agent to another agent:

1. From the Audit Vault Server, configure two agents, A and B, on two separate hosts.

For example:

```
avca add_agent -agentname A -agenthost host1.example.com
```

Adding agent...

Enter agent user name: *agent_user_name*

Enter agent user password: *agent_user_pwd*

Re-enter agent user password: *agent_user_pwd*

```
avca add_agent -agentname B -agenthost host2.example.com
```

...

2. Configure collector L to run under agent A and collect from source S.

For example:

```
avorcldb add_collector -collname L -srcname S -agentname A
```

3. The node that runs agent A fails.
4. Move the collector L from agent A to agent B.

For example:

```
avorcldb alter_collector -collname L -srcname S agentname=B
```

5. From the Audit Vault collection agent home, configure agent B to connect to source S.

For example:

```
avorcldb setup -srcname S
```

Enter Source user name: *source_user_name*

Enter Source password: *password*

...

6. From the Audit Vault Server, restart the collector.

For example:

```
avctl start_collector -collname L -srcname S
```

Starting Collector...

Collector started successfully.

10.5 alter_source

The `avsybdb alter_source` command modifies the attributes of the Sybase ASE source database.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb alter_source -srcname srcname  
[attrname=attrvalue...attrname=attrvalue]
```


Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database to be modified. Remember that the source database name is case-sensitive.
<code>attrname=attrvalue</code>	Enter the attribute pair (attribute name, new attribute value) for mutable source properties and attributes for this source type. This argument is optional. Separate multiple pairs by a space on the command line. See Table 10-3 for more information.

Usage Notes

[Table 10-3](#) lists the source database attributes, a brief description of the attribute, whether the attribute is mutable, and the default value. You can modify one or more source attributes at a time.

Table 10-3 Source Attributes

Attribute	Description	Mutable	Default Value
SOURCETYPE	The source type name for this source database. The default name is SYBDB.	No	NULL
NAME	The name for this source database	No	NULL
HOST	The source database host name	No	NULL
HOST_IP	The source database host IP address	No	NULL
VERSION	The source database version	Yes	NULL
DESCRIPTION	A new description for this source database	Yes	NULL
PORT	A new port number for this system where the source database audit data reside	Yes	None

Example

The following example shows how to alter the DESCRIPTION attribute for the source database named sybdb4 in Oracle Audit Vault:

```
avsybdb alter_source -srcname sybdb4 DESCRIPTION="HR Database"

***** Source Altered Successfully *****
```

10.6 drop_collector

The `avsybdb drop_collector` command disables (but does not remove) a SYBDB collector from Oracle Audit Vault. The `drop_collector` command does not delete the collector from Oracle Audit Vault; instead, it 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.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb drop_collector -srcname srcname -collname collname
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database to which the collector (specified in the -collname argument) belongs. Remember that the source database name is case-sensitive.
-collname <i>collname</i>	Enter the name of the collector to be dropped from Oracle Audit Vault.

Usage Notes

The `drop_collector` command does not delete the collector from Oracle Audit Vault. It only disables the collector. The collector metadata is still in the database after you run the `drop_collector` command. If you want to recreate the collector, create it with a different name.

Example

The following example shows how to drop the collector named `SybaseCollector` from Oracle Audit Vault:

```
avsybdb drop_collector -srcname sybdb4 -collname SybaseCollector
```

```
***** Collector Dropped Successfully *****
```

10.7 drop_source

The `avsybdb drop_source` command disables (but does not remove) a Sybase ASE source database from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb drop_source -srcname srcname
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database to be dropped from Oracle Audit Vault. Remember that the source database name is case-sensitive.

Usage Notes

- The `drop_source` command does not delete the source database from Oracle Audit Vault. It only disables the source database definition in Oracle Audit Vault. The source database metadata is still in the database after you run the `drop_`

source command. If you want to re-create the source database definition, create it with a different name.

- You cannot drop a source database if there are any active collectors for this source. You must drop all collectors associated with the source database before you can run the `drop_source` command on it.

Example

The following example shows how to drop the source named `sybdb4` from Oracle Audit Vault:

```
avsybdb drop_source -srcname sybdb4

***** Drop Source Successfully *****
```

10.8 -help

The `avsybdb -help` command displays help information for the AVSYBDB commands.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb -help

avsybdb command -help
```

Arguments

Argument	Description
<i>command</i>	Enter the name of an AVSYBDB command for which you want help to appear.

Usage Notes

None

Example

The following example shows how to display general AVSYBDB utility help in Oracle Audit Vault:

```
avsybdb -help
```

The following example shows how to display specific AVSYBDB Help for the `add_source` command in the Audit Vault Server home.

```
avsybdb add_source -help
avsybdb add_source command

add_source
```

```
-src <host:port> -srcname <srcname>
[-desc <desc>]
```

Purpose: The source is added to Audit Vault.

Arguments:

```
-src      : Source DB connection information
-srcname  : Name of a source
-desc    : Optional description of the source
```

Examples:

```
avsybdb add_source -src lnxserver:5000
                -desc 'HR Database'
```

10.9 setup

The `avsybdb setup` command adds the Sybase ASE source user credentials to the wallet, creates a database alias in the wallet for the source user, and verifies the connection to the source using the wallet. You also can use this command to change the source user credentials in the wallet after these credentials have been changed in the source database.

Where to Run This Command

Audit Vault collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.3](#).
- **Microsoft Windows:** Go to the Audit Vault collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb setup -srcname srcname
```

Arguments

Argument	Description
<code>-srcname <i>srcname</i></code>	Enter the name of the source database. Remember that the source database name is case-sensitive.

Usage Notes

- If you installed the collection agent on a Microsoft Windows computer, run the `avsybdb setup` command from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avsybdb setup` command prompts for the source user name and password. This user account must exist on the source database.

Example

```
avsybdb setup -srcname sybdb4
Enter a username : source_user_name
Enter a password : password

***** Credentials Successfully added *****
```

10.10 verify

The `avsybdb verify` command verifies that the Sybase ASE source database is compatible for setting up the specified collectors.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avsybdb verify -src host:port
```

Arguments

Argument	Description
<code>-src host:port</code>	Enter the source database connection information: host name and port number, separated by a colon. Typically, the host is the fully qualified domain name or IP address of the server on which the Sybase ASE source database is running, and the port number is 5000.

Usage Notes

- The `avsybdb verify` command checks the following:
 - Whether the version of the database is supported: Sybase ASE 15.0.2 or Sybase ASE 12.5.4
 - Whether the source user has the required privileges in the source database that is to be registered with Oracle Audit Vault
 - Whether auditing is enabled in the source database
 - Whether the operating system on which the source database is running is supported
- If you installed the collection agent on a Microsoft Windows computer and want to run the `avsybdb verify` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate environment variables before running this command. See [Section 2.2](#) for more information.
- The `avsybdb verify` command prompts for the source user name and password. This user account must exist on the source database.

Example

The following example verifies that the source is compatible with the SYBDB collector on a UNIX system.

```
avsybdb verify -src 192.0.2.7:5000
Enter a username : source_user_name
Enter a password : password
***** Source Verified *****
```


Audit Vault IBM DB2 (AVDB2DB) Utility Commands

Use the Audit Vault IBM DB2 Database (AVDB2DB) command-line utility to manage the relationship between Oracle Audit Vault an IBM DB2 source database and DB2 collector. When you run these commands, remember the following:

- **Enter the command in lowercase letters.** The commands are case-sensitive.
- **On UNIX systems, when you open a new shell to run a command, first set the appropriate environment variables.** See [Section 2.2.2](#) and [Section 2.2.3](#) for more information.
- **On Microsoft Windows systems, do not set any environment variables.** Instead, run the command from the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.
- **Oracle Audit Vault creates a log file of AVDB2DB command activity.** See [Section A.1](#) and [Section A.2](#) for more information.

[Table 11–1](#) describes the AVDB2DB commands and where each is used, whether on the Audit Vault Server, on the Audit Vault collection agent, or in both places.

Table 11–1 AVDB2DB Commands

Command	Where Used?	Description
add_collector	Server	Adds a collector to Oracle Audit Vault
add_source	Server	Registers an audit source with Oracle 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 Oracle Audit Vault
drop_source	Server	Drops a source from Oracle Audit Vault
-help	Both	Displays help information for the AVDB2DB commands
verify	Both	Verifies that the source is compatible with the collectors

11.1 avdb2db

The AVDB2DB command-line utility, which you use to configure an IBM DB database with Oracle Audit Vault.

Syntax

`avdb2db command -help`

`avdb2db command [options] arguments`

Arguments

Argument	Description
<i>command</i>	Enter one of the commands listed in Table 11-1 on page 11-1.
<i>arguments</i>	Enter one or more of the AVDB2DB command arguments.
<code>-help</code>	Displays help information for the AVDB2DB commands

Usage Notes

Issuing an AVDB2DB command generates the following log file: `$ORACLE_HOME/av/log/srcname-db2db-#.log`. The # is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit.

11.2 add_collector

The `avdb2db add_collector` command adds a collector for the given IBM DB2 source database to Oracle Audit Vault. Oracle Audit Vault verifies the source database for the collector requirements.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

`avdb2db add_collector -srcname srcname -agentname agentname
[-collname collname] [-desc desc]`

Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the source database name for which the collector is to be added. Remember that the source database name is case-sensitive. Typically, the host is the fully qualified domain name or IP address of the server on which the IBM DB2 source database is running, and the port number is 50000.

Argument	Description
<code>-agentname agentname</code>	Enter the name of the collection agent that was created when you ran the <code>avca add_agent</code> command. (In most cases, this is the agent that you created when you installed the Audit Vault collection agent, as described in <i>Oracle Audit Vault Collection Agent Installation Guide</i> .) If you are not sure of the agent name, then you can find it as follows: Log in to the Audit Vault Console, click the Configuration tab, and then click the Agent tab to display the Agents page. The name of the agent is displayed in the Agent column.
<code>-collname collname</code>	Create a name for the DB2 collector. Optional. If you do not create a name, Oracle Audit Vault names the collector <code>DB2_Coll</code> .
<code>-desc desc</code>	Enter a brief description of the collector. Optional.

Usage Notes

- Run any collector-specific preparation scripts before you execute the `avdb2db add_collector` command.
- The `avdb2db add_collector` command prompts for a user name and password. This user account must have privileges to run the IBM DB2 `db2audit` command (for example, a user who has the `sysadmin` privilege).

Example

The following example shows how to add an DB2 collector to Oracle Audit Vault on Linux and UNIX platforms.

```
avdb2db add_collector -srcname db2db4 -agentname agent1
Enter a username : source_user_name
Enter a password : password

***** Collector Added Successfully*****
```

11.3 add_source

The `avdb2db add_source` command registers an IBM DB2 source database with Oracle Audit Vault for audit data consolidation.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db add_source -src host:port -srcname srcname [-desc desc]
```

Arguments

Argument	Description
-src <i>host:port</i> or -src <i>host:port:database</i>	<p>Enter the source database connection information, using one of the following:</p> <ul style="list-style-type: none"> ▪ <i>host:port</i> connects to the DB2 instance to collect server audit records but omits database-specific records. ▪ <i>host:port:database</i> connects to a specified database in the DB2 instance to collect only audit records from the that database. <p>Enter the host name, port number, and optional database name separated by a colon.</p> <p>Typically, the host is the fully qualified domain name or IP address of the server on which the IBM DB2 source database is running, and the port number is 50000.</p>
-srcname <i>srcname</i>	<p>Create a name to associate with this source database. Remember that the source database name is case-sensitive. Oracle Audit Vault uses this name to connect to the IBM DB2 source database.</p>
-desc <i>desc</i>	<p>Enter a brief description of the source database. Optional.</p>

Usage Notes

The `avdb2db add_source` command prompts for a user name and password. This user account must have privileges to run the IBM DB2 `db2audit` command (for example, a user who has the `sysadmin` privilege).

Example

The following example shows how to register a source with Oracle Audit Vault.

```
avdb2db add_source -src lnxserver:50000 -srcname db2db4 -desc 'HR Database'
Enter a username : source_user_name
Enter a password : password

**** Source Verified ****
**** Source Added Successfully ****
```

11.4 alter_collector

The `avdb2db alter_collector` command modifies the attributes of a DB2 collector.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db alter_collector -srcname srcname -collname collname
[attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
<code>-srcname srcname</code>	Enter the name of the source database to which this collector belongs. Remember that the source database name is case-sensitive.
<code>-collname collname</code>	Enter the name of the collector to be modified.
<code>attrname=attrvalue</code>	Enter the attribute pair (attribute name, new attribute value) for mutable collector property and attributes for this collector type. This argument is optional. Enclose the attribute value in double quotation marks. For multiple values, enclose the entire set in double quotation marks and separate each value with a space. For example: ...="value1 value2 value3"

Usage Notes

You can modify one or more collector attributes at a time. [Table 11–2](#) lists the collector attributes, whether the parameter is mutable, its default value, and a brief description. You can enter these settings in any case; they are not case sensitive.

Table 11–2 DB2 Collector Attributes

Attribute	Description	Mutable	Default Value
DESCRIPTION	The description for this collector	Yes	NULL
DBCONNECTION	Number of connections to the database	No	1
DELAY_TIME	The delay time (in milliseconds) of the collector	Yes	20000
NO_OF_RECORDS	The maximum number of records to be fetched by the collector	Yes	1000
SINGLE_FILEPATH	The location of the directory where the DB2 collector will look for files to collect audit records from, or the location to which the DB2 extraction utility writes the text files. Enter an absolute path only, not a relative path.	Yes	NULL

Examples

The following example shows how to alter the NO_OF_RECORDS attribute and the collector description for the DB2Collector collector in Oracle Audit Vault:

```
avdb2db alter_collector -srcname db2db4 -collname DB2Collector
NO_OF_RECORDS=1500 DESCRIPTION="IBM DB2 collector 9"

***** Collector Altered Successfully *****
```

11.5 alter_source

The `avdb2db alter_source` command modifies the attributes of an IBM DB2 source database.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db alter_source -srcname srcname
    [attrname=attrvalue...attrname=attrvalue]
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database to be modified. Remember that the source database name is case-sensitive.
<i>attrname=attrvalue</i>	Enter the attribute pair (attribute name, new attribute value) for mutable source properties and attributes for this source type. This argument is optional. Separate multiple pairs by a space on the command line. See Table 11-3 for more information.

Usage Notes

[Table 11-3](#) lists the source database attributes, a brief description of the attribute, whether the attribute is mutable, and the default value. You can modify one or more source attributes at a time.

Table 11-3 Source Attributes

Attribute	Description	Mutable	Default Value
SOURCETYPE	The source type name for this source database. The default name is DB2DB.	No	NULL
NAME	The name for this source database.	No	NULL
HOST	The source database host name.	No	NULL
HOST_IP	The source database host IP address.	No	NULL
VERSION	The source database version.	Yes	NULL
DESCRIPTION	A new description for this source database.	Yes	NULL
PORT	A new port number for this system where the source database audit data resides	Yes	None

Example

The following example shows how to alter the DESCRIPTION attribute for the source database named db2db4 in Oracle Audit Vault:

```
avdb2db alter_source -srcname db2db4 DESCRIPTION="HR Database"
```

```
***** Source Altered Successfully *****
```

11.6 drop_collector

The avdb2db drop_collector command disables (but does not remove) a DB2 collector from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db drop_collector -srcname srcname -collname collname
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database to which the collector (specified in the -collname argument) belongs. Remember that the source database name is case-sensitive.
-collname <i>collname</i>	Enter the name of the collector to be dropped from Oracle Audit Vault.

Usage Notes

The `drop_collector` command does not delete the collector from Oracle Audit Vault. It only disables the collector. The collector metadata is still in the database after you run the `drop_collector` command. If you want to recreate the collector, create it with a different name.

Example

The following example shows how to drop a collector named `DB2Collector` from Oracle Audit Vault:

```
avdb2db drop_collector -srcname db2db4 -collname DB2Collector
```

```
***** Collector Dropped Successfully *****
```

11.7 drop_source

The `avdb2db drop_source` command disables (but does not remove) an IBM DB2 source database from Oracle Audit Vault.

Where to Run This Command

Audit Vault Server:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#).
- **Microsoft Windows:** Go to the Audit Vault Server `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db drop_source -srcname srcname
```

Arguments

Argument	Description
-srcname <i>srcname</i>	Enter the name of the source database to be dropped from Oracle Audit Vault. Remember that the source database name is case-sensitive.

Usage Notes

- The `drop_source` command does not delete the source database from Oracle Audit Vault. It only disables the source database definition in Oracle Audit Vault. The source database metadata is still in the database after you run the `drop_`

source command. If you want to re-create the source database definition, create it with a different name.

- You cannot drop a source database if there are any active collectors for this source. You must drop all collectors associated with the source database before you can run the `drop_source` command on it.

Example

The following example shows how to drop the source named `db2db4` from Oracle Audit Vault:

```
avdb2db drop_source -srcname db2db4

***** Drop Source Successfully *****
```

11.8 -help

The `avdb2db -help` command displays help information for the AVDB2DB commands.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db -help

avdb2db command -help
```

Arguments

Argument	Description
<i>command</i>	Enter the name of an AVDB2DB command for which you want help to appear.

Usage Notes

None

Example

The following example shows how to display general AVDB2DB utility help in Oracle Audit Vault:

```
avdb2db -help
```

The following example shows how to display specific AVDB2DB help for the `add_source` command in the Audit Vault Server home.

```
avdb2db add_source -help
avdb2db add_source command

add_source
```

```
-src <host:port> -srcname <srcname>
[-desc <desc>]
```

Purpose: The source is added to Audit Vault.

Arguments:

```
-src      : Source DB connection information
-srcname  : Name of a source
-desc     : Optional description of the source
```

Examples:

```
avdb2db add_source -src lnxserver:50000
-desc 'HR Database'
```

11.9 verify

The `avdb2db verify` command verifies that the IBM DB2 source database is compatible for setting up the specified collectors.

Where to Run This Command

Either Audit Vault Server and collection agent:

- **UNIX:** Set the appropriate environment variables, as described in [Section 2.2.2](#) for Audit Vault Server or [Section 2.2.3](#) for the collection agent.
- **Microsoft Windows:** Go to the Audit Vault Server or collection agent `ORACLE_HOME\bin` directory.

Syntax

```
avdb2db verify -src host:port:database_name
```

Arguments

Argument	Description
<code>-src host:port:database_name</code>	Enter the source database connection information: host name and port number, separated by a colon. Typically, the host is the fully qualified domain name or IP address of the server on which the IBM DB2 source database is running, and the port number is 50000. The <code>database_name</code> setting refers to the name of the DB2 source database.

Usage Notes

- The `avdb2db verify` command checks the following:
 - Whether the version of the database is supported: Versions 8.2 through 9.5
 - Whether the source user has the required privileges in the source database that is to be registered with Oracle Audit Vault
 - Whether auditing is enabled in the source database
 - Whether the operating system on which the source database is running is supported
- If you installed the collection agent on a Microsoft Windows computer and want to run the `avdb2db verify` command from there, run it from the `ORACLE_HOME\bin` directory. For UNIX or Linux installations, set the appropriate

environment variables before running this command. See [Section 2.2](#) for more information.

- The `avdb2db verify` command prompts for a user name and password. This user account must have privileges to run the IBM DB2 `db2audit` command (for example, a user who has the `sysadmin` privilege).

Example

The following example verifies that the source database is compatible with the DB2 collector on a Linux or UNIX system.

```
avdb2db verify -src 192.0.2.7:50000:sales_db
Enter a username : source_user_name
Enter a password : password

***** Source Verified *****
```

REDO Collector Database Reference

This chapter contains:

- [About the Recommended Settings for the REDO Collector](#)
- [Recommended Oracle Streams Supplemental Logging](#)
- [Oracle Database 11g Release 2 \(11.2\) Audit Source Parameter Recommendations](#)
- [Oracle Database 11g Release 1 \(11.1\) Audit Source Parameter Recommendations](#)
- [Oracle Database 10g Release 2 \(10.2\) Audit Source Parameter Recommendations](#)
- [Oracle Database 10g Release 1 \(10.1\) Audit Source Parameter Recommendations](#)
- [Oracle9i Database Release 2 \(9.2\) Audit Source Parameter Recommendations](#)

12.1 About the Recommended Settings for the REDO Collector

This chapter describes recommendations for setting initialization parameters if you plan to use the REDO collector to collect audit data. After you change the initialization parameters described in these sections, you must restart the source database before configuring the REDO collect to collect audit data.

See Also:

- [Table 1–10, "Oracle Database Redo Log Setting for the REDO Collector"](#) on page 1-14
- *Oracle Audit Vault Auditor's Guide* for instructions on creating a capture rule for redo log files

12.2 Recommended Oracle Streams Supplemental Logging

Oracle recommends that you enable Oracle Streams supplemental logging for at minimum the primary key columns. This enables auditors to identify the row for which they see before and after values. In addition to logging these columns, you should log any other columns that your site requires.

See Also: *Oracle Streams Replication Administrator's Guide* for information about managing supplemental logging in Oracle Streams

12.3 Oracle Database 11g Release 2 (11.2) Audit Source Parameter Recommendations

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.

Table 12–4 lists the initialization parameters that you must configure for each source database that will use the REDO log collector.

Table 12–1 Initialization Parameters to Be Configured for the 11.2 Source Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE	Mandatory	Default: 11.2.0 Range: 10.0.0 to default release 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 Oracle Streams features introduced in Oracle Database 11g Release 2, this parameter must be set to 11.2.0 or higher.
GLOBAL_NAMES	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 Oracle Streams to share information between databases, set this parameter to true at each database that is participating in your Oracle Streams environment.
LOG_ARCHIVE_CONFIG	Recommended	Default: 'SEND, RECEIVE, NODG_CONFIG' Range: Values: <ul style="list-style-type: none"> ▪ SEND ▪ NOSEND ▪ RECEIVE ▪ NORECEIVE ▪ DG_CONFIG ▪ NODG_CONFIG Modifiable? Yes	Enables or disables the sending of redo logs to remote destinations and the receipt of remote redo logs, and specifies the unique database names (DB_UNIQUE_NAME) for each database in the Data Guard configuration To use downstream capture and copy the redo data to the downstream database using redo transport services, specify the DB_UNIQUE_NAME of the source database and the downstream database using the DG_CONFIG attribute. This parameter must be set at both the source database and the downstream database.
LOG_ARCHIVE_DEST_ <i>n</i>	Recommended	Default: None Range: None Modifiable? Yes	Defines up to 31 log archive destinations, where <i>n</i> is 1, 2, 3, ... 31. To use downstream capture and copy the redo data to the downstream database using redo transport services, at least one log archive destination must be set at the site running the downstream capture process.
LOG_ARCHIVE_DEST_STATE_ <i>n</i>	Recommended	Default: enable Range: One of the following: <ul style="list-style-type: none"> ▪ alternate ▪ defer ▪ enable Modifiable? Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 31) specifies one of the corresponding LOG_ARCHIVE_DEST_ <i>n</i> destination parameters. To use downstream capture and copy the redo data to the downstream database using redo transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_ <i>n</i> destination for the downstream database is set to enable.

Table 12–1 (Cont.) Initialization Parameters to Be Configured for the 11.2 Source Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
LOG_BUFFER	Recommended	Default: 5 MB to 32 MB depending on configuration Range: Operating system-dependent Modifiable? No	Specifies the amount of memory (in bytes) that Oracle uses when buffering redo entries to a redo log file. Redo log entries contain a record of the changes that have been made to the database block buffers. If an Oracle Streams capture process is running on the database, then set this parameter properly so that the capture process reads redo log records from the redo log buffer rather than from the hard disk.
MEMORY_MAX_TARGET	Recommended	Default: 0 Range: 0 to the physical memory size available to Oracle Database Modifiable? No	Specifies the maximum systemwide usable memory for an Oracle database. If the MEMORY_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the maximum memory usage of the Oracle database.
MEMORY_TARGET	Recommended	Default: 0 Range: 152 MB to MEMORY_MAX_TARGET setting Modifiable? Yes	Specifies the systemwide usable memory for an Oracle database. Oracle recommends enabling the autotuning of the memory usage of an Oracle database by setting MEMORY_TARGET to a large nonzero value (if this parameter is supported on your platform).
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 an Oracle Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PROCESSES	Recommended	Default: 100 Range: 6 to operating system-dependent 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 and slave processes. In Oracle Streams, capture processes, apply processes, XStream inbound servers, and XStream outbound servers use background processes. Propagations use background processes in combined capture and apply configurations. Propagations use Oracle Scheduler slave processes in configurations that do not use combined capture and apply.
SESSIONS	Recommended	Default: Derived from: $(1.1 * PROCESSES) + 5$ Range: 1 to 2^{31} Modifiable? No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes, apply processes, XStream outbound servers, or XStream inbound servers in a database, you might need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system-dependent Modifiable? No	Specifies the maximum size of System Global Area (SGA) for the lifetime of a database instance. If the SGA_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the SGA size.

Table 12–1 (Cont.) Initialization Parameters to Be Configured for the 11.2 Source Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
SGA_TARGET	Mandatory	Default: 0 (SGA autotuning is disabled) Range: 64 MB to operating system-dependent Modifiable? Yes	<p>Specifies the total size of all System Global Area (SGA) components.</p> <p>If MEMORY_MAX_TARGET and MEMORY_TARGET are set to 0 (zero), then Oracle recommends enabling the autotuning of SGA memory by setting SGA_TARGET to a large nonzero value.</p> <p>If this parameter is set to a nonzero value, then the size of the Oracle Streams pool is managed by Automatic Shared Memory Management.</p>
SHARED_POOL_SIZE	Recommended	Default: When SGA_TARGET is set to a nonzero value: If the parameter is not specified, then the default is 0 (internally determined by Oracle Database). If the parameter is specified, then the user-specified value indicates a minimum value for the shared memory pool. When SGA_TARGET is not set (32-bit platforms): 64 MB, rounded up to the nearest granule size. When SGA_TARGET is not set (64-bit platforms): 128 MB, rounded up to the nearest granule size. Range: The granule size to operating system-dependent Modifiable? Yes	<p>Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures.</p> <p>If the MEMORY_MAX_TARGET, MEMORY_TARGET, SGA_TARGET, and STREAMS_POOL_SIZE initialization parameters are set to zero, then Oracle Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Oracle Streams pool.</p>

Table 12–1 (Cont.) Initialization Parameters to Be Configured for the 11.2 Source Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE	Mandatory	Default: 0 Range: 0 to operating system-dependent limit Modifiable? Yes	<p>Specifies (in bytes) the size of the Oracle Streams pool. The Oracle Streams pool contains buffered queue messages. In addition, the Oracle Streams pool is used for internal communications during parallel capture and apply.</p> <p>If the MEMORY_TARGET or MEMORY_MAX_TARGET initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Memory Management, and STREAMS_POOL_SIZE specifies the minimum size.</p> <p>If the SGA_TARGET initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Shared Memory Management, and STREAMS_POOL_SIZE specifies the minimum size.</p> <p>This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Oracle Streams processes and jobs might not run.</p> <p>Ensure that there is enough memory to accommodate the Oracle Streams components. The following are the minimum requirements:</p> <ul style="list-style-type: none"> 15 MB for each capture process parallelism 10 MB or more for each buffered queue. The buffered queue is where the buffered messages are stored. 1 MB for each apply process parallelism 1 MB for each XStream outbound server 1 MB for each XStream inbound server parallelism <p>For example, if parallelism is set to 3 for a capture process, then at least 45 MB is required for the capture process. If a database has two buffered queues, then at least 20 MB is required for the buffered queues. If parallelism is set to 4 for an apply process, then at least 4 MB is required for the apply process.</p> <p>You can use the V\$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter.</p>
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	<p>Specifies whether statistics related to time are collected.</p> <p>To collect elapsed time statistics in the dynamic performance views related to Oracle 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.</p>
UNDO_RETENTION	Recommended	Default: 900 Range: 0 to 2 ³² - 1 Modifiable? Yes	<p>Specifies (in seconds) the amount of committed undo information to retain in the database.</p> <p>For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period.</p> <p>If you run 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.</p>

12.4 Oracle Database 11g Release 1 (11.1) Audit Source Parameter Recommendations

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`.

Table 12–2 describes the hidden parameter that you must configure for each source database that will use the REDO log collector.

Table 12–2 Hidden Initialization Parameters to Be Configured for the 11.1 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>_job_queue_interval=1</code>	Recommended	5	Scan rate interval (seconds) of job queue

Table 12–4 lists the initialization parameters that you must configure for each source database that will use the REDO log collector. 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 parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table 12–3 Initialization Parameters to Be Configured for the 11.1 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>COMPATIBLE= 11.1.0</code>	Mandatory	Default: 11.1.0 Range: 10.1.0 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 10g 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 10g release 2, this parameter must be set to 10.2.0 or higher. To use the new Streams features introduced in Oracle Database 11g release 1, this parameter must be set to 11.1.0 or higher.
<code>GLOBAL_NAMES=true</code>	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 <code>true</code> at each database that is participating in your Streams environment.
<code>JOB_QUEUE_PROCESSES=4</code>	Mandatory	Default: 0 Range: 0 to 1000 Modifiable? Yes	Specifies the number of <i>Jnnn</i> job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by <code>DBMS_JOB</code> . 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 12–3 (Cont.) Initialization Parameters to Be Configured for the 11.1 Source Database

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: <i>Oracle Data Guard Concepts and Administration</i>
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.
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.
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. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
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. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.

Table 12–3 (Cont.) Initialization Parameters to Be Configured for the 11.1 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE=0	Recommended	<p>Default: 32-bit platforms: 32 MB, rounded up to the nearest granule size</p> <p>64-bit platforms: 84 MB, rounded up to the nearest granule size</p> <p>Range: Minimum: the granule size</p> <p>Maximum: operating system-dependent</p> <p>Modifiable? Yes</p>	<p>Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures.</p> <p>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.</p> <p>The STREAMS_POOL_SIZE initialization parameter should be set to 200 MB and, if necessary, increment the SGA_TARGET and SGA_MAX initialization parameters appropriately. For example, if the SGA_TARGET initialization parameter is already set to 2 GB, setting STREAMS_POOL_SIZE=200 MB would not require that the SGA_TARGET initialization parameter be increased. However, if the SGA_TARGET initialization parameter is set to 600 MB and the STREAMS_POOL_SIZE initialization parameter is increased to 200 MB, then it is recommended that the SGA_TARGET initialization parameter value be increased similarly.</p>

Table 12–3 (Cont.) Initialization Parameters to Be Configured for the 11.1 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE=200	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system-dependent Modifiable? Yes	<p>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.</p> <p>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.</p> <p>This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Streams processes and jobs will not run.</p> <p>You should increase the size of the Streams pool for each of the following factors:</p> <ul style="list-style-type: none"> 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 <p>You can use the V\$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter.</p> <p>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.</p>
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	<p>Specifies whether statistics related to time are collected.</p> <p>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:</p> <ul style="list-style-type: none"> V\$STREAMS_CAPTURE V\$STREAMS_APPLY_COORDINATOR V\$STREAMS_APPLY_READER V\$STREAMS_APPLY_SERVER
UNDO_RETENTION=3600	Recommended	Default: 900 Range: 0 to 2 ³² -1 (max value represented by 32 bits) Modifiable? Yes	<p>Specifies (in seconds) the amount of committed undo information to retain in the database.</p> <p>For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period.</p> <p>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.</p> <p>See Also: <i>Oracle Database Administrator's Guide</i> for more information about the UNDO_RETENTION parameter</p>

12.5 Oracle Database 10g Release 2 (10.2) Audit Source Parameter Recommendations

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.

Table 12–4 describes the hidden parameter that you must configure for each source database that will use the REDO log collector.

Table 12–4 Hidden Initialization Parameters to Be Configured for the 10.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue

Table 12–5 lists the initialization parameters that you must configure for each source database. 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 two parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table 12–5 Initialization Parameters to Be Configured for the 10.2 Source Database

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 database must maintain compatibility. Oracle databases with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10g release 1, set this parameter to 10.1.0 or higher. To use downstream capture, set this parameter 10.1.0 or higher for both the source database and the downstream database. To use the new Streams features introduced in Oracle Database 10g release 2, set this parameter 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 for each database that participates in your Streams environment.
JOB_QUEUE_PROCESSES=4	Mandatory	Default: 0 Range: 0 to 1000 Modifiable? Yes	Specifies the number of job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by the DBMS_JOB PL/SQL package. Set this parameter to at least 2 for each database that propagates events in your Streams environment, and then set it to the same value as the maximum number of jobs that can run simultaneously, plus 2.
LOG_ARCHIVE_DEST_n	Recommended	Default: None Range: None Modifiable? Yes	Defines up to ten log archive destinations, where <i>n</i> 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: <i>Oracle Data Guard Concepts and Administration</i>

Table 12–5 (Cont.) Initialization Parameters to Be Configured for the 10.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_ARCHIVE_DEST_ STATE_ <i>n</i>	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_ <i>n</i> 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_ <i>n</i> 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, external procedures, and cartridges, each of which uses a separate process. In a Streams environment, set this parameter 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 Database increases 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 an Oracle database. 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 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. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
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 you set this parameter to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.

Table 12–5 (Cont.) Initialization Parameters to Be Configured for the 10.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
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	<p>Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures.</p> <p>If you set the <code>SGA_TARGET</code> and <code>STREAMS_POOL_SIZE</code> initialization parameters to zero, then Streams transfers an amount equal to 10 percent of the shared pool from the buffer cache to the Streams pool.</p>

Table 12–5 (Cont.) Initialization Parameters to Be Configured for the 10.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE=200	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system-dependent Modifiable? Yes	<p>Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, Oracle Database uses the Streams pool for internal communications during parallel capture and apply.</p> <p>If you set the <code>SGA_TARGET</code> initialization parameter to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and <code>STREAMS_POOL_SIZE</code> specifies the minimum size.</p> <p>You should set the <code>STREAMS_POOL_SIZE</code> initialization parameter to 200 MB and, if necessary, increment the <code>SGA_TARGET</code> and <code>SGA_MAX</code> initialization parameters appropriately. For example, if the <code>SGA_TARGET</code> initialization parameter is already set to 2 GB, setting <code>STREAMS_POOL_SIZE=200 MB</code> does not require you to increase the <code>SGA_TARGET</code> initialization parameter setting. However, if the <code>SGA_TARGET</code> initialization parameter is set to 600 MB and the <code>STREAMS_POOL_SIZE</code> initialization parameter is increased to 200 MB, then you should increase the <code>SGA_TARGET</code> initialization parameter value similarly.</p> <p>This parameter is modifiable. If you reduce this parameter setting to zero when an instance is running, then Streams processes and jobs cannot run.</p> <p>You should increase the size of the Streams pool for each of the following factors:</p> <ul style="list-style-type: none"> ■ 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 <p>You can use the <code>V\$STREAMS_POOL_ADVICE</code> dynamic performance view to determine an appropriate setting for this parameter.</p> <p>For example, if you set parallelism to 3 for a capture process, then increase the Streams pool by 30 MB. If you set parallelism to 5 for an apply process, then increase the Streams pool by 5 MB.</p>
TIMED_STATISTICS	Recommended	Default: If <code>STATISTICS_LEVEL</code> is set to <code>TYPICAL</code> or <code>ALL</code> , then <code>true</code> If <code>STATISTICS_LEVEL</code> is set to <code>BASIC</code> , then <code>false</code> The default for <code>STATISTICS_LEVEL</code> is <code>TYPICAL</code> . Range: <code>true</code> or <code>false</code> Modifiable? Yes	<p>Specifies whether statistics related to time are collected.</p> <p>To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to <code>true</code>. The following views include elapsed time statistics:</p> <p><code>V\$STREAMS_CAPTURE</code> <code>V\$STREAMS_APPLY_COORDINATOR</code> <code>V\$STREAMS_APPLY_READER</code> <code>V\$STREAMS_APPLY_SERVER</code></p>

Table 12–5 (Cont.) Initialization Parameters to Be Configured for the 10.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
UNDO_RETENTION=3600	Recommended	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, set this parameter 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: <i>Oracle Database Administrator's Guide</i> for more information about the UNDO_RETENTION parameter

12.6 Oracle Database 10g Release 1 (10.1) Audit Source Parameter Recommendations

Table 12–6 describes the hidden parameter that you must configure for each source database that will use the REDO log collector.

Table 12–6 Hidden Initialization Parameters to Be Configured for the 10.1 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue

Table 12–7 lists the initialization parameters that you must configure for each source database that will use the REDO log collector.

Table 12–7 Initialization Parameters to Be Configured for the 10.1 Source Database

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 database must maintain compatibility. Oracle databases with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10g, set this parameter to 10.1.0 or higher. To use downstream capture, set the parameter to 10.1.0 or higher for 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 for each database in your Streams environment.

Table 12–7 (Cont.) Initialization Parameters to Be Configured for the 10.1 Source Database

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 job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by the DBMS_JOB PL/SQL package. Set this parameter to at least 2 at each database that propagates events in your Streams environment, and then set it to the same value as the maximum number of jobs that can run simultaneously, plus 2.
LOG_ARCHIVE_DEST_n	Recommended	Default: None Range: None Modifiable? Yes	Defines up to ten log archive destinations, where <i>n</i> is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, have at least one log archive destination on the site that runs the downstream capture process. See Also: <i>Oracle Data Guard Concepts and Administration</i>
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, external procedures, and cartridges, each of which uses a separate process. In a Streams environment, set this parameter 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 Database increases 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 Database. 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.

Table 12–7 (Cont.) Initialization Parameters to Be Configured for the 10.1 Source Database

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 you set the STREAMS_POOL_SIZE initialization parameter to zero, then Streams can use up to 10 percent of the shared pool.

Table 12–7 (Cont.) Initialization Parameters to Be Configured for the 10.1 Source Database

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	<p>Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, Oracle Database uses the Streams pool for internal communications during parallel capture and apply.</p> <p>If the size of the Streams pool is greater than zero, then Oracle Database allocates any SGA memory used by Streams from the Streams pool. If you set the Streams pool size to zero, then Oracle Database allocates SGA memory used by Streams from the shared pool and can use up to 10 percent of the shared pool.</p> <p>You can modify this parameter. However, if you set this parameter to zero when a database 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 you set this parameter to a value greater than zero when an instance starts and is then reduce it to zero when the instance is running, then Streams processes and jobs will not run.</p> <p>You should increase the size of the Streams pool for each of the following factors:</p> <ul style="list-style-type: none"> ■ 10 MB for each capture process parallelism ■ 1 MB for each apply process parallelism ■ 10 MB or more for each queue staging captured events <p>For example, suppose you set parallelism to 3 for a capture process, and then increase the Streams pool by 30 MB. If you set parallelism to 5 for an apply process, then you must increase the Streams pool by 5 MB.</p>
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	<p>Specifies whether statistics related to time are collected.</p> <p>To collect elapsed time statistics in the data dictionary views related to Streams, set this parameter to true. The following views include elapsed time statistics:</p> <p>V\$STREAMS_CAPTURE V\$STREAMS_APPLY_COORDINATOR V\$STREAMS_APPLY_READER V\$STREAMS_APPLY_SERVER</p>
UNDO_RETENTION=3600	Recommended	Default: 900 Range: 0 to 2 ³² -1 (max value represented by 32 bits) Modifiable? Yes	<p>Specifies (in seconds) the amount of committed undo information to retain in the database.</p> <p>For a database running one or more capture processes, set this parameter to specify an adequate undo retention period.</p> <p>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.</p> <p>See Also: <i>Oracle Database Administrator's Guide</i> for more information about the retention period and the undo tablespace</p>

12.7 Oracle9i Database Release 2 (9.2) Audit Source Parameter Recommendations

Table 12–8 describes the hidden parameter that you must configure for each source database that will use the REDO log collector.

Table 12–8 Hidden Initialization Parameters to Be Configured for the 9.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>_first_spare_parameter=200M/(current_shared_pool_size+200M)</code>	Mandatory	10	The threshold (percent) of <code>SHARED_POOL_SIZE</code> memory at which spillover to disk is triggered for captured messages
<code>_kghdsidx_count=1</code>	Recommended	Range: 10 to 80	This parameter prevents the <code>SHARED_POOL</code> from being divided among CPUs.
<code>_job_queue_interval=1</code>	Recommended	5	Scan rate interval (seconds) of job queue

Table 12–9 lists the initialization parameters that you must configure for each source database that will use the REDO log collector. The `SHARED_POOL_SIZE` parameter is of particular importance for REDO collectors.

Table 12–9 Initialization Parameters to Be Configured for the 9.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>AQ_TM_PROCESSES=4</code>	Mandatory	Default: 0 Range: 0 to 10	Establishes queue monitor processes. Setting the parameter to 1 or higher starts the specified number of queue monitor processes. These queue monitor processes manage time-based operations of messages such as delay and expiration, clean up retained messages after the specified retention time, and clean up consumed messages if the retention time is zero. This parameter is required for both Streams captured messages and user-enqueued messages.
<code>COMPATIBLE=9.2.0</code>	Mandatory	Default: 8.1.0 Range: 8.1.0 to Current Release Number	This parameter specifies the release with which the Oracle database must maintain compatibility. Oracle databases with different compatibility levels can interoperate. To use Streams, then set this parameter to 9.2.0 or higher.
<code>GLOBAL_NAMES=true</code>	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 <code>true</code> for each database that in your Streams environment.
<code>JOB_QUEUE_PROCESSES=4</code>	Mandatory	Default: 0 Range: 0 to 1000	Specifies the number of job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by <code>DBMS_JOB</code> . You can change the setting for <code>JOB_QUEUE_PROCESSES</code> dynamically by using the <code>ALTER SYSTEM SQL</code> statement. Set this parameter to at least 2 for each database that propagates events in your Streams environment, and set it to the same value as the maximum number of jobs that can run simultaneously, plus 2.

Table 12–9 (Cont.) Initialization Parameters to Be Configured for the 9.2 Source Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_PARALLELISM=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 set this parameter to 1. Setting this parameter to 1 does not affect the parallelism of capture. You can set parallelism for a capture process running 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, external procedures, and cartridges, each of which uses a separate process. In a Streams environment, set this parameter to the default value of 4 or higher.
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 Database increases 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 Database. 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 12–9 (Cont.) Initialization Parameters to Be Configured for the 9.2 Source Database

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 to store logical change records (LCRs) in the buffer queue. Size this parameter so that LCRs remain in memory as long as possible. Use the following formula to calculate the point at which LCRs will spill to disk. $\text{SHARED_POOL_SIZE} * _first_spare_parameter / 100$
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 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 following views include elapsed time statistics: 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 set to true, Oracle Database 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 Database 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 can 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. Set TRANSACTION_AUDITING to TRUE for databases that have a Streams capture process configured

Table 12–10 describes the initialization parameter that you must configure for an Oracle Real Application Clusters (Oracle RAC) environment, in addition to the parameters described in Table 12–8 and Table 12–9. Configure this parameter on each Oracle RAC instance.

Table 12–10 ARCHIVE_LAG_TARGET Recommended Setting

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 an Oracle 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 <i>Oracle9i Streams</i> release 2 (9.2)

Troubleshooting an Oracle Audit Vault System

This appendix contains:

- [Location of Audit Vault Server Log and Error Files](#)
- [Location of Audit Vault Collection Agent Log and Error Files](#)
- [Troubleshooting Tips](#)

A.1 Location of Audit Vault Server Log and Error Files

[Table A-1](#) describes the Audit Vault Server log and error files. These files are located in the Audit Vault Server `$ORACLE_HOME/av/log` directory. They contain important information about the return status of commands and operations. Use this information to diagnose problems. You should periodically monitor these files, and delete these files to control the amount of disk space the log files use.

Table A-1 Names and Descriptions of Audit Vault Server Log and Error Files

File Name	Description
<code>agent.err</code>	Contains a log of errors encountered in collection agent initialization. You can delete this file at any time.
<code>agent.out</code>	Contains a log of all primary collection agent-related operations and activity. You can delete this file at any time.
<code>alert-email-%g.log.n</code>	Contains a log of the e-mail alert operations and any errors returned from those operations. You can delete this file at any time. The <code>%g</code> is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. A concurrent existence of this file is indicated by a <code>.n</code> suffix appended to the file type name, such as <code>av_client-%g.log.n</code> , where <code>n</code> is an integer issued in sequence (for example, <code>alert-email-0.log.1</code>).
<code>alert_troubleticket-%g.log.n</code>	Contains a log of the trouble ticket alert operations and any errors returned from those operations. You can delete this file at any time. The <code>%g</code> is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. A concurrent existence of this file is indicated by a <code>.n</code> suffix appended to the file type name, such as <code>av_client-%g.log.n</code> , where <code>n</code> is an integer issued in sequence (for example, <code>alert_troubleticket-0.log.1</code>).
<code>avca.log</code>	Contains a log of all AVCA and AVCTL commands that have been run and the results of running each command. You can only delete this file only after you have shut down the Audit Vault Server.

Table A-1 Names and Descriptions of Audit Vault Server Log and Error Files

File Name	Description
av_client-%g.log.n	Contains a log of the collection agent operations and any errors returned from those operations. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 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).
avorcldb.log	Contains a log of all AVORCLDB commands that have been run and the results of running each command. You can delete this file at any time.
DB2DB-%g.log	Contains a log of all AVDB2DB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVDB2DB commands, restart Oracle Audit Vault from the Audit Vault Server with the log level set to debug, as follows: avctl stop_av -loglevel debug avctl start_av -loglevel debug
MSSQLDB-%g.log	Contains a log of all AVMSSQLDB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVMSSQLDB commands, restart Oracle Audit Vault from the Audit Vault Server with the log level set to debug, as follows: avctl stop_av -loglevel debug avctl start_av -loglevel debug
report-generation-%g.log	Contains a report for both recurring scheduled and manual log messages. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit.
SYBDB-%g.log	Contains a log of all AVSYBDB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVSYBDB commands, restart Oracle Audit Vault from the Audit Vault Server with the log level set to debug, as follows: avctl stop_av -loglevel debug avctl start_av -loglevel debug
report-generation-0.log	Contains report generation-related log messages. This file is created when Oracle Audit Vault generates PDF reports in the Audit Vault Server. You can delete this file at any time.
policy-0.log	Contains policy-related log messages for Oracle database audit policies created in Audit Vault. This file is created when Oracle Audit Vault fetches audit settings from a source database, or provisions the audit settings back to the source database. You can delete this file at any time.

If you need to troubleshoot the Audit Vault Console, enable Oracle Enterprise Manager logging. To do so, modify the `emomslogging.properties` file (located in the `$ORACLE_HOME/sysman/config` directory) in the Audit Vault Server home. Add the following lines to this file:

```
log4j.appender.avAppender=org.apache.log4j.RollingFileAppender
log4j.appender.avAppender.File=$ORACLE_HOME/oc4j/j2ee/OC4J_DBConsole__/_log/av-application.log
log4j.appender.avAppender.Append=true
log4j.appender.avAppender.MaxFileSize =20000000
```

```
log4j.appender.avAppender.Threshold = DEBUG
log4j.appender.avAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.avAppender.layout.ConversionPattern=%d [%t] %-5p %c{2} %M.%L - %m\n
log4j.category.oracle =DEBUG, avAppender
```

You can use this information to debug communication problems between the server and the collection agents.

A.2 Location of Audit Vault Collection Agent Log and Error Files

[Table A-2](#) lists the names and a description of the Audit Vault collection agent log and error files located in the \$ORACLE_HOME/av/log directory. These files contain important information about the return status of commands and operations. Use this information to diagnose problems.

Table A-2 Names and Descriptions of Audit Vault Collection Agent Log and Error Files

File Name	Description
agent.err	Contains a log of all errors encountered in collection agent initialization and operation. You can delete this file at any time.
agent.out	Contains a log of all primary collection agent-related operations and activity. You can delete this file at any time.
avca.log	Contains a log of all AVCA and AVCTL commands that have been run and the results of running each command. You can delete this file at any time.
avorcldb.log	Contains a log of all AVORCLDB commands that have been run and the results of running each command. You can delete this file at any time.
collname_srcname_src_id.log	Contains a log of information about what was collected and any collection errors for the DBAUD and OSAUD collectors. This file has no maximum size limit. To delete this log, shut down the collector, delete the log, and then restart the collector. See also Section A.3.4 for more information troubleshooting collectors.

Table A–2 (Cont.) Names and Descriptions of Audit Vault Collection Agent Log and Error Files

File Name	Description
<code>srcname-collname-#.log</code>	<p>Applies to all collectors, as follows:</p> <ul style="list-style-type: none"> ■ Oracle Database DBAUD, OSAUD, and REDO collectors. Contains monitoring information, such as whether the collector is active and how many records were sent. For the REDO collector, the Streams framework performs the actual collection, so the Oracle Audit Vault agent has no knowledge of the collection. ■ Non-Oracle Database collectors. Contains a log of all collection operations for the MSSQLDB, SYBDB, and DB2 collectors. <p>The # symbol refers to the generation number of the log file. The maximum log file size is 100 MB.</p> <p>A <code>srcname-collname-#.log.lck</code> accompanies the log files. You can safely ignore this file.</p> <p>You can only delete this file after you have shut down the agent (for Release 10.2.3.2 collection agents) or OC4J (for Release 10.2.3.1 or earlier agents but not yet upgraded). For example, to delete the log where # is 0, you must stop the agent or OC4J. To delete the logs where # is higher than 0, you can do so while the agent or OC4J is running.</p> <p>To increase the log level, restart the agent or OC4J with the appropriate debug level, as in the following examples:</p> <p>Release 10.2.3.2:</p> <pre>avctl stop_agent avctl start_agent -loglevel error</pre> <p>See Section 7.12 and Section 7.9 for information about these commands, including the available log levels.</p> <p>Release 10.2.3.1 or earlier:</p> <pre>avctl stop_oc4j avctl start_oc4j -loglevel error</pre> <p>See Section 7.15.3 and Section 7.15.2 for information about these commands, including the available log levels.</p>
<code>agent_client-%g.log.n</code>	<p>Contains a log of the collection 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 100 MB limit. A concurrent existence of this file is indicated by a .n suffix appended to the file type name, such as <code>av_client-%g.log.n</code>, where n is an integer issued in sequence, for example, <code>av_client-0.log.1</code>. You can delete this file at any time.</p>

Table A–2 (Cont.) Names and Descriptions of Audit Vault Collection Agent Log and Error Files

File Name	Description
DB2DB-%g.log	<p>Contains a log of all AVDB2DB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVDB2DB commands, restart the agent (for Release 10.2.3.2 agents) or OC4J (for Release 10.2.3.1 or earlier but not yet upgraded) with the log level set to debug, as follows:</p> <p>Release 10.2.3.2:</p> <pre>avctl stop_agent avctl start_agent -loglevel error</pre> <p>See Section 7.12 and Section 7.9 for information about these commands, including the available log levels.</p> <p>Release 10.2.3.1 or earlier:</p> <pre>avctl stop_oc4j avctl start_oc4j -loglevel error</pre> <p>See Section 7.15.3 and Section 7.15.2 for information about these commands, including the available log levels.</p>
MSSQLDB-%g.log	<p>Contains a log of all AVMSSQLDB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVMSSQLDB commands, restart the agent (for Release 10.2.3.2 agents) or OC4J (for Release 10.2.3.1 or earlier but not yet upgraded) on the collection agent side with the log level set to debug, as follows:</p> <p>Release 10.2.3.2:</p> <pre>avctl stop_agent avctl start_agent -loglevel error</pre> <p>See Section 7.12 and Section 7.9 for information about these commands, including the available log levels.</p> <p>Release 10.2.3.1 or earlier (but not yet upgraded):</p> <pre>avctl stop_oc4j avctl start_oc4j -loglevel error</pre> <p>See Section 7.15.3 and Section 7.15.2 for information about these commands, including the available log levels.</p>
SYBDB-%g.log	<p>Contains a log of all AVSYBDB commands that have been run and the results of running each command. You can delete this file at any time. The %g is a generation number that starts from 0 (zero) and increases once the file size reaches the 100 MB limit. To enable detailed logging of AVSYBDB commands, restart the agent (for Release 10.2.3.2 agents) or OC4J (for Release 10.3.2.1 or earlier, but not yet upgraded) on the collection agent side with the log level set to debug, as follows:</p> <p>Release 10.2.3.2:</p> <pre>avctl stop_agent avctl start_agent -loglevel error</pre> <p>See Section 7.12 and Section 7.9 for information about these commands, including the available log levels.</p> <p>Release 10.2.3.1 or earlier:</p> <pre>avctl stop_oc4j avctl start_oc4j -loglevel error</pre> <p>See Section 7.15.3 and Section 7.15.2 for information about these commands, including the available log levels.</p>

Table A–2 (Cont.) Names and Descriptions of Audit Vault Collection Agent Log and Error Files

File Name	Description
sqlnet.log	Contains a log of SQL*Net information.

The Oracle Audit Vault collection agent `$ORACLE_HOME/oc4j/j2ee/home/log` contains the logs generated by the collection agent OC4J. In this directory, the file `AVAgent-access.log` contains a log of requests that the collection agent receives from the Audit Vault Server. Use this information to debug communication problems between the server and the collection agent.

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

A.3 Troubleshooting Tips

This section contains:

- [Checking Trace Files for Detailed Information About Oracle Database Errors](#)
- [Troubleshooting Audit Vault Server](#)
- [Troubleshooting Audit Vault Collection Agent](#)
- [Troubleshooting the Audit Vault Collectors](#)
- [Troubleshooting Oracle Audit Vault Console](#)
- [Troubleshooting the Oracle Audit Vault Audit Reports](#)
- [Troubleshooting Oracle Audit Vault in an Oracle Real Application Clusters Environment](#)

A.3.1 Checking Trace Files for Detailed Information About Oracle Database Errors

For detailed information about the cause of an Oracle Database error message, check the trace files. The trace files also indicate problems that may have occurred with the Audit Vault data warehouse, alert, and some configuration issues. The `USER_DUMP_DEST` initialization parameter specifies the current location of the trace files. You can find the value of this parameter by issuing `SHOW PARAMETER USER_DUMP_DEST` in SQL*Plus. See *Oracle Database Performance Tuning Guide* for more information about trace files.

A.3.2 Troubleshooting Audit Vault Server

This section contains:

- [Tuning Audit Vault Server Performance for the REDO Collector](#)

A.3.2.1 Tuning Audit Vault Server Performance for the REDO Collector

Problem: You are concerned that the Audit Vault Server performance for the REDO collector is slow. The Audit Vault Server installation process sets the `STREAMS_POOL_SIZE` initialization parameter to 150 MB. If you plan to use the REDO collector, you must tune this parameter to maximize REDO collector performance. In an Oracle Real Application Clusters (Oracle RAC) environment, tune this parameter on all nodes, because it is uncertain where the queue will be after a database instance starts.

Solution: Typically, after you have configured and started the REDO collector, let it run for a while. This enables the Oracle Database autotuning feature to allocate memory for the best database performance for the `STREAMS_POOL_SIZE` parameter. Using Automatic Workload Repository (AWR), check if Streams AQ has a flow control problem, such as enqueue being blocked. If the performance is slow (for example, only 500 records are applied per second), you may need to tune the `STREAMS_POOL_SIZE` parameter.

If you have at least 1 GB of physical memory in your Audit Vault Server system, set the `STREAMS_POOL_SIZE` parameter to 200 MB using the `ALTER SYSTEM SQL` statement, as follows:

```
ALTER SYSTEM SET STREAMS_POOL_SIZE=200;
```

The record apply rate should be 2000 records per second, which is a typical maximum rate for the REDO collector. Usually, setting the value to 200 MB is sufficient. If you are using Oracle Audit Vault in an Oracle RAC environment, set this parameter value accordingly on all nodes in the cluster, as follows:

```
ALTER SYSTEM SET STREAMS_POOL_SIZE=200 SID=avn;
```

Replace `avn` with the SID for each node in the cluster.

A.3.3 Troubleshooting Audit Vault Collection Agent

This section contains:

- [Blank Status on Windows Services Panel for Audit Vault Agent](#)
- [Debugging a Collection Agent Problem](#)
- [The Agent OC4J or Audit Vault Console OC4J Failing to Start](#)
- [Failed Source Database Connection Due to Invalid Wallet Credentials](#)

A.3.3.1 Blank Status on Windows Services Panel for Audit Vault Agent

Problem: After you install Audit Vault Agent for Microsoft Windows (32-bit), configure a source database and collectors, and then start the agent on the Audit Vault Server side, you notice that the Services Panel on the Windows system where the Audit Vault collection agent resides shows that the status is blank, rather than **Started**.

Solution: This is normal behavior for the Audit Vault collection agent on Microsoft Windows systems because the service is a short-lived process. Once the Agent service process completes its task, it exits, so the status of the service will not show as Started. However, the Audit Vault collection agent is running without problems.

Run the `avctl show_agent_status` command to check the status of the Audit Vault Agent, as follows:

```
C:\ORACLE_HOME\bin\avctl show_oc4j_status
```

A.3.3.2 Debugging a Collection Agent Problem

Problem: You discover that there is a problem with the Audit Vault collection agents, so you want to enable debug logging while trying to diagnose the problem.

Solution:

1. Open a shell or command prompt for the Audit Vault collection agent.
 - **UNIX:** Set the environment variables, as described in [Section 2.2.3](#).
 - **Microsoft Windows:** Go to the collection agent `ORACLE_HOME\bin` directory.

2. Run the following AVCTL commands on the command line:

- **For Release 10.2.3.2 agents:** Run the following commands:

```
avctl stop_agent
avctl start_agent -loglevel debug
```

- **For Release 10.2.3.1 or earlier agents that have not been upgraded:** Run these commands:

```
avctl stop_oc4j
avctl start_oc4j -loglevel debug
```

3. Check the log output in the Audit Vault collection agent \$ORACLE_HOME/av/log directory.

4. Because debugging creates more logging and writing overhead, remember to disable it when you no longer need it.

- **For Release 10.2.3.2 agents:** Run these commands:

```
avctl stop_agent
avctl start_agent -loglevel info
```

- **For Release 10.2.3.1 or earlier agents that have not been upgraded:** Run these commands:

```
avctl stop_oc4j
avctl start_oc4j -loglevel info
```

A.3.3.3 The Agent OC4J or Audit Vault Console OC4J Failing to Start

Problem: After you run the `avctlstart_oc4j` command, an `avctl show_oc4j_status` command shows that OC4J is not running. Or, after you issue `avctl start_av` command, an `avctl show_av_status` command shows that OC4J is not running.

Solution: Go to \$ORACLE_HOME/av/log/agent.err log file and check the error message that appears in the log.

Or, go to \$ORACLE_HOME/oc4j/j2ee/home and issue the following command to find the error message that appears on the console:

```
java -jar oc4j.jar
```

This problem is most likely caused by a port conflict. For example, if the problem is caused by an RMI port conflict, you would see a message similar to the following:

```
C:\oracle\product\10.2.3\avagentrc3_01\oc4j\j2ee\home>java -jar oc4j.jar
```

```
09/05/16 10:39:51 Error starting ORMI-Server. Unable to bind socket: Address
already in use: JVM_Bind
```

The RMI, JMS, and HTTP ports are necessary for starting OC4J or the Audit Vault Console OC4J. The agent OC4J and Audit Vault Console OC4J can fail to start or the agent service of the Audit Vault Console can become unavailable if these ports have a conflict. If there is a port conflict, see [Section 4.9](#) for information about changing the Oracle Audit Vault port number. See also [Section 1.3.4.3](#) for the default collection agent port numbers.

A.3.3.4 Failed Source Database Connection Due to Invalid Wallet Credentials

Problem: The `setup` command for the AVORCLDB, AVMSQLDB, AVSYBDB, or AVDB2DB command-line utility returns an error message saying that the connection to the source database using the credentials in the wallet was not successful. This problem is most likely due to your entering an incorrect user name or password or both when you issued the `setup` command.

Solution: Reissue the `setup` command again using the correct credentials. See the following sections:

- [Section 8.9](#) for Oracle databases
- [Section 9.9](#) for SQL Server databases
- [Section 10.9](#) for Sybase ASE databases
- **IBM DB2 databases:** The `avdb2db` utility has no `setup` command. For IBM DB2 databases, you only need to change the password of the designated user account.

A.3.4 Troubleshooting the Audit Vault Collectors

This section contains:

- [ORA-01031 Error When You Try to Create a an Oracle Database Collector](#)
- [Oracle Source Database DBAUD Log Errors When Starting DBAUD Collector](#)
- [DBAUD Collector Does Not Start and the Listener Is Not Available](#)
- [Not Sure if the DBAUD and OSAUD Collectors Are Working](#)
- [ORA-01017 Error When You Try to Start the DBAUD or REDO Collectors](#)
- [MSSQLDB, SYBDB, or DB2 Collector Log Indicates Jar File Is Missing](#)
- [Collector Unable to Connect to the Source Database](#)
- [Failure of the Computer on Which a Collector Resides](#)
- [DB2 Collector Connection Being Denied Due to Lack of License](#)

A.3.4.1 ORA-01031 Error When You Try to Create a an Oracle Database Collector

Problem: You are able to add a collector, but the following error appears in the `avorcldb add_collector` command output:

```
ERROR: java.sql.SQLException: ORA-01031: insufficient privileges
```

Afterward, the collector is added, but it fails to collect any audit data.

Solution: The source database user account that you used to create the collector may not have the correct privileges. To remedy this problem:

1. Run the `zarsspriv.sql` script for the source database user account, as described in [Section 2.3.1](#).
2. Restart the collector, as described in [Section 2.8](#).

Another problem can be the compatibility between versions of the Audit Vault Server and source database. See *Oracle Audit Vault Installation Guide* for your platform for the requirements.

A.3.4.2 Oracle Source Database DBAUD Log Errors When Starting DBAUD Collector

Problem: For Oracle source databases that use the DBAUD collector, errors similar to the following may appear in the DBAUD log file when the collectors before the collectors have started:

```
INFO @ '12/08/2009 06:50:01 02:00':
Could not call Listener, NS error 12541, 12560, 511, 2, 0
INFO @ '12/08/2009 06:50:03 02:00':
Could not call Listener, NS error 12541, 12560, 511, 2, 0
INFO @ '12/08/2009 06:51:03 02:00':
Could not call Listener, NS error 12541, 12560, 511, 2, 0
INFO @ '12/08/2009 06:51:11 02:00':
Could not call Listener, NS error 12541, 12560, 511, 2, 0
INFO @ '12/08/2009 06:51:11 02:00':

        ***** Started logging for 'AUD$ Audit Collector' *****

INFO @ '12/08/2009 06:51:11 02:00':
        ***** Collector Name = DBAUD_Collector

INFO @ '12/08/2009 06:51:11 02:00':
        ***** Source Name = HUKSA.EXAMPLE.COM

INFO @ '12/08/2009 06:51:11 02:00':
        ***** Av Name = AV

INFO @ '12/08/2009 06:51:11 02:00':
        ***** Initialization done OK

INFO @ '12/08/2009 06:51:11 02:00':
        ***** Starting CB

INFO @ '12/08/2009 06:51:13 02:00':
Getting parameter |AUDAUDIT_DELAY_TIME|, got |20|

INFO @ '12/08/2009 06:51:13 02:00':
Getting parameter |AUDAUDIT_SLEEP_TIME|, got |5000|

INFO @ '12/08/2009 06:51:13 02:00':
Getting parameter |AUDAUDIT_ACTIVE_SLEEP_TIME|, got |1000|

INFO @ '12/08/2009 06:51:13 02:00':
Getting parameter |AUDAUDIT_MAX_PROCESS_RECORDS|, got |1000|

INFO @ '12/08/2009 06:51:13 02:00':
        ***** CSDK initied OK + 1

INFO @ '12/08/2009 06:51:13 02:00':
        ***** Src alias = SRCDB1

INFO @ '12/08/2009 06:51:13 02:00':
        ***** SRC connected OK

INFO @ '12/08/2009 06:51:13 02:00':
        ***** SRC data retrieved OK

INFO @ '12/08/2009 06:51:13 02:00':
        ***** Recovery done OK
```

Solution: You can disregard these error messages. To check that the collector has truly started, you can run the `avctl show_collector_status` command. See [Section 7.6](#).

A.3.4.3 DBAUD Collector Does Not Start and the Listener Is Not Available

Problem: You cannot start the DBAUD collector for an Oracle source database, and the listener is not available. The DBAUD collector log file (in the Audit Vault collection agent home directory) shows the following entry:

```
INFO @ '17/08/2009 15:05:48 02:00':
Could not call Listener, NS error 12541, 12560, 511, 2, 0
```

Solution:

Ensure that you completed the last step for configuring the source database and collectors, as described in [Section 2.3.5](#), which describes how to run the `avorcldb setup` command in the Audit Vault collection agent home. See also [Section 2.2.3](#) and [Section 2.2.4](#).

Follow these steps:

1. Change directories to the `network/admin` directory:

```
cd $ORACLE_HOME/network/admin
```

2. Perform the `cat` command on your `tnsnames.ora` file.

There should be an entry similar to `SRCDDB1`. If there is no `SRCDDB1` entry in your `tnsnames.ora` file, then run the `avorcldb setup` command as shown in [Section 2.3.5](#).

3. Try to connect to the source database with the following command, assuming your `tnsnames.ora` file has an `SRCDDB2` entry.

For example:

```
sqlplus /@SRCDDB1
```

If the connection is successful, then your source database is set up correctly.

4. Try starting the DBAUD collector using the `avctl start_collector` command.

For example:

```
avctl start_collector -collname REDO_Collector -srcname ORCLSRC1.EXAMPLE.COM
```

See [Section 7.11](#) for more information about the `avctl start_collector` command.

A.3.4.4 Not Sure if the DBAUD and OSAUD Collectors Are Working

Problem: You are not sure if the DBAUD collector is collecting from the `SYS.AUD$` table and the OSAUD collector is collecting from the operating system audit file.

Solution: To determine if the DBAUD collector is collecting from the `AUD$` table, check the contents of the DBAUD log file, located in the `$ORACLE_HOME/av/log` directory.

To determine if the OSAUD collector is collecting from the OS file, check the contents of the `osaud_collector-name_source-name_source-id.log` file in the Audit Vault collection agent- home `$ORACLE_HOME/av/log` directory.

Check each file for entries that indicate that the collector is collecting audit records.

For example, the DBAUD collector log file would have entries similar to the following:

```
***** Started logging for 'AUD$ Audit Collector' *****
.
.
.
INFO @ '25/10/2008 19:08:42 -8:00':
***** SRC connected OK

INFO @ '25/10/2008 19:08:53 -8:00':
***** SRC data retrieved OK
.
.
.
```

The OSAUD collector log file could have an entry as follows:

```
File opened for logging source "DBS1.REGRESS.RDBMS.DEV.US.ORACLE.COM"
INFO @ '24/10/2008 18:16:18 -8:00':
***** Started logging for 'OS Audit Collector' *****
```

Log in to the Audit Vault Console as the Audit Vault auditor. 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.

A.3.4.5 ORA-01017 Error When You Try to Start the DBAUD or REDO Collectors

Problem: When you try to start the DBAUD collector or configure the REDO collector, the following error message appears:

```
ORA-01017: invalid username/password; logon denied
```

Solution: Ensure that the host that you specified for the `-av` argument of the `avorcldb add_collector` command is correct. You can confirm the host name by checking the `tnsnames.ora` file for the source database.

Alternatively, there may be a problem with your user name or password in the password file, or a problem with the wallet credentials. Try re-creating the user name and password. If the problem persists, re-create the password file. If this does not correct the problem, then add the source user to the wallet again using the `avorcldb setup` command. Ensure that this user is the same user name and password that you are using on the source database.

A.3.4.6 MSSQLDB, SYBDB, or DB2 Collector Log Indicates Jar File Is Missing

Problem: The collector log for the MSSQLDB, SYBDB, or DB2 collector indicates that a jar file is missing. If the following JDBC driver jar files are missing from the Audit Vault collection agent `$ORACLE_HOME/jlib` library, then this error message appears in the collector log of the respective collector being used.

- **SQL Server:** `sqljdbc.jar`
- **Sybase ASE:** `jconn3.jar`
- **IBM DB2:** `db2jcc.jar`

Under other circumstances, such as when you use either the AVMSQLDB, AVSYBDB, or AVDB2DB command-line utilities, the following error appears when the JDBC driver is not in this directory:

JDBC Driver is missing. Please make sure that the JDBC jar exists in the location specified in Audit Vault documentation.

Solution: See the following sections:

- **SQL Server:** [Section 2.4.1](#) for information about the `sqljdbc.jar` file
- **Sybase ASE:** [Section 2.5.1](#) for information about the `jconn3.jar` file
- **IBM DB2:** [Section 2.6.1](#) for information about the `db2jcc.jar` file

After you download and copy these JDBC drivers in place, restart the collection agent. See [Section 7.12](#) and [Section 7.9](#) for more information about stopping and starting the agent for Release 10.2.32 agents. For agents that were created in Release 10.2.3.1 or earlier, restart OC4J by running the `avctl stop_oc4j` and `avctl start_oc4j` commands.

A.3.4.7 Collector Unable to Connect to the Source Database

Problem: When you try to verify the ORCLDB, MSSQLDB, SYBDB, or DB2 collector using the `verify` command, the following error message appears:

Unable to connect to source database

Solution: This error appears if the source user that you specified in the `verify` command for the source database does not have sufficient privileges to connect to the source database. Check if the source user has sufficient privileges to connect to the respective database. See the following sections for information about creating a source user with sufficient privileges:

- [Section 2.3.1](#) for Oracle databases
- [Section 2.4.2](#) for Microsoft SQL Server databases
- [Section 2.5.2](#) for Sybase ASE databases
- [Section 2.6.2](#) for IBM DB2 databases

A.3.4.8 Failure of the Computer on Which a Collector Resides

Problem: The computer on which you have created a collector fails.

Solution: For collectors that retrieve audit data from the database (and not operating system files), you can collect audit trails from another host computer by moving the collector to a different computer. To do so, see the following sections:

- [Section 8.4](#), for the `avorcldb alter_collector` command; applies to the DBAUD collector only
- [Section 9.4](#), for the `avmssqldb alter_collector` command; applies to the server-side trace logs only
- [Section 10.4](#), for the `avsybdb alter_collector` command

A.3.4.9 DB2 Collector Connection Being Denied Due to Lack of License

Problem: When you run the `avdb2db verify` command or perform other DB2 collector-related functions, the log file may report that the connection was denied because the license is missing. This can result from having the wrong version of the

IBM Data Server Driver for JDBC and SQLJ installed. You must have version 3.50 or later.

Solution: Check the version of the IBM Data Server Driver for JDBC and SQLJ driver, and if necessary, upgrade it.

To check the version of this driver, run the following command on the `db2jcc.jar` file:

```
java -cp jar_file_directory_path/db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version
```

If the version of the driver is earlier than version 3.50, then follow the instructions in [Section 2.6.1](#) to upgrade to the correct version.

A.3.5 Troubleshooting Oracle Audit Vault Console

This section contains:

- [Audit Vault Console Not Appearing in the Web Browser](#)
- [Audit Vault Console Problem Requiring Debugging](#)
- [Oracle RAC Node Containing the Audit Vault Console Becomes Disabled](#)

A.3.5.1 Audit Vault Console Not Appearing in the Web Browser

Problem: When you try to access 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 the Audit Vault Console is down. To check the status of the Audit Vault Console, issue an `avctl show_av_status` command in the Audit Vault Server shell or command prompt. If the status indicates that the Audit Vault Console is down, issue the `avctl start_av` command in the Audit Vault Server shell or command prompt to restart it. Then start the Audit Vault Console in the Web browser. The Audit Vault Console should appear and let you log in to the management system of the Audit Vault auditor administrator.

A.3.5.2 Audit Vault Console Problem Requiring Debugging

Problem: You want to enable debug logging while trying to diagnose an Audit Vault Console problem.

Solution: Run the following commands on the command-line:

```
avctl stop_av
avctl start_av -loglevel debug
```

Then check the log output in the Audit Vault Server `$ORACLE_HOME/av/log` directory.

Because debugging creates more logging and writing overhead, remember to disable it when you no longer need it, as follows:

```
avctl stop_av
avctl start_av
```

See [Section 7.10](#) and [Section 7.13](#) for more information about these commands.

A.3.5.3 Oracle RAC Node Containing the Audit Vault Console Becomes Disabled

Problem: In an Oracle RAC environment, the node on which the Audit Vault Console is installed becomes disabled. When this node becomes unavailable, the Console does

not automatically fail over to another node as the repository database does. As a result, the Audit Vault Console application is no longer available to users.

Solution: You must manually bring up the Audit Vault Console on another node in the Oracle RAC cluster. See [Section 4.6](#) for more information.

A.3.6 Troubleshooting the Oracle Audit Vault Audit Reports

This section contains:

- [Oracle Audit Vault Reports Not Displaying](#)
- [Oracle Audit Vault Reports Not Showing Any Data](#)
- [Not Sure if Audit Data Is Appearing in the Data Warehouse](#)
- [Advanced Alerts Unable to Fire and New Alerts Cannot Be Created](#)

A.3.6.1 Oracle Audit Vault Reports Not Displaying

Problem: When you select the **Reports** tab in the Audit Vault Console, an error message appears saying that the report cannot be displayed.

This problem can occur in the following situations:

- **The Oracle Audit Vault installation may not have completed successfully.** Check the Audit Vault Server installation log files, which are located in the \$ORACLE_HOME/av/log directory. See ["Location of Audit Vault Server Log and Error Files"](#) on page A-1 for more information.
- **The database cannot register the Oracle listener XDB HTTP endpoint.** Check the Audit Vault Server database listener status:

```
lsnrctl status
```

The output should contain the following line of text:

```
... (PORT=5707 ) (Presentation=HTTP) (Session=RAW)
```

If it does not, then follow these steps:

1. Log in to SQL*Plus as the XDB user or a user who has been granted the EXECUTE privilege for the DBMS_XDB PL/SQL package.

```
sqlplus xdb_admin
Enter password: password
```

2. Run the following procedure:

```
SQL> EXEC DBMS_XDB.SETHTTPPORT(5707);
```

3. Connect as user SYS with the SYSDBA privilege, and then run the following ALTER SYSTEM statement:

```
SQL> ALTER SYSTEM REGISTER;
```

Alternatively, follow these steps:

1. Disable Oracle Database Vault.

See *Oracle Database Vault Administrator's Guide* for instructions on disabling (and re-enabling) Oracle Database Vault.

2. Log in to SQL*Plus as user SYS with the SYSDBA privilege, and then run the following SQL statements:

```
SQL> EXEC DBMS_XDB.SETHTTPPORT(5707);
SQL> ALTER SYSTEM REGISTER;
```

3. Re-enable Oracle Database Vault.

A.3.6.2 Oracle Audit Vault Reports Not Showing Any Data

Problem: When you generate a report, the Oracle Audit Vault reports are not showing any data, even in cases where the audit trail data can be retrieved from source database.

Solution: A report filter may be incorrectly set, or the collection agent or collectors may not be running. Try the following solutions:

- **Check the filters for the report.** For example, the report may have been enabled to show only events that occurred in the last 24 hours. Disable this filter and then check that the warehouse data is being refreshed. See *Oracle Audit Vault Auditor's Guide* for more information.
- **If the audit trail data cannot be retrieved, ensure that the collectors are enabled.** See [Section 2.7](#) and [Section 2.8](#) for more information.

A.3.6.3 Not Sure if Audit Data Is Appearing in the Data Warehouse

Problem: Even though the Oracle Audit Vault data warehouse is refreshed automatically with audit data, you are not sure if the data warehouse is capturing this data.

Solution: If you believe that the audit data is not being updated in the data warehouse, then check the Activity Overview Report, described in *Oracle Audit Vault Auditor's Guide*. If you find that data is missing, then check the server-side log files (alert and trace logs, located in the \$ORACLE_HOME/av/log directory) for errors. If there are errors, then contact Oracle Support.

A.3.6.4 Advanced Alerts Unable to Fire and New Alerts Cannot Be Created

Problem: An advanced alert that uses a user-defined function is no longer able to be fired. Furthermore, you find that you cannot add any new alerts for the affected Audit Vault alert rule set, which is comprised of the category and source database type. For example, you would no longer be able to create or use alerts for the Account Management category of the Oracle Database source type. In fact, none of the alerts for the affected rule set may work. This problem can occur if the function has been changed or dropped, or the privileges for running the function have been changed. As a result, the alert is no longer valid.

Solution: Check that the function has not been modified or its privileges changed. Ensure that the AVREPORTUSER account has been granted the EXECUTE privilege for the function. Then recreate the alert to use the corrected function. Afterward, the alert and other alerts in the rule set should work correctly.

A.3.7 Troubleshooting Oracle Audit Vault in an Oracle Real Application Clusters Environment

This section contains:

- [avca drop_agent Command Failing](#)

A.3.7.1 avca drop_agent Command Failing

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 run the `avca add_agent` command from one of the Oracle RAC nodes, the command fails.

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

To find where the `av.ear` file is deployed, locate the `$ORACLE_HOME/oc4j/j2ee/oc4j_applications/applications/av/av/WEB-INF/classes/av.properties` file is located.

Once you locate the node, run the 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. See [Section 6.6](#) for more information about this command.

When you run the `avca deploy_av` command, on the other node Oracle Database creates a wallet containing the default `avadmin` entries. You must add the other entries, such as the source user credentials, to the wallet by using the `setup` command for the appropriate utility (`AVORCLDB`, `AVMSSQLDB`, `AVSYBDB`, or `AVDB2DB`), depending on the collectors being used.

To access the Audit Vault Console from this other node, enter the following URL in the Web browser:

```
http://host:port/av
```

In this specification:

- *host* is the host name or IP address of the other Oracle RAC node
- *port* is the port number for the Oracle RAC node

Oracle Audit Vault Error Messages

The following sections describe the Oracle Audit Vault error messages:

- [Audit Vault Server Error Messages](#)
- [Oracle Audit Vault Client Error Messages](#)

B.1 Audit Vault Server Error Messages

This section describes the following Audit Vault Server-side error message codes:

- [Generic Error Codes](#)
- [Source Database and Event Error Codes](#)
- [Collector Error Codes](#)
- [Attribute Definition Error Codes](#)
- [Alert Error Codes](#)
- [Server-Side Audit Service Error Messages](#)
- [Data Warehouse Error Messages](#)
- [Other Audit Vault Policy Error Messages](#)

B.1.1 Generic Error Codes

This section describes the generic error codes. Code numbers 46500 to 45599 are reserved for these 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. Remember that even if you drop an object from Oracle Audit Vault, such as an agent or a source database, the name of the dropped object is stored internally.

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, object attribute %s exists in %s

Cause: Attribute specified was already present.

Action: Provide a different value.

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.

46509, offset "%s" is incorrectly formatted"

Cause: The specified offset value is not in the format +/-hh:mm.

Action: Specify the offset in the correct format: +/-hh:mm. See [Section 6.23](#) for more information.

B.1.2 Source Database and Event Error Codes

This section describes the source database and event error codes. Code numbers 46521 to 46540 are reserved for these 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 database specified had collectors which were active.

Action: Drop active collectors for the given source database. Run the `drop_collector` command of the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source database type.

46525, Sourcetype-specific extension for Category already exists

Cause: Event category was specified which already has a format extension for the given source database type.

Action: Provide an event category that does not have a source database type-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: Source type specified had active source databases.

Action: Drop the active source databases before dropping this source type. Run the `drop_source` command of the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source database type.

46531, unsupported Source version

Cause: Version specified for the source database was not supported.

Action: Provide a source database version that is equal to or greater than the minimum supported version for the corresponding source database type. See [Section 1.3.1](#) for a listing of supported database versions.

B.1.3 Collector Error Codes

This section describes the collector error codes. Code numbers 46541 to 46550 are reserved for these 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. Run the `drop_collector` command of the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source database type.

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. Run the `avctl stop_agent` command to stop disable the collector, then the `drop_collector` command of the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source database type.

B.1.4 Attribute Definition Error Codes

This section describes the attribute definition error codes. Code numbers 46551 to 46560 are reserved for these 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.

B.1.5 Alert Error Codes

This section describes the alert error codes. Code numbers 46561 to 46599 are reserved for these error codes.

46561, no Format defined for the Source Type and Category

Cause: Format for the specified source database type and category pair was not present in the system.

Action: Provide source database 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. See *Oracle Audit Vault Auditor's Guide* for more information about configuring alert conditions.

46563, attempting to drop a nonuser-defined Alert

Cause: Nonuser-defined alert was specified.

Action: Provide a user-defined alert. See *Oracle Audit Vault Auditor's Guide* for more information about configuring alert conditions.

46581, notification profile \"%s\" already exists

Cause: Notification profile already exists.

Action: Create the notification profile with another name.

46582, cannot delete notification profile \"%s\" as it is being used in alert definitions

Cause: Notification profile is being used in alert definitions.

Action: Change the alert definition to use a different notification profile name before deleting this one.

46583, notification profile \"%s\" does not exist

Cause: Notification profile does not exist.

Action: Specify a valid notification profile name.

46584, \"%s\" is not a well-formed e-mail address list

Cause: The specified e-mail address list was not well formed.

Action: Specify a well-formed e-mail address list. For example:

`ima.kuksa@example.com,auditors@example.com`

46585, notification template \"%s\" already exists

Cause: Notification template already exists.

Action: Create the notification template with another name.

46586, \"%s\" is not a well-formed e-mail address

Cause: The specified e-mail address was not well formed.

Action: Specify a well-formed e-mail address. For example:

`ida.neau@example.com`

46587, remedy %s trouble ticket template \"%s\" already exists

Cause: Trouble ticket template already exists.

Action: Create the template with another name.

46588, %s is not one of %s values

Cause: The specified value is not in the list of values expected for this entity.

Action: Choose a different value from the list of values.

46589, Warning level Alert and Critical level Alert cannot be mapped to the same Remedy Urgency level

Cause: Warning alert and critical alert is mapped to the same remedy urgency level.

Action: Map them to different remedy urgency levels.

46599, Internal error %s %s %s %s %s

Cause: Internal error occurred in Oracle Audit Vault.

Action: Contact Oracle Support Services

B.1.6 Server-Side Audit Service Error Messages

This section describes the server-side audit service error codes. Code numbers 46600 to 46619 are reserved for these 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 properties of the source database.

46602, Error on audit record insert as RADS partition full

Cause: RADS partition table is full.

Action: Purge the RADS partition table through archive. See [Section 4.11](#) for information about purging the Oracle Audit Vault repository.

46603, Error on audit record insert as RADS_INVALID table full

Cause: RADS_INVALID table is full.

Action: Purge the RADS_INVALID table or make its size larger.

46604, Error on insert as Error table full

Cause: Error table is full.

Action: Purge the error table. See [Section 4.11](#) for information about purging the Oracle Audit Vault repository.

46605, There are more recovery entries than the maximum member can be returned

Cause: There are more recovery entries for this collector.

Action: Purge the old entries from the recovery table. See [Section 4.11](#) for information about purging the Oracle Audit Vault repository.

46606, There is no recovery entry for the given name

Cause: There was no recovery context matching to the given name.

Action: 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: Reduce the configuration entries for this collector. Use the `alter_collector` command of the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source collector.

B.1.7 Data Warehouse Error Messages

This section describes messages from the data warehouse. Code numbers 46620 to 46639 are reserved for these error codes.

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. See [Section 3.4.2](#).

46621, invalid start date %s for data warehouse operation; must be less than %s

Cause: Invalid start date was specified for data warehouse load or purge operation.

Action: Specify valid start date. The start date must be less than current date for the warehouse duration. See [Section 3.4.3](#) or [Section 3.4.4](#).

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 or purge operation.

Action: Specify valid number of days. The number of days must be positive. See [Section 3.4.3](#) or [Section 3.4.4](#)

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.

46626, Invalid number of years %s for audit data retention; must be positive

Cause: Invalid number of years was specified for audit data retention

Action: Specify valid number, the number should be positive. See [Section 3.4.2](#).

B.1.8 Other Audit Vault Policy Error Messages

This section describes Oracle Audit Vault policy error messages. Code numbers 46640 to 46699 are reserved for these error codes.

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.

B.2 Oracle Audit Vault Client Error Messages

This section describes the following Oracle Audit Vault client error messages:

- [General Error Messages](#)
- [CSDK Error Messages](#)
- [Command-Line Interface Error Messages](#)
- [OSAUD Collector Error Messages](#)
- [DBAUD Collector Error Messages](#)

B.2.1 General Error Messages

This section describes the general Oracle Audit Vault client error messages. Code numbers 46800 to 46819 are reserved for these error codes.

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.

B.2.2 CSDK Error Messages

This section describes the CSDK error messages. Code numbers 46820 to 46839 are reserved for these error codes.

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 the Oracle Audit Vault tables.

Action: Configure the collector properly.

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: Oracle Call Interface (OCI) layer returned error.

Action: Contact collector owner.

46829, category %s unknown

Cause: Collector attempted to pass category not configured in Oracle Audit Vault.

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), additional information %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: Event ID attributes of audit record are missing.

Action: Contact collector owner.

46838, Internal Error: Failed to insert %s into %s hash table

Cause: Core hash table insertion function failed.

Action: Contact collector owner.

B.2.3 Command-Line Interface Error Messages

This section describes the command-line error messages. Code numbers 46840 to 46899 are reserved for these error codes.

46840, no smtp server registered

Cause: SMTP server is not registered.

Action: Register SMTP server using the `avca register_smtp` command.

46841, smtp server already registered

Cause: SMTP server is already registered.

Action: Unregister the SMTP server using the `avca register_smtp -remove`. Alternatively, use `avca alter_smtp` to update the SMTP parameters.

46842, %s command requires the %s parameter

Cause: A required parameter is missing

Action: Provide all the required parameters for the command.

46843, invalid value \"%s\" specified for parameter %s

Cause: A parameter was specified using an invalid or incorrect value.

Action: Provide correct values for the indicated parameter.

46844, no value specified for \"%s\" in parameter %s

Cause: No value was specified for a sub-parameter in a main parameter.

Action: Provide correct values for the indicated parameter.

46845, input value \"%s\" exceeds maximum allowed length of %s

Cause: Input value exceeds the maximum allowed length.

Action: Input a value within the allowed length limits.

46846, input value \"%s\" in parameter %s is not a number

Cause: Input value for port number must be a numeric value.

Action: Input a numeric value for the port number.

46847, input value \"%s\" for parameter %s is not a valid email address

Cause: Input value does not seem to be a valid e-mail address.

Action: Input a valid e-mail address of the form `user@domain`.

46848, smtp server is already in secure mode using protocol \"%s\"

Cause: The specified SMTP server configuration is already secure using the protocol specified.

Action: Use `avca alter_smtp` to change the protocol settings.

46849, smtp server is not configured to use a secure protocol

Cause: The specified SMTP server is not configured to use a secure protocol

Action: Use `avca secure_smtp` to specify a secure SMTP protocol first.

46850, file \"%s\" does not exist

Cause: The specified file does not exist.

Action: Specify a valid file.

46851, smtp integration is already enabled

Cause: The SMTP configuration registered with Audit Vault is already in enabled state.

Action: None.

46852, smtp integration is already disabled

Cause: The SMTP configuration registered with Audit Vault is already in disabled state.

Action: None.

46853, parameters \"%s\" and \"%s\" cannot be specified together

Cause: The user specified two mutually exclusive parameters.

Action: Provide one of the two parameters.

46854, unsupported remedy version: \"%s\"

Cause: The user specified an unsupported Remedy version.

Action: Specify 6 or 7 for Remedy version.

46855, remedy server already registered

Cause: Remedy server is already registered.

Action: Unregister the Remedy server by using `avca register_remedy -remove` first or use `avca alter_remedy` to update Remedy parameters.

46856, no remedy server registered

Cause: Remedy server is not registered.

Action: Register the Remedy server using `avca register_remedy` first.

46857, remedy integration is already enabled

Cause: The Remedy configuration registered with Audit Vault is already in enabled state.

Action: None.

46858, remedy integration is already disabled

Cause: The Remedy configuration registered with Audit Vault is already in disabled state.

Action: None.

46859, remedy server is already in secure mode using protocol \"%s\"

Cause: The specified Remedy server configuration is already secure using the protocol specified.

Action: None.

46860, remedy server is not configured to use a secure protocol

Cause: The specified Remedy server is not configured to use a secure protocol.

Action: Use `avca secure_remedy` to specify a secure Remedy protocol first.

46861, specified ticket id \"%s\" does not exist in the remedy server database

Cause: Specified ticket does not exist in the Remedy Server.

Action: Provide a ticket ID which exists in the Remedy Server.

B.2.4 OSAUD Collector Error Messages

This section describes the OSAUD collector error messages. Code numbers 46900 to 46939 are reserved for these error codes.

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: 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: Consult the log file for detailed operating system error. See [Section A.1](#) or [Section A.2](#).

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 the `add_collector` for the `avorcldb`, `avmssqldb`, `avsybdb`, or `avdb2db` utility, depending on the source database used.

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], Error code[%u]

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 the `avctl start_collector` command.

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.

46923, OCI error encountered for source database %s access, audit trail cleanup support disabled.

Cause: An error was encountered while attempting to connect to or execute SQL statements on the source database.

Action: Verify source database and listener are up and connect information is correct.

46924, Corrupted recovery information detected for collector %s for source %s

Cause: Corrupted recovery information detected.

Action: Contact Oracle Support Services.

46925, error in parsing XML file %s for collector %s and source database %s : error code %u.

Cause: An internal error occurred while parsing data for collector.

Action: Verify that collector has read permissions on the file and the file is in proper XML format. Contact Oracle Support Services for patch set.

46926, error in recovery of XML file %s for collector %s and source database %s : error code %u.

Cause: An internal error has occurred while parsing data for collector.

Action: Verify that collector has read permissions on the file and the file is in proper XML format. Contact Oracle Support Services for patch set.

46927, Syslog is not configured or error in getting audit files path for syslog for collector %s and source database %s.

Cause: One of the following occurred:

- `facility.priority` was not valid.
- There was no corresponding path for `facility.priority` setting.
- Source database was only returning facility and there was no corresponding path for `facility.*` setting.

Action: Configure syslog auditing to a valid `facility.priority` setting and corresponding valid path. If source database only returning the facility, then contact Oracle Support Services for patch set.

46928, Collector %s for source %s cannot read complete file %s

Cause: File size is more than 2 GB.

Action: File size should be less than 2 GB. Use log rotation to limit the file size to less than 2 GB.

B.2.5 DBAUD Collector Error Messages

This section describes the DBAUD collector error messages. Code numbers 46940 to 46979 are reserved for these error codes.

46941, internal error, on line %d in file ZAAC.C, additional information %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: Make sure that context 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 in column %s for <%s>

Cause: The VARCHAR retrieved from AUD\$ or FGA_LOG\$ table could not 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 exceeded 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 Collector.

46949, log level

Cause: Specified log level was invalid.

Action: Use a legal log level (1,2,3).

46950, log file

Cause: An error occurred during the opening of the 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-Oracle RAC source database was incompatible with Oracle RAC recovery context.

Action: Clean up AUD\$ and FGA_LOG\$ tables and recovery context.

46958, Non-RAC recovery context

Cause: Oracle RAC source database was incompatible with non-Oracle RAC recovery context

Action: Clean up the AUD\$ and FGA_LOG\$ tables and recovery context.

46959, bad authentication information

Cause: Incorrect format of authentication information in the column COMMENT\$TEXT of the Oracle Database audit trail.

Action: Contact Oracle Support Services.

46960, bad metric request

Cause: Unknown metric name (%s) was provided in metric request.

Action: Contact Oracle Support Services.

46961, internal error, on line %d in file ZAAC.C, additional info |%s|

Cause: There was a generic internal exception for AUD\$ Audit Collector.

Action: Contact Oracle Support Services.

46962, Database Vault audit table is not accessible

Cause: Oracle Database Vault was not set up properly or the proper role was not granted to user being used by the collector.

Action: Set up Oracle Database Vault and ensure that the DVSYS.AUDIT_TRAIL\$ audit trail is accessible to the user used by collector.

46963, Some rows may have been missed by Audit Vault or may be duplicated

Cause: Collector encountered rows in the SYS.AUD\$ or FGA_LOG\$ tables with SESSIONID less than or equal to 0.

Action: Contact Oracle Support Services.

46964, Connector was not able to reconnect to Source Database

Cause: Maximum number of attempts to reconnect was exceeded.

Action: Verify connectivity and that the database is started. You can use the `lsnrctl status` command to check the status of the database.

46965, Attribute %s is longer than 4000 bytes and was clipped

Cause: When the attribute was converted to UTF8 encoding, it became longer than 4000 bytes.

Action: None. It was clipped automatically after conversion.

46966, Function AV_TRUNCATE_CLOB does not exist in source database

Cause: The latest version of script `zarsspriv.sql` was not run. This can happen if you had configured the source database using a release earlier than the latest release of Oracle Audit Vault. The agent from the earlier Oracle Audit Vault release could contain a `zarsspriv.sql` script that is not compatible with the latest installed release of Oracle Audit Vault. You can find the `zarsspriv.sql` script in the `$ORACLE_HOME/av/scripts/streams/source` directory in the Oracle Audit Vault collection agent home directory.

Action: None. Function created automatically.

46967, Audit Trail Cleanup package is not proper. Audit Trail Cleanup cannot be performed for source database.

Cause: Audit Trail Cleanup package was not properly installed.

Action: Contact Oracle Support Services.

Glossary

alert

An indicator signifying that a particular metric condition has been encountered. The following conditions trigger alerts:

- 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 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 raises an alert. An alert rule is based on the data in a single audit record.

audit data source

See [source database](#).

audit data warehouse

A data store within Oracle Audit Vault that stores processed audit data from the [raw audit data store](#). Auditors can access this data by generating the Oracle Audit Vault reports.

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 which audit events should be collected in Oracle 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, and is the audience for this manual. This user configures and manages collectors, collection 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 account granted the AV_AGENT role. This is an internal user only.

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 create alerts and evaluate alert scenarios, and manage audit settings. This user can use the data warehouse services to further review the audit data and look for trends, intrusions, anomalies, and other items of interest. See *Oracle Audit Vault Auditor's Guide* for more information about the auditor's duties.

Audit Vault Configuration Assistant (AVCA)

See [AVCA](#).

Audit Vault Control (AVCTL)

See [AVCTL](#).

Audit Vault IBM DB2 Database (AVDB2DB)

See [AVDB2DB](#).

Audit Vault Microsoft SQL Server Database (AVMSSQLDB)

See [AVMSSQLDB](#).

Audit Vault Oracle Database (AVORCLDB)

See [AVORCLDB](#).

Audit Vault Sybase ASE Database (AVSYBDB)

See [AVSYBDB](#).

AVCA

Audit Vault Configuration Assistant, a command-line utility that you use to manage various Oracle Audit Vault components, manage collection agents (adding, altering, or dropping), secure communication between the Audit Vault Server and Audit Vault collection agent, set warehouse scheduling and audit data retention settings, and create a wallet and certificates for the collection agent, as needed. See [Chapter 6, "Audit Vault Configuration Assistant \(AVCA\) Reference,"](#) for more information.

AVCTL

Audit Vault Control, a command-line utility that you use to manage the Oracle Audit Vault components, such as starting and stopping collection agents, collectors, the Audit Vault Console, and OC4J. See [Chapter 7, "Audit Vault Control \(AVCTL\) Reference,"](#) for more information.

AVDB2DB

Audit Vault IBM DB2 Database, a command-line utility that you use to configure Oracle Audit Vault to retrieve audit data from an IBM DB2 database. The process entails adding the source database and configuring the [DB2 collector](#). See [Chapter 11, "Audit Vault IBM DB2 \(AVDB2DB\) Utility Commands,"](#) for more information.

AVMSSQLDB

Audit Vault Microsoft SQL Server Database, a command-line utility that you use to configure Oracle Audit Vault to retrieve audit data from a SQL Server database. The configuration process entails adding the source database and configuring the **MSSQLDB collector**. See [Chapter 9, "Audit Vault SQL Server \(AVMSSQLDB\) Utility Commands,"](#) for more information.

AVORCLDB

Audit Vault Oracle Database, a command-line utility that you use to configure Oracle Audit Vault to retrieve audit data from an Oracle database. The configuration process entails adding the source database and configuring the appropriate collector (**DBAUD collector**, **OSAUD collector**, or **REDO collector**). See [Chapter 8, "Audit Vault Oracle Database \(AVORCLDB\) Utility Commands,"](#) for more information.

AVSYBDB

Oracle Audit Vault Sybase ASE Database, a command-line utility that you use to configure Oracle Audit Vault to retrieve audit data from a Sybase ASE database. The configuration process entails adding the source database and configuring the **SYBDB collector**. See [Chapter 10, "Audit Vault Sybase ASE \(AVSYBDB\) Utility Commands,"](#) for more information.

capture rule

A rule in an audit policy setting that specifies an audit event that is sent to Oracle Audit Vault.

certificate

A digitally signed statement by a certificate authority (CA), saying that it has certified the identity of an entity in some way. Upon request, the CA verifies the identity of the entity, and signs and grants a certificate, with a private key. This indicates that the certificate has been checked for data integrity and authenticity, where integrity means that data has not been modified or tampered with, and authenticity means that data comes from the entity claiming to have created and signed it.

A certificate is 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

collection agent

A process in which **collectors** run. A collection agent defines the connection between the collector and the audit service, and interacts with the management service to manage and monitor collectors. See [Section 1.3.4](#) for detailed information about collection agents.

collector

A component that collects audit data for a source and sends the audit records to Audit Vault. Each of the supported source database products has one or more associated collectors. See [Table 1–5](#) on page 1-8 for detailed information about the available collectors.

See also [DB2 collector](#), [DBAUD collector](#), [MSSQLDB collector](#), [OSAUD collector](#), [REDO collector](#); and [SYBDB collector](#).

composite audit setting

See [audit setting](#).

configuration data

The Oracle Audit Vault metadata (stored within Oracle Audit Vault) that describes how to process and control the audit data as it passes through the Oracle 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 the analysis workload from the transaction workload and enables a business to consolidate data from several sources. In Oracle Audit Vault, the data warehouse stores audit data that has been inserted into the data warehouse tables. From there, an Oracle Audit Vault auditor can see this data by generating the Oracle Audit Vault reports. See *Oracle Audit Vault Auditor's Guide* for more information.

See also [audit data warehouse](#) and [raw audit data store](#).

DB2 collector

IBM DB2 audit log collector. This collector extracts and collects IBM DB2 (releases 8 and 9.5) audit records from the audit trail logged in the ASCII text files generated by the source database. The DB2 collector belongs to the DB2 collector type.

DBAUD collector

Oracle Database DB audit log collector. This collector collects audit data from the Oracle Database `SYS.AUD$` table and the Oracle Database Vault audit trail `DVSYS.AUDIT_TRAIL$` table. 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: columns that contain facts and columns that are foreign keys to dimension tables. The primary key of a fact table is usually a composite key composed 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 called summary tables). A fact table usually contains facts with the same level of aggregation.

In Oracle Audit Vault, the [audit data warehouse](#) tables are in a star schema.

HTTPS

Hypertext Transmission Protocol, Secure. The use of Secure Sockets Layer (SSL) as a sublayer under the regular HTTP application layer. To configure HTTPS communication for Oracle Audit Vault, see [Section 5.6](#).

Hypertext Transmission Protocol, Secure

See [HTTPS](#).

keystore

A repository that includes the following:

- Certificates identifying trusted entities. When a keystore 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 that Oracle Audit Vault uses to generate the keystore. It enables users to self-authenticate by administering their own public and private key pairs and associated certificates or data integrity and authentication services, using digital signatures. The `keytool` utility is located at `$ORACLE_HOME/jdk/bin`.

For Oracle Audit Vault, you must run the `keytool` utility to generate a keystore file if you want to configure HTTPS communication for Audit Vault. See [Section 5.6](#) for more information.

LCR

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 database and target objects.

metric

Unit of measurement used to report the health of the system.

MSSQLDB collector

Microsoft SQL Server Database audit log collector. This collector extracts and collects Microsoft SQL Server Database (SQL Server 2000 and SQL Server 2005) (for Windows platforms) audit records from the Windows Event logs, Server-side Traces, and C2 auditing logs. The MSSQLDB collector belongs to the MSSQLDB collector type.

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 Microsoft Windows, the OS audit trail depends on the AUDIT_TRAIL parameter setting:

- If the setting is OS, the OS audit trail is the Windows Event Log.
- If the setting is XML, then the OS audit trail is the XML file.

The OSAUD collector automatically extracts and collects audit records from either audit trail.

PKI

Public key infrastructure. This information security technology uses the principles of public key cryptography to encrypt and decrypt information using a shared public and private key pair. It provides for secure, private communications within a private network.

public key infrastructure (PKI)

See [PKI](#).

raw audit data store

The first location in which Oracle Audit Vault places audit data it collects from a source database. It stores this unprocessed audit data in partitioned tables based on timestamp, and in unpartitioned tables based on source ID. Oracle Audit Vault then sends this data to the [data warehouse](#), where it is organized into tables. Auditors access this data by generating audit reports.

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.

source database

A database instance that has been configured to send audit data to Oracle Audit Vault.

The audit data source consists of databases, applications, or systems that generate audit data. For the current release of Oracle Audit Vault, the following database products are audit data sources:

- Oracle Database
- Microsoft SQL Server
- Sybase ASE
- IBM DB2

These databases can run on the same or different computers, potentially resulting in multiple source databases on the same system. Audit data from audit sources represent a variety of audit formats. Source types represent a class of audit sources. For example, Oracle Database audit sources with the same audit formats, audit events, and collection mechanisms represent an audit source type. [Table 1–5](#) on page 1-8 lists the collectors that are associated with these database products.

See also [DB2 collector](#), [DBAUD collector](#), [MSSQLDB collector](#), [OSAUD collector](#), [REDO collector](#); and [SYBDB collector](#).

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.

SYBDB collector

Sybase ASE Database audit log collector. This collector extracts and collects Sybase ASE (ASE 12.5.4 and ASE 15.0.2) audit records from the audit trail logged in audit tables in the `sybsecurity` database. The SYBDB collector belongs to the SYBDB collector type.

trust store

See [keystore](#).

X.509

A widely used standard for defining digital certificates. X.509 defines a standard certificate format for public key certificates and certificate validation.

user entitlement

The range of access that a user has to a database. User entitlement covers system and other SQL privileges, object privileges, role privileges, and user profiles that enable users to have access to the database system. In Oracle Audit Vault, you can monitor user entitlements through the default entitlement reports, which are described in *Oracle Audit Vault Auditor's Guide*.

Index

A

add_agent command (AVCA utility), 6-3

add_collector command

- IBM DB2 databases, 11-2
- Oracle databases, 8-2
- SQL Server databases, 9-2
- Sybase ASE databases, 10-2

add_source command

- IBM DB2 databases, 11-3
- Oracle databases, 8-5
- SQL Server databases, 9-3
- Sybase ASE databases, 10-3

adding

- Audit Vault collection agents, 6-3
- collectors for IBM DB2 databases, 11-2
- collectors for Oracle databases, 8-2
- collectors for SQL Server databases, 9-2
- collectors for Sybase ASE databases, 10-2

administrators

- general steps for using Oracle Audit Vault, 1-2
- main tasks, 1-1
- managing security, 5-1 to 5-20

agents

- See Audit Vault collection agents

alert processing

- about, 3-3
- managing, 3-3
- setting time zones, 6-24

alert settings

- disabling globally, 3-3
- e-mail notifications for, 3-14
- enabling globally, 3-3
- error messages, B-4
- trouble ticket notifications for, 3-16

alerts, A-16

- functions not working, A-16
- not firing, A-16

alter_collector command

- IBM DB2 databases, 11-4
- Oracle databases, 8-6
- SQL Server databases, 9-4
- Sybase ASE databases, 10-4

alter_smtp command (AVCA utility), 6-4

alter_source command

- IBM DB2 databases, 11-5

Oracle databases, 8-10

SQL Server databases, 9-8

Sybase ASE databases, 10-6

altering

- DB2DB collector attributes, 11-4
- DBAUD collector attributes, 8-6
- MSSQLDB collector attributes, 9-4
- OSAUD collector attributes, 8-6
- REDO collector attributes REDO collector
 - altering, 8-6
- source database collector attributes, 3-6 to 3-7
- SYBDB collector attributes, 10-4

archive log disk space

- monitoring in Audit Vault Server, 4-2

attributes

collectors

- about, 3-6
- altering Audit Vault Console, 3-6
- altering from command line, 3-6
- source databases
 - about, 3-12
 - altering from command line, 3-13
 - altering in Audit Vault Console, 3-12

audit data

- loading to Audit Vault, 3-10
- loading to warehouse, 7-4
- purging from warehouse, 7-5
- setting a retention period, 6-25

audit events

- error codes, B-2
- viewing categories, 3-3

audit trail cleanup

- Audit Vault repository, 4-13
- IBM DB2 audit files, 2-25
- new features, xx
- Oracle source databases, 4-11
- SQL Server audit files, 2-18

Audit Vault administrator roles

AV_ADMIN

- about, 1-11
- roles and privileges granted, 5-10

AV_AGENT

- about, 1-11
- roles and privileges granted, 5-10

AV_AUDITOR

- about, 1-11

- roles and privileges granted, 5-10
- See also* Oracle Database Vault, administrator roles
- Audit Vault collection agents
 - about, 1-7
 - adding, 6-3
 - audit data collection when agent is stopped, 1-7
 - audit record collection when agents are
 - down, 2-31
 - checking status of pre-Release 10.2.3.2 collection agent, 7-14
 - checking status of Release 10.2.3.2 agents, 7-6
 - configuring connectivity for Oracle RAC nodes, 4-5
 - configuring for Oracle RAC nodes, 4-4
 - debugging advice, A-7
 - dropping, 6-10
 - errors log file
 - Audit Vault collection agent, A-3
 - Audit Vault Server, A-1
 - finding names of existing agents, 2-30
 - locations
 - for DB2DB collector, 1-16
 - for DBAUD collector, 1-12
 - for MSSQLDB collector, 1-14
 - for OSAUD collector, 1-12
 - for REDO collector, 1-12
 - for SYBDB collector, 1-15
 - log file
 - Audit Vault collection agent, A-3
 - Audit Vault Server, A-1
 - port numbers used by, 1-8
 - port numbers, changing, 4-5
 - ratio to collectors, 1-7
 - redeploying av.ear or AVAgent.ear file, 6-16
 - remote agents, affect on SYSDBA and SYSOPER
 - audit data, 1-7
 - running commands in Windows
 - environment, 2-5
 - securing, 6-20
 - starting, 7-9
 - status blank on Windows Services Panel, A-7
 - stopping, 7-17
 - troubleshooting tips, A-7 to A-9
 - UNIX environment variable settings, 2-4
 - using on Windows, 2-5
 - wallet credentials not successful, A-9
- Audit Vault collectors
 - about, 1-7
 - adding for DB2, 11-2
 - adding for Oracle database, 8-2
 - adding for SQL Server, 9-2
 - adding to Sybase ASE, 10-2
 - adding, general steps, 2-1
 - attributes
 - about, 3-6
 - altering in Audit Vault Console, 3-6
 - altering in shell, 3-6
 - DB2DB collector, 11-4
 - DBAUD collector, 8-6, 8-7
 - MSSQLDB collector, 9-4
 - OSAUD collector, 8-6, 8-8
 - REDO collector, 8-9
 - SYBDB collector, 10-4
 - checking status of, 2-31, 7-7
 - collector not starting, 7-12
 - DB2DB collector
 - location of agent, 1-16
 - DBAUD
 - moving to different agent, 8-7
 - DBAUD collector
 - location of agent, 1-12
 - dropping
 - from IBM DB2, 11-6
 - from Oracle databases, 8-11
 - from SQL Server databases, 9-9
 - from Sybase ASE databases, 10-7
 - host computer failure, A-13
 - moving collector to a different agent
 - DBAUD, 8-7
 - example for DBAUD, 8-9
 - example for SQL Server, 9-7
 - example for Sybase ASE, 10-5
 - SQL Server collector, 9-6
 - Sybase collector, 10-5
 - MSSQLDB collector
 - location of agent, 1-14
 - new features, xxi
 - OSAUD collector
 - location of agent, 1-12
 - ratio to collection agents, 1-7
 - REDO collector
 - location of agent, 1-12
 - starting, 7-11
 - stopping, 7-13
 - SYBDB
 - moving to different agent, 9-6, 10-5
 - SYBDB collector
 - location of agent, 1-15
 - timestamps for purge process, 4-12
 - troubleshooting tips, A-11 to A-13
- Audit Vault Configuration Assistant (AVCA) utility
 - commands
 - add_agent command, 6-3
 - alter_smtp command, 6-4
 - create_credential command, 6-6
 - create_wallet command, 6-7
 - deploy_av command, 6-7
 - disable_remedy command, 6-9
 - disable_smtp command, 6-9
 - drop_agent command, 6-10
 - enable_remedy command, 6-10
 - enable_smtp command, 6-11
 - generate_csr command, 6-12
 - help command, 6-13
 - import_cert command, 6-15
 - redeploy command, 6-16
 - register_remedy command, 6-17
 - register_smtp command, 6-18
 - remove_cert command, 6-19
 - secure_agent command, 6-20

- secure_av command, 6-21
- secure_remedy command, 6-23
- secure_smtp command, 6-23
- set_server_tz command, 6-24
- set_warehouse_retention command, 6-25
- set_warehouse_schedule command (deprecated), 0-xx
- show_remedy_config command, 6-26
- show_server_tz command, 6-27
- show_smtp_config command, 6-27
- table of, 6-1
- test_remedy command, 6-28
- test_smtp command, 6-29
- log file
 - Audit Vault collection agent, A-3
 - Audit Vault Server, A-1
- new features, xxii
- Audit Vault Console
 - checking status, 3-2
 - checking status of, 7-7
 - debugging advice, A-14
 - deploying in an Oracle RAC environment, 4-3
 - logging in, 3-2
 - starting, 3-2
 - stopping, 3-3
 - troubleshooting tips, A-14
 - viewing
 - Audit Vault errors, 3-5
 - Web browser hanging, A-14
- Audit Vault Control (AVCTL) utility
 - commands
 - help command, 7-2
 - load_warehouse command, 7-4
 - purge_warehouse command, 7-5
 - refresh_warehouse command (deprecated), 0-xx
 - show_agent_status command, 7-6
 - show_av_status command, 7-7
 - show_collector_status command, 2-31, 7-7
 - show_oc4j_status command, 7-14
 - show_remedy_status command, 7-8
 - show_smtp_status command, 7-9
 - start_agent command, 7-9
 - start_av command, 7-10
 - start_collector command, 7-11
 - start_oc4j command, 7-15
 - stop_agent command, 7-12
 - stop_av command, 3-3, 7-13
 - stop_collector command, 7-13
 - stop_oc4j command, 7-17
 - table of, 7-1
 - log file
 - Audit Vault collection agent, A-3
 - Audit Vault Server, A-1
 - new features, xxii
- Audit Vault data warehouse
 - about, 3-8
 - audit data not appearing in, A-16
 - error messages, B-6
 - loading data
 - about, 3-10
 - from command line, 3-11
 - using Audit Vault Console, 3-10
 - new features, xx
 - purging data
 - about, 3-11
 - from command line, 3-12
 - using Audit Vault Console, 3-11
 - setting a retention period
 - about, 3-8
 - example, 3-8
 - setting with Audit Vault Console, 3-9
 - setting with avca set_warehouse_retention command, 3-9
 - setting data retention period, 6-25
- Audit Vault IBM DB2 (AVDB2DB) utility
 - commands
 - add_collector command, 11-2
 - add_source command, 11-3
 - alter_collector command, 11-4
 - alter_source command, 11-5
 - drop_collector command, 11-6
 - drop_source command, 11-7
 - help command, 11-8
 - table of, 11-1
 - verify command, 11-9
 - log file
 - Audit Vault collection agent, A-5
 - syntax, 11-1
 - See also* IBM DB2 databases
- Audit Vault Microsoft SQL Server Database (AVMSSQLDB) utility
 - commands
 - add_collector command, 9-2
 - add_source command, 9-3
 - alter_collector command, 9-4
 - alter_source command, 9-8
 - drop_collector command, 9-9
 - drop_source command, 9-10
 - help command, 9-10
 - setup command, 9-11
 - table of, 9-1
 - verify command, 9-12
 - log file
 - Audit Vault collection agent, A-5
 - Audit Vault Server, A-2
 - new features, xxii
 - syntax, 9-2
 - See also* Microsoft SQL Server databases
- Audit Vault Oracle Database (AVORCLDB) utility
 - commands
 - add_collector command, 8-2
 - add_source command, 8-5
 - alter_collector command, 8-6
 - alter_source command, 8-10
 - drop_collector command, 8-11
 - drop_source command, 8-12
 - help command, 8-13
 - setup command, 8-14
 - table of, 8-1

- verify command, 8-15
 - log file, A-6
 - Audit Vault collection agent, A-3
 - Audit Vault Server, A-2
 - new features, xxii
 - syntax, 8-2
 - See also* Oracle databases
- Audit Vault policies
 - internal service for, 1-5
 - location in Audit Vault Server, 1-4
 - log file, A-2
 - Oracle databases, 8-6
 - Oracle RAC, 4-5
 - script for policy management (zarsspriv.sql), 2-6
 - where created from, 1-5
- Audit Vault Server
 - about, 1-4
 - administrative tasks
 - archive log disk space, 4-2
 - backup and recovery operations, 4-2
 - changing user passwords, 5-4
 - configuring collection agent connectivity for RAC, 4-5
 - configuring collection agent to listen to RAC nodes, 4-4
 - flash recovery area, 4-2
 - SYSAUX tablespace usage, 4-1
 - alert settings, managing, 3-3
 - audit event categories, viewing, 3-3
 - Audit Vault Console status, checking, 3-2
 - checking errors, 3-5
 - components, 1-5
 - error codes
 - alert errors, B-4
 - attribute definition errors, B-4
 - collector errors, B-3
 - data warehouse errors, B-6
 - event errors, B-2
 - generic errors, B-1
 - policy errors, B-7
 - service-side audit service errors, B-5
 - performance tuning, A-6
 - port numbers used by, 1-6
 - port numbers, changing, 4-5
 - running commands in Windows
 - environment, 2-5
 - securing, 6-21
 - starting console, 7-10
 - troubleshooting tips, A-6
 - UNIX environment variable settings, 2-2
- Audit Vault Sybase ASE Database (AVSYBDB) utility
 - commands
 - add_collector command, 10-2
 - add_source command, 10-3
 - alter_collector command, 10-4
 - alter_source command, 10-6
 - drop_collector command, 10-7
 - drop_source command, 10-8
 - help command, 10-9
 - setup command, 10-10

- table of, 10-1
 - verify command, 10-11
- log file
 - Audit Vault collection agent, A-5
 - Audit Vault Server, A-2
- syntax, 10-2
- See also* Sybase ASE databases
- authentication
 - securing Audit Vault, 6-21
 - securing Audit Vault collection agent, 6-20
- AV_ADMIN role
 - about, 1-11
 - changing user password, 5-5
 - roles and privileges granted, 5-10
- AV_AGENT role
 - about, 1-11
 - changing user password, 5-6
 - roles and privileges granted, 5-10
- AV_AUDITOR role
 - about, 1-11
 - changing user password, 5-9
 - roles and privileges granted, 5-10
- AVCA_SMTPLUS environment variable, 6-5
- AVDB2DB command-line utility
 - See* Audit Vault IBM DB2 (AVDB2DB) utility
- AVMSSQLDB command-line utility
 - See* Audit Vault Microsoft SQL Server Database (AVMSSQLDB) utility
- AVORCLDB command-line utility, 8-2
 - See* Audit Vault Oracle Database (AVORCLDB) utility
- AVREPORTUSER account
 - changing password of, 5-6
- AVSYBDB command-line utility
 - See* Audit Vault Sybase ASE Database (AVSYBDB) utility

B

- back-up and recovery for Audit Vault Server, 4-2
- BMC Remedy Action Request (AR) System Server
 - See* trouble tickets

C

- certificates
 - See* Oracle wallets
- collection agents
 - See* Audit Vault collection agents
- collectors
 - See* Audit Vault collectors
- commands
 - log file, A-6
- compressed syslog files, 1-8
- coraenv UNIX script, 2-2
- create_credential command (AVCA utility), 6-6
- create_wallet command, 6-7

D

- data warehouse

- See Audit Vault data warehouse
- DB2 collector attributes, 11-4
- DB2DB collector
 - about, 1-8
 - audit trail settings for, 1-16
 - detailed information about audit trails, 1-16
 - See also IBM DB2 databases
- db2jcc.jar file, 2-22
- DBAUD collector
 - about, 1-8
 - attributes, 8-7
 - audit trail settings for, 1-13
 - detailed information about audit trails, 1-13
- DBAUD collector attributes, 8-6
- DBSNMP account
 - how Oracle Audit Vault handles, 5-11
- deploy_av command (AVCA utility), 6-7
- deprecated Oracle Audit Vault utility
 - commands, xxiii
- disable_remedy command (AVCA utility), 6-9
- disable_smtp command (AVCA utility), 6-9
- drop_agent command (AVCA utility), 6-10
- drop_collector command
 - IBM DB2 databases, 11-6
 - Oracle databases, 8-11
 - SQL Server databases, 9-9
 - Sybase ASE databases, 10-7
- drop_source command
 - IBM DB2 databases, 11-7
 - Oracle databases, 8-12
 - SQL Server databases, 9-10
 - Sybase ASE databases, 10-8
- dropping
 - Audit Vault collection agents, 6-10
 - collectors from IBM DB2 databases, 11-6
 - collectors from Oracle Database, 8-11
 - collectors from SQL Server, 9-9
 - collectors from Sybase ASE, 10-7
- DV_ACCTMGR role
 - about, 1-11
- DV_ACCTMGR roles and privileges granted
 - about, 5-10
- DV_OWNER role
 - about, 1-11
 - roles and privileges granted, 5-10

E

- e-mail notifications
 - about, 3-14
 - altering SMTP configuration, 6-4
 - configuring, 3-14 to 3-16
 - configuring for secure server, 6-23
 - configuring users for, 3-15
 - disabling SMTP configuration, 6-9
 - enabling SMTP configuration, 6-11
 - finding SMTP configuration, 6-27
 - finding SMTP status, 7-9
 - log file
 - Audit Vault Server, A-1

- registering for, 6-4
- registering SMTP service, 6-18
- testing configuration, 6-29
- unregistering SMTP service, 6-18
- enable_remedy command (AVCA utility), 6-10
- enable_smtp command (AVCA utility), 6-11
- environment variables
 - AVCA_SMTPUSR, 6-5
 - LANG, 2-3
 - LD_LIBRARY_PATH, 2-2
 - LIBPATH, 2-2
 - ORACLE_HOME, 2-2
 - ORACLE_SID, 2-2
 - PATH, 2-2
 - SHLIB_PATH, 2-2
- error and log files
 - Audit Vault collection agent
 - {collector-name}{source-name}{source-id}.log, A-3
 - agent.err, A-3
 - agent.out, A-3
 - av_client-0.log, A-3
 - avca.log, A-3
 - avorcldb.log, A-3
 - sqlnet.log, A-3
 - Audit Vault Server
 - agent.out, A-1
 - av_client-0.log, A-1
 - avca.log, A-1
 - log file location, A-1
- debugging advice for Audit Vault collection
 - agents, A-7
- debugging Audit Vault Console, A-14
- error messages, B-1 to B-16
- failed commands
 - configToolFailedCommands, A-6
- OC4J
 - AVAgent-access.log, A-6
- operational errors, 3-5
- Oracle Enterprise Manager
 - logging, A-2
- sqlnet.log, A-6
- See also troubleshooting
- examples
 - See also reference chapters for utilities

F

- failover recovery for collectors, 8-7, 9-6, 10-5
 - example for DBAUD, 8-9
 - example for SQL Server, 9-7
 - example for Sybase ASE, 10-5
- flash recovery area
 - monitoring in Audit Vault Server, 4-2

G

- generate_csr command (AVCA utility), 6-12
- granting required privileges
 - for policy management, 2-6

- to source database user
 - for the REDO collector, 2-6
- to source database user for the DBAUD collector, 2-6
- to source database user for the OSAUD collector, 2-6

H

- help command
 - AVCA utility, 6-13
 - AVCTL utility, 7-2
 - AVDB2DB utility, 11-8
 - AVMSSQLDB utility, 9-10
 - AVORCLDB utility, 8-13
 - AVSYBDB utility, 10-9
- HTTPS communication, 5-11

I

- IBM DB2 databases
 - adding collector to Oracle Audit Vault, 2-24
 - compatibility with collector, 2-23
 - converting binary audit file to ASCII text file, 2-25
 - creating user account, 2-23
 - IBM Data Server Driver for JDBC and SQLJ, 2-22
 - jar file missing, A-12
 - modifying collector attributes, 3-6 to 3-7
 - modifying source attributes, 3-12 to 3-14
 - planning configuration, 1-16
 - registering with Oracle Audit Vault, 2-22 to 2-27
 - removing from Oracle Audit Vault, 3-17 to 3-18
 - source database errors, B-2
 - unable to connect to source database, A-13
 - verifying compatibility with collector, 11-9
 - See also* Audit Vault IBM DB2 (AVDB2DB) utility
- import_cert command (AVCA), 6-15
- initialization parameters
 - hidden
 - redo log audit source release 10.1, 12-14
 - redo log audit source release 10.2, 12-6, 12-10
 - redo log audit source release 9.2, 12-18
 - redo log
 - audit source release 10.1, 12-14
 - audit source release 10.2, 12-6, 12-10
 - audit source release 11.2, 12-2
 - audit source release 9.2, 12-18
- init.ora parameters
 - See* initialization parameters

L

- LANG environment variable, 2-3
- languages supported, 2-3
- LD_LIBRARY_PATH environment variable, 2-2
- LIBPATH environment variable, 2-2
- load_warehouse command (AVCTL utility), 7-4
- log file locations and descriptions
 - Audit Vault collection agent, A-3
 - Audit Vault failed commands, A-6

- Audit Vault Server, A-1

M

- managing collection agents and collectors
 - starting
 - collection agents, pre-Release 10.2.3.2, 7-15
 - collection agents, Release 10.2.3.2, 7-9
 - collectors, 7-11
 - stopping
 - collection agents, Release 10.2.3.2, 7-12
 - collectors, 7-13
- Microsoft SQL Server databases
 - checking collector status, 2-31
 - collection agent credentials, adding, 2-17
 - collector, adding to Oracle Audit Vault, 2-16
 - compatibility with collector, 2-15
 - creating user account, 2-14
 - downloading SQL Server JDBC Driver, 2-14
 - jar file missing, A-12
 - modifying collector attributes, 3-6 to 3-7
 - modifying source attributes, 3-12 to 3-14
 - planning configuration, 1-14
 - registering with Oracle Audit Vault, 2-13 to 2-18
 - removing from Oracle Audit Vault, 3-17 to 3-18
 - setting up in collection agent home, 9-11
 - source database errors, B-2
 - trace files, preventing from being deleted by accident, 2-18
 - unable to connect to source database, A-13
 - verifying compatibility with collector, 9-12
 - See also* Audit Vault Microsoft SQL Server Database (AVMSSQLDB) utility
- Microsoft Windows
 - running commands in, 2-5
- MSSQLDB collector
 - about, 1-8
 - attributes, 9-4
 - audit trail settings for, 1-15
 - detailed information about audit trails, 1-15
 - See also* Microsoft SQL Server databases
- My Oracle Support, xvi

N

- new features in this release, xix to xxiv
- not able to be created, A-16

O

- OC4J agent
 - about, 1-5
 - checking status for, 7-14
 - checking status for Release 10.2.3.2, 7-6
 - collection agent components, 1-7
 - failing to start, A-8
 - how it fits in general process flow, 1-10
 - log file locations, A-6
 - requirements for IBM DB2, 2-22
 - requirements for SQL Server, 2-14
 - requirements for Sybase ASE, 2-19

- starting, 7-15
 - stopping, 7-17
 - using in Microsoft Windows, 2-5
 - when starting Audit Vault Console, 3-2
 - Oracle Audit Vault
 - administrative tasks for high volume systems, 4-1
 - components, 1-3
 - configuring source databases, 2-1 to 2-31
 - how administrators use, 1-1
 - how components work together, 1-9
 - how it is secured, 5-1 to 5-20
 - languages supported, 2-3
 - maintenance tasks, 3-1 to 3-18
 - new features in this release, xix to xxiv
 - roles, 5-1
 - tools, 1-10
 - user accounts creating during installation, 5-1
 - See also* entries beginning with Audit Vault
 - Oracle Audit Vault clients
 - error messages, B-8 to B-16
 - Oracle Container for Java
 - See* OC4J agent
 - Oracle Database Vault
 - how it implements security, 5-10
 - included in Audit Vault Server, 1-6
 - Oracle Database Vault administrator roles
 - DV_ACCTMGR
 - about, 1-11
 - DV_ACCTMGR role
 - roles and privileges granted, 5-10
 - DV_OWNER
 - about, 1-11
 - roles and privileges granted, 5-10
 - Oracle databases
 - adding collectors to Oracle Audit Vault, 2-10
 - checking collector status, 2-31
 - collection agent credentials, adding, 2-13
 - collectors not working, A-11
 - compatibility with collectors, 2-7
 - creating user account, 2-5
 - log file for policy creation (policy-0.log), A-2
 - modifying collector attributes, 3-6 to 3-7
 - modifying source attributes, 3-12 to 3-14
 - planning configuration, 1-12
 - registering with Oracle Audit Vault, 2-5 to 2-13
 - removing from Oracle Audit Vault, 3-17 to 3-18
 - setting up in collection agent home, 8-14
 - source database errors, B-2
 - unable to connect to source database, A-13
 - verifying compatibility with collectors, 8-15
 - See also* Audit Vault Oracle Database (AVORCLDB) utility
 - Oracle Enterprise Manager Database Control
 - console, 5-3
 - Oracle MetaLink
 - See* My Oracle Support
 - Oracle Real Application Clusters
 - avca add_agent command failing on node, A-17
 - configuring collection agent connectivity for, 4-5
 - configuring collection agents for, 4-4
 - creating collectors for, 2-10
 - creating source database user account, 2-5
 - deploying av.ear file to nodes, 6-7
 - troubleshooting tips, A-17
 - where to run AVCA commands, 6-2
 - where to run AVCTL commands, 7-2
 - Oracle Streams
 - supplemental logging for REDO collectors, 12-1
 - Oracle wallets
 - creating, 6-7
 - creating credentials, 6-6
 - credentials not successful, A-9
 - generating certificate requests, 5-12, 6-12
 - how Oracle Audit Vault uses, 5-3
 - importing certificate requests, 6-15
 - locations, 5-3
 - removing certificates, 6-19
 - updating XDB certificate, 5-19
 - ORACLE_HOME environment variable, 2-2
 - ORACLE_SID environment variable, 2-2
 - oraenv UNIX script, 2-2
 - OSAUD collector
 - about, 1-8
 - attributes, 8-8
 - audit trail settings for, 1-13
 - detailed information about audit trails, 1-13
 - operating system .aud files, 1-8
 - syslog files, 1-8
 - syslog files, compressed, 1-8
 - Windows Event Log, 1-8
 - XML files, 1-8
 - OSAUD collector attributes, 8-6
- ## P
-
- passwords
 - guidelines for changing, 5-4
 - PATH environment variable, 2-2
 - performance tuning
 - Audit Vault Server, A-6
 - policies
 - See* Audit Vault policies
 - port numbers
 - Audit Vault collection agent
 - changing, 4-5
 - finding, 1-8
 - Audit Vault Server
 - changing, 4-5
 - finding, 1-6
 - purge_warehouse command (AVCTL utility), 7-5
 - purging audit trail
 - IBM DB2 audit files, 2-25
 - new features, xx
 - Oracle Audit Vault repository audit trail, 4-13
 - Oracle source databases, 4-11
 - source database in Audit Vault
 - environment, 4-12
 - SQL Server audit files, 2-18

R

- redeploy command (AVCA utility), 6-16
- REDO collector
 - about, 1-8
 - attributes, 8-9
 - audit trail settings for, 1-14
 - detailed information about audit trails, 1-14
 - recommended init.ora settings, 12-1 to 12-20
 - supplemental Oracle Streams logging, 12-1
- refresh_warehouse command (AVCTL utility) (deprecated), 0-xx
- register_remedy command (AVCA utility), 6-17
- register_smtp command (AVCA utility), 6-18
- Remedy trouble ticket service
 - registering with Oracle Audit Vault, 6-17
- Remedy trouble tickets
 - See* trouble tickets
- remedy.properties.tmpl descriptor properties file, 3-16
- remove_cert command (AVCA utility), 6-19
- removing
 - source databases from Audit Vault, 3-17 to 3-18
- reports
 - cannot be viewed, A-15
 - checking time zone used for, 6-27
 - data not showing, A-16
 - log file, A-2
 - log file created during PDF generation, A-2
 - new features, xxi
 - setting time zones, 6-24
- roles used with Oracle audit Vault, 5-1

S

- scheduling audit collections
 - See* Audit Vault data warehouse
- Secure Sockets Layer (SSL)
 - SMTP configuration, 6-24
- secure_agent command (AVCA), 6-20
- secure_av command (AVCA), 6-21
- secure_remedy command (AVCA utility), 6-23
- secure_smtp command (AVCA utility), 6-23
- securing
 - Audit Vault by mutual authentication, 6-21
 - Audit Vault Collection Agent by mutual authentication, 6-20
 - Audit Vault collection agents, 6-20
 - Audit Vault Server, 6-21
 - Oracle Audit Vault accounts, 5-1
- server.xml file, 5-3
- set_server_tz command (AVCA utility), 6-24
- set_warehouse_retention command (AVCA utility), 6-25
- set_warehouse_schedule command (AVCA utility) (deprecated), 0-xx
- setup command
 - Oracle databases, 8-14
 - SQL Server databases, 9-11
 - Sybase databases, 10-10
- SHLIB_PATH environment variable, 2-2

- show_agent_status command (AVCTL utility), 7-6
- show_av_status command (AVCTL utility), 7-7
- show_collector_status command (AVCTL utility), 2-31, 7-7
- show_oc4j_status command (AVCTL), 7-14
- show_remedy_config command (AVCA utility), 6-26
- show_remedy_status command (AVCTL utility), 7-8
- show_server_tz command (AVCA utility), 6-27
- show_smtp_config command (AVCA utility), 6-27
- show_smtp_config command (AVCTL utility), 7-9
- SMTP servers
 - See* Audit Vault e-mail notification service
- source databases
 - about, 1-3
 - altering collector attributes, 3-6 to 3-7
 - altering source database attributes, 3-12 to 3-14
 - changing source user password, 5-7
 - general steps for adding to Oracle Audit Vault, 2-1
 - log file created for Oracle database policies, A-2
 - removing from Audit Vault
 - about, 3-17
 - from command line, 3-18
 - using Audit Vault Console, 3-18
 - supported database products, 1-3
 - UNIX environment variable settings, 2-2
 - See also* IBM DB2 databases, Microsoft SQL Server databases, Oracle databases, and Sybase ASE databases
- SQL*Net
 - log file, A-6
- start_agent command (AVCTL utility), 7-9
- start_av command (AVCTL utility), 7-10
- start_collector command (AVCTL utility), 7-11
- start_oc4j command (AVCTL utility), 7-15
- starting
 - Audit Vault collection agent, Release 10.2.3.2, 7-9
 - Audit Vault Console, 3-2
 - collectors, 7-11
- state of
 - Audit Vault collection agents, pre-Release 10.2.3.2, 7-14
 - Audit Vault collection agents, Release 10.2.3.2, 7-6
 - Audit Vault Console, 3-2, 7-7
 - collectors, 7-7
- stop_agent command (AVCTL utility), 7-12
- stop_av command (AVCTL utility), 3-3, 7-13
- stop_collector command (AVCTL utility), 7-13
- stop_oc4j command (AVCTL utility), 7-17
- stopping
 - Audit Vault collection agents, for pre-Release 10.2.3.2, 7-17
 - Audit Vault Console, 3-3
 - collectors, 7-13
- Sybase ASE databases
 - adding collector to Oracle Audit Vault, 2-21
 - collector status, checking, 2-31
 - compatibility with collector, 2-20

- creating user account, 2-19
- jar file missing, A-12
- jConnect for JDBC driver, 2-19
- modifying collector attributes, 3-6 to 3-7
- modifying source attributes, 3-12 to 3-14
- planning configuration, 1-15
- registering with Oracle Audit Vault, 2-19 to 2-22
- removing from Oracle Audit Vault, 3-17 to 3-18
- setting up in collection agent home, 10-10
- source database errors, B-2
- unable to connect to source database, A-13
- verifying compatibility with collector, 10-11
- See also* Audit Vault Sybase ASE Database (AVSYBDB) utility
- SYBDB collector
 - about, 1-8
 - attributes, 10-4
 - audit trail settings for, 1-15
 - detailed information about audit trails, 1-15
 - See also* Sybase ASE databases
- SYS account
 - how Oracle Audit Vault handles, 5-11
- SYS_AUX tablespace
 - monitoring in Audit Vault Server, 4-1
- SYSDBA privilege
 - how Oracle Audit Vault handles, 5-11
 - remote collection agent, effect on, 1-7
- syslog files, 1-8
- SYSMAN account
 - how Oracle Audit Vault handles, 5-11
- SYSOPER privilege
 - how Oracle Audit Vault handles, 5-11
 - remote collection agent, effect on, 1-7
- SYSTEM account
 - how Oracle Audit Vault handles, 5-11

T

- test_remedy command (AVCA utility), 6-28
- test_smtp command (AVCA utility), 6-29
- time zones, setting for reports and alerts, 6-24
- tnsnames.ora file
 - updated by avorcldb setup command, 8-14
- trace files
 - Microsoft SQL Server, preventing from being deleted, 2-18
- Transport Layer Security (TLS)
 - SMTP configuration, 6-24
- trouble tickets
 - about, 3-16
 - configuring, 3-16 to 3-17
 - disabling configuration, 6-9
 - disabling security configuration, 6-23
 - enabling configuration, 6-10
 - enabling security configuration, 6-23
 - log file
 - Audit Vault Server, A-1
 - removing from Oracle Audit Vault, 6-17
 - status checking, 6-26
 - testing connection to Oracle Audit Vault, 6-28

- updating with deployment descriptor properties file, 6-4
- troubleshooting
 - alerts not firing, A-16
 - Audit Vault collector, A-11 to A-13
 - Audit Vault Console, A-14
 - Audit Vault Console, disabled in an Oracle RAC node, 4-3
 - Audit Vault data warehouse, audit data not appearing in, A-16
 - Audit Vault in an Oracle RAC environment, A-17
 - Audit Vault reports
 - data not showing, A-16
 - reports cannot be viewed, A-15
 - Audit Vault Server, A-6
 - collector host computer failure, A-13
 - collector not starting, 7-12
 - data not showing in reports, A-16
 - error messages, B-1 to B-16
 - failover recovery for collectors, 8-7, 9-6, 10-5
 - example for DBAUD, 8-9
 - example for SQL Server, 9-7
 - example for Sybase ASE, 10-5
 - finding detailed information about an error, A-6
 - finding Oracle Database trace files, A-6
 - new alerts not able to be created, A-16
 - SQL Server trace files being deleted by
 - accident, 2-18
 - viewing operational errors, 3-5
 - See also* errors and log files

U

- UNIX environment variable settings, 2-5
- users
 - default Oracle Audit Vault user accounts, 5-1
- UTC time zone
 - status checking, 6-27

V

- verify command
 - IBM DB2 databases, 11-9
 - Oracle databases, 8-15
 - SQL Server databases, 9-12
 - Sybase ASE databases, 10-11
- verifying source database compatibility
 - with DB2 collector, 11-9
 - with Oracle Database collectors, 8-15
 - with SQL Server collector, 9-12
 - with Sybase ASE collector, 10-11
- viewing
 - Audit Vault errors, 3-5

W

- wallets
 - See* Oracle wallets
- Windows
 - See* Microsoft Windows

