

Oracle® Audit Vault

Release Notes

10g Release 2 (10.2.2.0.0)

B31587-06

April 2007

These release notes describe issues and workarounds for Oracle Audit Vault 10g Release 2 (10.2.2.0.0).

For the latest release notes, and to view other Audit Vault documentation, see the Oracle Documentation page on the Oracle Technology Network. The URL is as follows:

<http://www.oracle.com/technology/documentation>

This document contains the following sections:

- [About Oracle Audit Vault](#)
- [Installation and Uninstallation Issues](#)
- [General Administration and Configuration Issues](#)
- [Agent Installation Supported on Additional Platforms](#)
- [Source Configuration Issues](#)
- [Collector Configuration Issues](#)
- [Documentation Accessibility](#)

1 About Oracle Audit Vault

Government regulations require businesses to provide security for data on customers, employees, and partners. Databases, applications, and other systems produce vast quantities of data. Auditors must analyze this data in a timely fashion across geographically dispersed and heterogeneous systems. Business users must consolidate data across all systems and monitor the data for a holistic view of enterprise data access. The consolidation process must use a single audit data warehouse that is secure, scalable, reliable, and highly available.

Oracle Audit Vault is an enterprise-wide auditing solution that monitors corporate data and provides alerts and reports for security auditing and compliance. Oracle Audit Vault collects audit data and critical events from databases and consolidates the data in a centralized and secure audit warehouse.

Oracle Audit Vault solves security and audit problems by performing the following functions:

- Consolidating audit information from multiple systems across the enterprise
- Detecting changes to data and generating reports and alerts
- Protecting audit data from modification

2 Installation and Uninstallation Issues

For information on platform support, licensing, and installation, read the following documents:

- Oracle Audit Vault Server Installation Guide for Linux x86
- *Oracle Audit Vault Server Installation Guide for Solaris Operating System (SPARC 64-Bit)*
- *Oracle Audit Vault Server Installation Guide for AIX 5L Based Systems (64-Bit)*
- *Oracle Audit Vault Server Installation Guide for HP-UX PA-RISC (64-Bit)*
- *Oracle Audit Vault Server Installation Guide for Linux x86-64*
- *Oracle Audit Vault Agent Installation Guide*
- *Oracle Audit Vault Licensing Information*

PostInstallation Task

After installing Oracle Audit Vault, check to see if there is a patchset or critical patch update (CPU) available.

Patchsets

Any mandatory Oracle Audit Vault patchesets can be found on the Oracle*MetaLink* Web site:

<http://metalink.oracle.com>

Click the **Patches & Updates** tab, then select the **Quick Links to the Latest Patches, Mini Packs, and Maintenance Packs** link. Look for Audit Vault under the heading **Latest Oracle Server/Tools Patchsets**, then select the desired platform and language. All available mandatory patchsets display. Click the patchset number to view the details. Click **View Readme** for more information about the patch and instructions on installing the patchset. Click **Download** to download and save the patchset.

Critical Patch Update (CPU)

A CPU is a collection of patches for security vulnerabilities. It also includes non-security fixes required (because of interdependencies) by those security patches. CPUs are cumulative, and they are provided quarterly on the Oracle Technology Network. Oracle Audit Vault 10.2.2.0.0 does not include the April 2007 RDBMS CPU for the underlying 10.2.0.3 database, thus install this RDBMS CPU. If a later RDBMS CPU is available, then install that. For more information about CPUs, see:

<http://www.oracle.com/security/critical-patch-update.html>

For the latest information on whether a specific CPU is certified with Oracle Audit Vault, review the certification matrix on the Oracle*MetaLink* Web site.

The Oracle*MetaLink* Web site is available at:

<http://metalink.oracle.com>

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

<http://www.oracle.com/technology/support/metalink/content.html>

Known Issues and Workarounds

The rest of this section describes known issues and workarounds pertaining to installation and uninstallation. The following topics are discussed:

- Restarting Oracle Enterprise Manager DBConsole After an Audit Vault Server Installation May Return an Error
- Restarting Oracle Audit Vault Database After an Audit Vault Server Installation Takes a Long Time for the Data to Appear in Audit Vault Console Overview and Reports Pages
- Immediately Following an Audit Vault Server Installation in an Oracle RAC Environment Access to Audit Vault Console Returns a 500 Server Error
- The Silent Installer Does Not Issue an Error When the SID Is Omitted
- The Silent Installer for the Agent Does Not Validate Against the Server
- Silent Installation May Not Report on a Failed dvca Command
- Silent Installation Proceeds Even When Variables Are Not Populated
- Silent Installation for the Agent Does Not Report Incorrect Parameters
- Silent Installation on HP-UX PA-RISC (64bit) Fails When the DISPLAY Environment Variable Is Not Set
- The Required Storage Is Not Updated When Adding to the ASM Disk Group
- The -record Option Is Not Supported
- The Same sysdba Password Is Required for Audit Vault and ASM
- An Error Occurs After Selecting a Non-Empty Oracle Home for Agent Installation
- The "One-Click" Installer Does Not Start Up
- After an Oracle RAC Installation, an Error Is Issued During Creation of the Database
- In an Oracle RAC Environment, Preparatory Steps Are Required Before Installing Additional Nodes
- In an Oracle RAC Environment, an SPFILE Error Is Issued During Installation
- Database Is in an UNKNOWN State after Rebooting Cluster Nodes
- Manual Cleanup Is Required After Uninstalling the Audit Vault Database
- Error File Getting Generated During Audit Vault Server Installation
- On Solaris 10, Oracle Audit Vault Server One-Off Patches Configuration Assistant Can Fail If O/S Patches Are Not Installed
- avsys User Cannot Change Its Password After the Account Is Unlocked by the Database Vault Account Manager

2.1 Restarting Oracle Enterprise Manager DBConsole After an Audit Vault Server Installation May Return an Error

After an Audit Vault Server installation, if you restart Oracle Enterprise Manager DBConsole, the operation may return an error because DBConsole is not restarting in UTC time zone.

Because both Audit Vault database and Oracle Enterprise Manager DBConsole are always in UTC time zone, Oracle Enterprise Manager DBConsole must be started up again in UTC time zone. To ensure this happens, you can either perform the AVCTL `start_av` command, which automatically starts up Oracle Enterprise Manager DBConsole and Audit Vault Console in UTC time zone, or you must first set the environment variable `TZ` to UTC, and then use the `emctl start dbconsole` command.

2.2 Restarting Oracle Audit Vault Database After an Audit Vault Server Installation Takes a Long Time for the Data to Appear in Audit Vault Console Overview and Reports Pages

Whenever you restart the Audit Vault database, you must first set the time zone to UTC in the Audit Vault Server shell before starting the database. For example:

1. Set the `TZ` environment variable to UTC time zone.

```
setenv TZ UTC
```

2. Start the database.

```
sqlplus / as sysoper  
SQL> startup
```

3. Set the `TZ` environment variable back to your local time zone for the Audit Vault Server shell.

```
setenv TZ <to your local time zone>
```

Otherwise, it takes a very long time to see the audit records appear on the Audit Vault Console **Overview** and reports pages. This is because the Audit Vault database will start up in local time zone and will not be synchronized with the Audit Vault Console which is set to UTC time zone.

2.3 Immediately Following an Audit Vault Server Installation in an Oracle RAC Environment Access to Audit Vault Console Returns a 500 Server Error

In an Oracle RAC Environment, immediately following an Audit Vault Server installation, an attempt to bring up the Audit Vault Console in a Web browser returns the following error:

```
500 Server Error  
The following error occurred: [code=CANT_CONNECT] Could not connect because  
of networking problems. Contact your system administrator.  
Could not open error file
```

The workaround is to perform, in the Audit Vault Server shell, an `avctl stop_av` command to stop the Audit Vault Console and then perform an `avctl start_av` command to start the Audit Vault Console. Restarting the Audit Vault Console in this way allows access to it in a Web browser using the URL provided upon completion of the Audit Vault Server installation.

2.4 The Silent Installer Does Not Issue an Error When the SID Is Omitted

When performing silent installation for the Audit Vault Server, if you do not provide a value for the `s_dbSid` option, the SID defaults to `av`.

The workaround is to ensure that you have set the correct value for the `s_dbSid` option in the response file before running the silent installation.

2.5 The Silent Installer for the Agent Does Not Validate Against the Server

When performing a silent installation of the Audit Vault Agent, the installer does not connect to the specified Audit Vault Server and check the user-provided information. This type of validation is only available when using one-click installation.

The following are workarounds:

- Ensure that you are installing the agent on the computer that you specified when issuing the `avca add_agent` command on the server.
- Manually check the user-provided information in the response file for the silent installation.
- Verify that the Audit Vault database is up.

2.6 Silent Installation May Not Report on a Failed `dvca` Command

When running a silent installation, the `dvca` command may fail to run. However, the silent installer will report that it ran successfully.

The workaround for this issue is to check the installation logs after running silent installation. The log files are located as follows:

```
ORACLE_HOME/cfgtoollogs/oui/installActionsdate_time.log
```

2.7 Silent Installation Proceeds Even When Variables Are Not Populated

When you run the silent installation program, as follows, you may receive an error:

```
./runInstaller -silent -responseFile <absolute path to av.rsp file>
```

If you have not properly supplied all required variables in the silent installation file, the following error appears:

```
'SEVERE:Abnormal program termination. An internal error has occurred.  
Please provide the following files to Oracle Support :'
```

If you receive this error, check the silent installation response file and ensure that you have provided proper input for all required variables.

2.8 Silent Installation for the Agent Does Not Report Incorrect Parameters

On Windows, silent installation of the Audit Vault Agent can report that the `avca` command succeeded, even if you supplied incorrect parameters in the response file.

You should check the installation logs after completing silent installation. Errors are reported correctly in the log file.

2.9 Silent Installation on HP-UX PA-RISC (64bit) Fails When the DISPLAY Environment Variable Is Not Set

When performing a silent installation on HP-UX PA-RISC (64bit) platform, if the `DISPLAY` environment variable is not set to a proper `DISPLAY` value, the installation will fail during the Oracle Net Services configuration assistant operation.

The workaround is before starting the silent installation on HP-UX PA-RISC (64-bit), set the `DISPLAY` environment variable to a valid `DISPLAY` value.

2.10 Silent Installation on AIX 5L Based Systems (64-Bit) Asks for `rootpre.sh` Confirmation

When performing a silent install on AIX 5L Based Systems (64-Bit), the installer asks for confirmation that the `rootpre.sh` script was run. It is important to run the `rootpre.sh` script to setup the AIX 5L system the first time. If this has already been performed, the silent install confirmation can be bypassed by setting the following environment variable before starting the `runInstaller`:

```
$ export SKIP_ROOTPRE=TRUE
```

2.11 The Required Storage Is Not Updated When Adding to the ASM Disk Group

When adding disks to an existing Automatic Storage Management (ASM) disk group during Audit Vault Server installation, the amount of required storage space may not be updated.

The workaround is to click the **Change Discovery Path** button and update the discovery path before adding the disks.

2.12 The `-record` Option Is Not Supported

In this release, the installer does not support the `-record` option.

2.13 The Same `sysdba` Password Is Required for Audit Vault and ASM

After installing Automatic Storage Management (ASM) and Oracle Audit Vault Server, you may receive the following error when connecting to ASM:

```
"Supllied ASM SYSDBA password is invalid"
```

The workaround is to provide the same `sysdba` password for both ASM and Audit Vault Server.

2.14 An Error Occurs After Selecting a Non-Empty Oracle Home for Agent Installation

When installing an Audit Vault Agent, if you select a non-empty Oracle Home directory, you receive the following error:

Recommendation: Choose a new Oracle Home or a home that contains Oracle Database 10g Client Release 1 software or a home that contains Oracle Database 10g Release 2 software for installing this product.

This message is applicable to the Oracle 10g Release 1 client, not the Audit Vault Agent. You should install the Audit Vault Agent in a new home directory, or in an existing Oracle Audit Vault home directory.

2.15 The "One-Click" Installer Does Not Start Up

On Windows, if you run `setup.exe` using additional options, for example, `-record`, or if the system is running Cluster Ready Services (CRS), the one-click installation program may not start up.

The workaround is to add the following option when invoking `setup.exe` with additional options:

```
-oneclick
```

2.16 After an Oracle RAC Installation, an Error Is Issued During Creation of the Database

After installing Audit Vault Server, the following error appears when creating an Oracle RAC database using the `dbca` command:

```
Failed to retrieve network listener Resources
```

The workaround for this error is to click **yes** on the error screen and continue the installation.

2.17 In an Oracle RAC Environment, Preparatory Steps Are Required Before Installing Additional Nodes

You can receive an SPFILE error when running the `dvca` command on a remote node after installation in an Oracle RAC environment.

To avoid this error, perform the following steps after installing Audit Vault Server on a single node in an Oracle RAC environment, and before adding other nodes using the `addnode` script on the local node:

1. Stop the database, as follows:

```
srvctl stop database -d db_name -c "sys/sys_passwd as sysdba"
```

Where *db_name* is the name of the database you are stopping, *sys* is the ID that was generated during the database installation, and *sys_passwd* is the corresponding password.

2. Start the database with the NOMOUNT option, as follows:

```
$ sqlplus /NOLOG
SQL> CONNECT SYS/SYS_password AS SYSDBA
SQL> STARTUP NOMOUNT
```

3. Create an SPFILE from PFILE, as follows:

```
SQL> CREATE SPFILE='SHARED_LOCATION/SPFILE.ORA'  
FROM 'PFILE=pfile_location/init.ora'
```

Where *pfile_location* is usually *ORACLE_HOME/admin/db_name/pfile* for Optimal Flexible Architecture-compliant databases.

4. Shut down the database:

```
SQL> SHUTDOWN IMMEDIATE  
SQL> EXIT
```

5. Clear the contents of the PFILE located at *ORACLE_HOME/dbs/initsid.ora* and set the value of SPFILE to *SHARED_LOCATION/SPFILE.ORA*.

6. Restart the database.

2.18 In an Oracle RAC Environment, an SPFILE Error Is Issued During Installation

When installing Audit Vault Server on a single node in an Oracle RAC environment, the following messages are written to the *dvca_install.log* file:

```
Error executing task INIT_AUDIT_SYS_OPERATIONS:java.sql.SQLException:  
ORA-32001: write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_REMOTE_OS_AUTHENT:java.sql.SQLException: ORA-32001:  
write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_REMOTE_OS_ROLES:java.sql.SQLException: ORA-32001:  
write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_OS_ROLES:java.sql.SQLException: ORA-32001: write to  
SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_SQL92_SECURITY:java.sql.SQLException: ORA-32001:  
write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_OS_AUTHENT_PREFIX:java.sql.SQLException: ORA-32001:  
write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_REMOTE_LOGIN_PASSWORDFILE:java.sql.SQLException:  
ORA-32001: write to SPFILE requested but no SPFILE specified at startup  
Error executing task INIT_RECYCLEBIN:java.sql.SQLException: ORA-32001: write  
to SPFILE requested but no SPFILE specified at startup
```

You can ignore the errors, and after the installation is complete, edit the pfile using the following information and restart the database:

```
audit_sys_operations=TRUE  
remote_os_authent=FALSE  
remote_os_roles=FALSE  
os_roles=FALSE  
sql92_security=TRUE  
os_authent_prefix=''  
remote_login_passwordfile=EXCLUSIVE  
recyclebin=OFF
```

The pfile location is usually *ORACLE_HOME/admin/db_name/pfile* for Optimal Flexible Architecture-compliant databases.

2.19 Database Is in an UNKNOWN State after Rebooting Cluster Nodes

In an Audit Vault Oracle RAC environment, if you reboot the cluster nodes after installation, the database can revert to an UNKNOWN status. For example, if you enter the following command, the application state is listed as UNKNOWN:

```
crs_stat -t
```

Name	Type	Target	State	Host
ora...v1.inst	application	ONLINE	UNKNOWN	staka09
ora...v2.inst	application	ONLINE	UNKNOWN	staka10
ora.av.db	application	ONLINE	OFFLINE	
ora...09.lsnr	application	ONLINE	ONLINE	staka09
ora...a09.gsd	application	ONLINE	ONLINE	staka09

To return the database to an ONLINE state, restart the database after rebooting the nodes, as follows:*

```
$ORACLE_HOME/bin/srvctl stop database -d db_name -c "sys/<sys passwd> as sysdba"  
$ORACLE_HOME/bin/srvctl start database -d db_name -c "sys/<sys passwd> as sysdba"
```

Where *db_name* is the name of the database, *sys* is the ID that was generated during database installation, and *sys passwd* is the corresponding password.

2.20 Manual Cleanup Is Required After Uninstalling the Audit Vault Database

After uninstalling the Audit Vault database, the configuration files that Audit Vault created are not removed.

You must manually delete the Audit Vault home directory after uninstalling the Audit Vault database.

2.21 Error File Getting Generated During Audit Vault Server Installation

When installing Oracle Audit Vault Server using Oracle Universal Installer, after clicking **Next** on the **Prerequisite Checks** screen, the following runtime exception content is written to the error file that is generated:

```
Runtime exception during validation of variable :s_racSid  
java.lang.NullPointerException  
    at  
Components.oracle.rdbms.dv.v10_2_0_3_0.CompContext.validate_s_racSid(Unknown  
Source)  
    at  
Components.oracle.rdbms.dv.v10_2_0_3_0.CompContext.validate(Unknown Source)  
    at  
oracle.sysman.oii.ois.OiisVariable.validate(OiisVariable.java:1409)  
    at  
oracle.sysman.oii.ois.OiisVariable.validateChildVariables(OiisVariable.java:  
1836)  
    at  
oracle.sysman.oii.ois.OiisVariable.setValue(OiisVariable.java:1124)  
    at
```

```

oracle.sysman.oii.ois.OiisVariable.setVariable(OiisVariable.java:2197)
    at
oracle.sysman.oii.ois.OiisCompContext.doOperation(OiisCompContext.java:1093)
    at
oracle.sysman.oii.oif.oifb.OiifbLinearIterator.iterate(OiifbLinearIterator.
java:147)
    at
oracle.sysman.oii.oic.OiicCompsWizEngine.doOperation(OiicCompsWizEngine.java
:202)
    at
oracle.sysman.oii.oif.oifb.OiifbLinearIterator.iterate(OiifbLinearIterator.
java:147)
    at
oracle.sysman.oii.oic.OiicInstallSession$OiicSelCompsInstall.doOperation(Oii
cInstallSession.java:3838)

```

This exception is a benign error and will be suppressed in a future release. It does not affect the installation or the functionality of the installed Audit Vault databases for a single instance installation or for an Oracle RAC environment installation. Please ignore this error.

2.22 On Solaris 10, Oracle Audit Vault Server One-Off Patches Configuration Assistant Can Fail If O/S Patches Are Not Installed

Oracle Audit Vault Server One-Off Patches configuration assistant can fail or report installation warnings on the Solaris 10 platform, unless the following Operating System patch is installed:

123908-01 SunOS 5.10: ar patch

Ensure that this Operating System patch has been applied to the system prior to installing Oracle Audit Vault.

For additional information, see Note 353150.1 available on Oracle Metalink.

2.23 avsys User Cannot Change Its Password After the Account Is Unlocked by the Database Vault Account Manager

Following an Audit Vault Server installation, the `avsys` user cannot change its own password after the account is unlocked by the Database Vault account manager. For example:

```

sqlplus <Database Vault Account Manager>/<pwd>
SQL> alter user avsys account unlock;
User altered.
SQL> connect avsys/avsys
ERROR:
ORA-28001: the password has expired
Changing password for avsys
New password: <provided new pwd>
Retype new password: <confirmed pwd>
ERROR:
ORA-00604: error occurred at recursive SQL level 1
ORA-01031: insufficient privileges
ORA-06512: at "DVSYS.DBMS_MACUTL", line 10
ORA-06512: at "DVSYS.DBMS_MACUTL", line 367
ORA-06512: at line 26
Password unchanged

```

Warning: You are no longer connected to ORACLE.

The workaround is to have the Database Vault account manager change the avsys password. For example:

```
sqlplus <Database Vault Account Manager>/<pwd>
SQL> alter user avsys account unlock;
User altered.
SQL> alter user avsys identified by <new password>;
User altered.
SQL> connect avsys/<new password>;
Connected.
```

3 General Administration and Configuration Issues

This section discusses administration and configuration issues and workarounds.

This section discusses the following topics:

- [Adding Source and Collectors in the Audit Vault Console](#)
- [Supported Versions of the Oracle Database Source](#)
- [Some Agent and Alert Configuration Messages Are Inaccurate or Unclear](#)
- [Some Translated Error Messages Are Displayed in English](#)
- [Garbled Multibyte User Name Is Displayed on the Login Page](#)
- [You Cannot Log In After a Timeout](#)
- [Inconsistent Behavior When Deleting an Alert](#)
- [Changing the Focus of an Alert Can Cause the Audit Vault Console to Crash](#)
- [FGA Policy Names Cannot Contain Special Characters](#)
- [For Certain Complex Condition Statements it is Necessary to Escape Single Quotes within String Arguments](#)
- [Do Not Modify or Delete the Two Table Capture Rules on the STREAMS_HEARTBEAT Table](#)
- [On Occasion the NEEDED Count Displayed May be Out-of-Sync with the Audit Setting Status](#)
- [500 Error Occurs if You Specify An Invalid Warehouse Retention Time](#)
- [Warehouse Configuration Buttons Are Missing](#)
- [Subpools for Streams Can Become Too Large](#)

3.1 Adding Source and Collectors in the Audit Vault Console

Refer to Section 3.3 in *Oracle Audit Vault Administrator's Guide* to add sources and collectors to Audit Vault using the AVORCLDB command-line utility. Only use the Audit Vault Console to view and edit the sources, agents, and collectors.

3.2 Supported Versions of the Oracle Database Source

For this release, Oracle Database releases 9.2.X, 10.1.X, 10.2.X are supported for the OSAUD, DBAUD collector types as an audit data source.

For this release, Oracle Database releases 9.2.0.8, 10.1.0.6, and 10.2.0.3 are supported for the REDO collector type as an audit data source.

For the latest information on supported Oracle Database releases as an audit data source, review the certification matrix on the *OracleMetaLink* Web site.

The *OracleMetaLink* Web site is available at:

<http://metalink.oracle.com>

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

<http://www.oracle.com/technology/support/metalink/content.html>

3.3 Some Agent and Alert Configuration Messages Are Inaccurate or Unclear

When configuring Audit Vault, you can encounter a few error messages that require clarification.

The following is a list of errors that you may find misleading:

- When you add an agent, you can receive the message, "Agent added successfully" even if the agent has not been added.
- When you edit an agent, you can receive the error, "Please provide the agentname" even if you have supplied the agent name.

The same message can appear when you click **OK** on this page.

- When enabling an alert, you can receive the following message:

"Enabling Alerts Failed"

This message should state, "Enabling Alerts Failed. Alerts are already enabled."

A similar problem occurs when disabling an alert.

3.4 Some Translated Error Messages Are Displayed in English

Some error messages are displayed in English even if the rest of the Audit Vault product has been localized. For example, if you do the following in a localized version of Audit Vault you may see an English error:

1. Log in to Audit Vault Console as an Audit Vault administrator and connect as AV_ADMIN.
2. Click the **Agent** sub-tab.
3. Click **Start** for an already-started agent.

3.5 Garbled Multibyte User Name Is Displayed on the Login Page

If you enter an invalid multibyte user name on the login page for the Audit Vault Console, an error is displayed and the user name is displayed in a garbled manner.

For example, this problem occurs if you do the following:

1. Set the browser to simplified Chinese.
2. Access the Audit Vault Console URL.
3. On the login page, enter an invalid multibyte user name and click **Login**.

3.6 You Cannot Log In After a Timeout

When working in the Audit Vault Console, after an inactivity timeout you must supply your login credentials. However, when you re-enter your credentials, Audit Vault Console issues an error.

The workaround is to reenter the Audit Vault Console URL by removing all text after `http://<system-name>:<port number>/av` and pressing **Enter** on the keyboard to launch the search for the URL.

3.7 Inconsistent Behavior When Deleting an Alert

When you click the trash icon in the *Remove* column to remove an alert, the alert is removed immediately.

In other sections of the Audit Vault Console, a confirmation page appears.

3.8 Changing the Focus of an Alert Can Cause the Audit Vault Console to Crash

When logged in as an auditor administrator and configuring an alert, the Audit Vault Console can exit unexpectedly. For example, this can happen when you do the following:

1. From the Audit Vault Console, select **Audit Policy**, then **Alerts**.
2. Change the default focus from **Basic** to **Advanced**, then back to **Basic**.
3. Click **OK**.

3.9 FGA Policy Names Cannot Contain Special Characters

FGA Policy names can only have alphanumeric characters. If you use a special character, for example a hyphen ("-") in the name, the Audit Vault database truncates everything that follows the special character.

For example, if you do the following, the policy name "Test-123" is truncated to "Test":

1. From the Audit Vault Console Audit Reports **Overview** page, click the **Audit Policy** tab.
2. If required, click **Audit Settings** in the upper left.
3. Select the Audit Source where you want to define settings.
4. Go to the **Overview** page, click **FGA** subtab, and create a policy named Test-123.

3.10 For Certain Complex Condition Statements it is Necessary to Escape Single Quotes within String Arguments

While defining FGA Audit Settings using the Audit Vault Console, it is necessary to escape single quotes within string arguments in certain complex condition statements. For example, to define an audit condition where the condition is 'dept equals SALES', it should be defined as dept = "SALES". Another example would be: SYS_CONTEXT("USERENV","SESSION_USER")<>"APPS".

3.11 Do Not Modify or Delete the Two Table Capture Rules on the STREAMS_HEARTBEAT Table

When the REDO collector is deployed on a Release 10.2.0.3 source database and when audit settings are retrieved, two table capture rules (on the STREAMS_HEARTBEAT table) are automatically defined. Recommendation: The two table rules are defined by the STREAMS package automatically. They are needed for the REDO collector to work correctly.

3.12 On Occasion the NEEDED Count Displayed May be Out-of-Sync with the Audit Setting Status

In some rare circumstances, the NEEDED count displayed may be out-of-sync with the audit setting status. The workaround is to refresh the state of the system by doing a retrieve action or provision action or both to re-sync the counts.

3.13 500 Error Occurs if You Specify An Invalid Warehouse Retention Time

If you provide an illegal retention time for the data warehouse, you can receive a "500 Internal Server Error."

For example, this problem can occur if you do the following:

1. Install an Audit Vault Server and Agent.
2. Set up and start a source and REDO, DBAUD, and OSAUD Collectors for a database.
3. Log in to Audit Vault Console as an Audit Vault administrator and connect as AV_ADMIN.
4. Click **Configuration**, then click **Warehouse**.
5. Set an invalid retention time, for example, specify 15 in the **Month** field.
6. Click **Reply**.

An error similar to the following appears:

```
500 Internal Server Error
java.lang.NumberFormatException
at oracle.sql.INTERVALYM.toBytes(INTERVALYM.java:173)
at oracle.sql.INTERVALYM.<init>(INTERVALYM.java:108)
at oracle.sysman.emo.avt.configuration.AVWarehouseConfigViewObject.
getIntervalString(AVWarehouseConfigViewObject.java:485)
at oracle.sysman.emo.avt.facade.AVWarehouseConfigService.setDuration
(AVWarehouseConfigService.java:156)
at oracle.sysman.db.adm.avt.AVWarehouseConfigController.handleEvent
(AVWarehouseConfigController.java:189)
```

```
at oracle.sysman.emSDK.svlt.PageHandler.handleRequest(PageHandler.  
java:376)  
at oracle.sysman.db.adm.RootController.handleRequest(RootController.  
java:170)  
at oracle.sysman.db.adm.AVControllerResolver.handleRequest  
(AVControllerResolver.java:125)  
...
```

3.14 Warehouse Configuration Buttons Are Missing

In the Audit Vault Console pages for Warehouse configuration, buttons are missing for **Load Warehouse** on the **History of Loading** page and **Purge Warehouse** on the **History of Purging** page.

The workaround for this is to use the AVCTL command line for these functions, as follows:

```
avctl load_warehouse -startdate start_date -numofdays number_of_days  
[-dateformat date_format] [-wait]
```

```
avctl purge_warehouse -startdate start_date -numofdays number_of_days  
[-dateformat date_format] [-wait]
```

See the *Oracle Audit Vault Administrator's Guide* for details.

3.15 Subpools for Streams Can Become Too Large

The REDO collector uses Oracle Streams technology to retrieve logical change records (LCRs) from the REDO logs. On the source database, a Streams capture process uses LogMiner to extract new LCRs from the REDO logs based on capture rules that are defined by the user.

If you configure initialization parameters for a streams pool with subpool durations for instance, session, cursor, and execution, you can receive 403 errors.

The workaround is to combine the durations into one pool using the following initialization parameter in `init.ora`:

```
_enable_shared_pool_durations = false
```

The disadvantage of this parameter is that the streams pool will never shrink.

Another possible solution is to find what allocations made a particular duration subpool too large and change their durations, for example, from `session` to `cursor` or `execution`.

4 Agent Installation Supported on Additional Platforms

The section discusses additional platforms that are supported for Audit Vault Agent installation.

This section discusses the following topics:

4.1 Audit Vault Agent Installation Is Supported on Novell SuSE Linux Enterprise Server 10.0 (SLES-10) Platform

For the current release, Release 10.2.2, Audit Vault Agent installation is supported on the Novell SuSE Linux Enterprise Server 10.0 (SLES-10) platform. For details on the hardware and software requirements, see the *Oracle Audit Vault Server Installation Guide for Linux x86*.

5 Source Configuration Issues

This section discusses source issues that you may encounter with Audit Vault. It also provides the workarounds for these issues.

This section discusses the following topics:

- [Some Source Configuration Messages Are Inaccurate or Unclear](#)
- [Audit Vault Console Configuration and Other Problems](#)
- [Double-Byte Source Names Can Be Garbled in Search Fields](#)
- [Audit Vault Console Does Not Show Agent-to-Source Mapping](#)

5.1 Some Source Configuration Messages Are Inaccurate or Unclear

When configuring Audit Vault using Audit Vault Console logged in as an Audit Vault administrator and connected as AV_ADMIN, you can encounter a few error messages that require clarification.

The following is a list of errors that you may find unhelpful:

- After adding a source, you can receive a message stating that the add action has failed, however, after a short delay the source is added and appears in the user interface.
- If you click **Configuration**, then click **Audit Source**, click **Source**, and then click **View**, the port number is shown as a floating number (8235.0).
It should be a whole number.
- If you click **Configuration**, then click **Audit Source**, click **Source**, click **Edit**, and then click **OK**, an error appears even if no values have been changed.

5.2 Audit Vault Console Configuration and Other Problems

When using Audit Vault Console, you may see the following problems:

- When you navigate (Configuration -> Audit Source -> Source -> Edit), the value for the **Authentication Attribute** field is missing, and it should be either AUTH_TYPE_PWD or AUTH_TYPE_SSL.
- When you navigate (Management -> Collectors), the bread crumb is missing the word Collectors.
- When you navigate (Management -> Agents), then click the Agents bread crumb, it takes you to the **Collectors** page instead of the **Agents** page.
- When you navigate (Configuration -> Collector -> Edit), if there are 11 attributes, the 11th attribute displays on another page. Clicking **Next Attribute** takes you to a page that does not show the 11th attribute nor any of the property names and values for that collector.

- When you navigate (Configuration -> Agent -> Edit), if you attempt to edit all the fields, then click **OK** to save your changes, only the **User** field is updated. The values for the other fields are not changed.
- When you navigate (Configuration -> Collector -> Create), on the **Add Collector: Attributes (Step 2 of 3)** page, values are entered corresponding to the attribute names; however, on the **Review (Step 3 of 3)** page, these values are shown against the incorrect attribute names. The order of appearance of the attribute names is changed, but the attribute value order remains unchanged.
- When you navigate (Configuration -> Agent -> Create), the port number is shown as a required field when it should not be. This is inconsistent with the AVCA `add_agent` command. The port number is always assigned automatically.
- When you navigate (Configuration -> Collector -> Edit), updating any attributes several times results in the following error message: ORA-01000: maximum open cursors exceeded ORA-01000: maximum open cursors exceeded ORA-06512: at "AVSYS.DBMS_AUDIT_VAULT", line 119 ORA-06512: at line 6
- When you navigate (Configuration -> Audit Source -> Source -> Create), and enter attributes on the **Add Source: Attributes (Step 2 of 3)** page, they do not display correctly on the **Review (Step 3 of 3)** page. The value for the `GLOBAL_DATABASE_NAME` attribute and `PORT` attribute are swapped, causing source creation to fail.
- When you navigate (Activity Reports -> + Activity Reports -> Account Management Activity -> Save definition -> Create Report), a report generation error displays because there is no corresponding text box beside the **Audit Event Category** field on the **Report Generation** page. This is a problem with languages other than English.
- When you navigate (Audit Policy -> Audit Settings -> Audit Source link -> Capture Rule -> Create -> OK), untranslated error messages display when the language is other than English.
- When you navigate (Audit Policy -> Audit Settings -> Audit Source link -> Overview), on the **Overview** page, in languages other than English the following subtabs are not translated and display in English (Statement, Object, Privilege, FGA, and Capture Rule).
- When you navigate (Configuration -> Warehouse), on the **Warehouse Settings** page, change a value for a field, such as **Retention Time**, then click **Apply**, the following error message displays: "The configuration change apply operation failed." However, if you click the **Warehouse** tab again, you will notice that the change was applied and saved. Please ignore this error message, but always check to see that your change was applied and saved by clicking the **Warehouse** tab again any time you change values for any of the fields on the **Warehouse Settings** page.
- When you navigate (Audit Policy -> Audit Settings), you may see a discrepancy in the value shown in the **Needed** column compared to the value shown in the **Needed** column that displays when you navigate (Audit Policy -> Audit Settings -> Audit Source link -> Overview). This difference is due to the fact that the **Needed** column in the **Overview** page indicates whether an audit setting is set up by an auditor and saved, but is not in use (active) on the source, therefore it is not yet provisioned, and "needs" to be

provisioned. However, the value in the **Needed** column for the **Audit Settings** page is not incremented until the audit setting is saved. Once the audit setting is provisioned to the source, the **Audit Settings** page indicates that the audit setting is in use by incrementing the value in the **In Use** column by the number of audit settings that have been provisioned. If you return to the **Overview** page, the audit setting is no longer indicated as being needed because it was provisioned, thus the value in the **Needed** column is reset to zero (0) and the value for the **In Use** column is incremented by the number of audit settings that were provisioned. The discrepancy in the value displayed in the **Needed** column for the **Audit Settings** page thus shows a running total of the audit settings that were needed for this source, while the **Overview** page indicates only whether an audit policy is in need of being provisioned. Another way of understanding the value in the **Needed** column is to realize that it represents the total number of check marks in the **Needed** columns for the **Statement** page, **Object** page, **Privilege** page, **FGA** page, and **Capture Rule** page.

5.3 Double-Byte Source Names Can Be Garbled in Search Fields

When using Audit Vault Console to conduct a search for a source in an environment that uses a double-byte character set, a search field can be pre-populated with garbled data.

For example, if you do the following, this problem can occur.

1. Log in to Audit Vault Console as an auditor administrator using zh_CN as the locale in the browser.
2. Click **Audit Policy** from the Audit Reports **Overview** page.
3. Select a source with a multi-byte name and click **Retrieve from Source**.
4. Click the link for the retrieved source.
5. Click **FGA**, then **Create**.
6. Click the icon next to the **Object** field.
7. In the **Search and Select** page, the multi-byte source name in the input field is garbled.

The workaround is to manually enter the name in the input field.

5.4 Audit Vault Console Does Not Show Agent-to-Source Mapping

When using Audit Vault Console to add a source, no agent mappings are displayed. To work around this issue, use the AVORCLDB command-line utility to add the source, for example:

```
avorcldb add_source -src lnxserver:2222:sourceldb.domain.com
-srcusr srcuser1/<pwd> -avsrcusr avsrcuser1 -desc 'HR Database'
-agentname agent1
```

The `-agentname` parameter maps the source to the agent.

6 Collector Configuration Issues

This section contains issues regarding Collector configuration for Oracle Audit Vault.

This section discusses the following topics:

- [Collector Setup May Succeed with an Error Indicating AUDIT_FILE_DEST Database Parameter Contains an Invalid "?" Character](#)
- [Collector Startup Can Be Slow](#)
- [Some Collector Configuration Messages Are Inaccurate or Unclear](#)
- [When Starting a Collector, Multibyte Error Messages Are Not Displayed Properly](#)
- [The AVCTL start_collector Command Returns Garbled Multibyte Names](#)
- [When to Properly Set the NLS_LANG Environment Variable](#)
- [Traces Can Cause a REDO Collector to Crash](#)

6.1 Collector Setup May Succeed with an Error Indicating AUDIT_FILE_DEST Database Parameter Contains an Invalid "?" Character

The AUDIT_FILE_DEST database parameter may use a default value of `?/rdbms/audit`, where the "?" question mark character is supposed to represent the value of the \$ORACLE_HOME environment variable for the Oracle home. During OSAUD collector setup, the value of AUDIT_FILE_DEST is used for the OSAUDIT_FILE_DEST and OSAUDIT_DEFAULT_FILE_DEST initialization parameters. The "?" character is an invalid character for these two initialization parameters.

When you add an OSAUD collector and the AUDIT_FILE_DEST database parameter contains this invalid "?" character, the AVORCLDB `add_collector` command succeeds, but shows the following error message in its output as a reminder to modify the OSAUDIT_FILE_DEST and OSAUDIT_DEFAULT_FILE_DEST initialization parameters with a valid value to represent the Oracle home; otherwise, the OSAUD collector will start up incorrectly:

```
avorcldb add_collector -srcname SRC1.REGRESS.RDBMS.DEV.US.ORACLE.COM
-srcusr srclusr/welcome_1 -agentname avagent1 -colltype OSAUD
-av system01:1521:av.us.oracle.com -avsrcusr avsrclusr/welcome_1
ERROR: use of '?' in audit file destination is not supported
Adding collector...
Collector added successfully.
collector successfully added to Audit Vault
.
remember the following information for use in avctl
Collector name (collname): OSAUD_Collector
```

6.2 Collector Startup Can Be Slow

After several restarts, a Collector can take a while to start up. In most cases, once the AVCTL `start_collector` command is successful, the AVCTL `show_collector_status` command and Audit Vault Console will indicate that the collector is running. However, in some cases the collector status may indicate that it is not running. This can be due to working in a slow environment and it takes more time to respond to the metrics query, or the collector is doing an initialization and recovery. In either case, you should wait a little longer before making another collector status query. The collector status will eventually indicate a running state.

The workaround is to wait until startup is complete. Operations should be normal after the Collector has finished starting up.

6.3 Some Collector Configuration Messages Are Inaccurate or Unclear

When configuring a Collector, you can encounter a few error messages that require clarification.

The following is a list of errors that you may find unhelpful:

- After adding a Collector, you can receive a message stating that the add action has failed, however, after a short delay the Collector is added and appears in the user interface.
- When you edit a Collector, the edited information may not appear in the user interface.
- When you delete a Collector, you can receive a message stating that the delete action failed, even if the Collector has been deleted.

6.4 When Starting a Collector, Multibyte Error Messages Are Not Displayed Properly

When using Audit Vault Console, if there is an error when starting up a Collector on a browser that is configured for a multibyte language, the error message is displayed partially in English and partially in a garbled format in the target language, as follows:

"Failed to initialize Audit Service, ORA-28150: *garbled multibyte text*"

For example, this can occur if you do the following:

1. Set the browser to simplified Chinese.
2. Log in to Audit Vault Console as an Audit Vault administrator and connect as AV_ADMIN.
3. Click **Management**, then click **Collector**.
4. Select a Collector and click **Start**.

6.5 The AVCTL start_collector Command Returns Garbled Multibyte Names

When you configure multibyte source and collector names, you can receive an error when you start the Collector, as follows:

1. Add a multibyte source name using the AVORCLDB `add_source` command.
2. Add a multibyte collector name using the AVORCLDB `add_collector` command.
3. Run the AVORCLDB `setup` command using the multibyte source name.
4. Start the Collector as follows:

```
avctl start_collector -collname from_step_2 -srcname from_step_1
```

You will receive an "Error executing task start_collector" message with garbled multibyte source and Collector names.

The workaround is as follows:

1. On the host for the agent, set the LANG and NLS_LANG environment variables to the character set for your multibyte language.

For example, you can configure Simplified Chinese as follows:

```
LANG=zh_CN.gbk  
NLS_LANG=.zhs16gbk
```

To support multiple languages, set the environment variables to use Unicode, as follows:

```
LANG=zh_CN.utf-8  
NLS_LANG=.al32utf8
```

2. Restart OC4J using the AVCTL `start_oc4j` command in the Audit Vault Agent shell.

6.6 When to Properly Set the NLS_LANG Environment Variable

The NLS_LANG environment value must be set before performing an AVCTL `start_oc4j` command in the Audit Vault Agent shell and performing an AVCTL `start_agent` command or AVCTL `start_collector` command in the Audit Vault Server shell. When this sequence is followed, the AVCTL `start_collector` command will succeed with a multibyte source name or collector name.

6.7 Traces Can Cause a REDO Collector to Crash

When you turn on a trace for a REDO collector, the collector can crash.

7 Documentation Accessibility

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

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Oracle Audit Vault Release Notes, 10g Release 2 (10.2.2.0.0)
B31587-06

Copyright © 2007, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.