Oracle® Audit Vault

Readme

Patch Set 1 Release 10.2.3.1.0

E10512-05

September 2008

These *Release Notes* contain important information that was not included in the Oracle Audit Vault Patch Set 1 Release 10.2.3.1.0 documentation. For the most current information, refer to updates of this document, which are located at the following Web site:

`http://www.oracle.com/technology/documentation`

This document contains the following sections:

1 Installing the Oracle Audit Vault Patch Set on the Audit Vault Server

This section describes how to install Oracle Audit Vault Patch Set 1 (Release 10.2.3.1.0) on an existing Oracle Audit Vault Server Release 10.2.3.0.0 and Oracle Audit Vault Agent release 10.2.3.0.0 installations. You must install Patch Set 1 (Release 10.2.3.1.0) on the Oracle Audit Vault Server 10.2.3.0.0 before you can upgrade the Agent Release 10.2.3.0.0 installations.

This section contains:

1.1 Step 1: Back Up Oracle Audit Vault

As a best practice, you should back up your Oracle Audit Vault database, the Audit Vault Sever home, and the Audit Vault collection agent home before you begin the upgrade.

Oracle Audit Vault patches cannot be rolled back; therefore you should take precautions to backup the files before the patch is applied until you have tested the patch set.

Back Up the Database

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

1. Sign on to RMAN:

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

2. Issue the following RMAN commands:

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

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

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

Back Up Oracle Audit Vault Server Home

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

Back Up Oracle Audit Vault Collection Agent Home

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

If the Patch Set Apply Fails, You Can Abandon the Upgrade

If the patch set apply does not succeed, you can abandon the upgrade by performing the following steps:

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

2. If you completed the steps in Back Up the Database to back up your database, then restore that backup. Complete the following steps:

   a. Log in to the system as the owner of the Oracle home directory of the previous release.

   b. Sign on to RMAN:

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

   c. Issue the following RMAN commands:

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

1.2 Step 2: Set the NLS_LANG Environment Variable

Set the `NLS_LANG` environment variable to the same value that was used during the base installation of Oracle Audit Vault release 10.2.3.0.0. Otherwise, an ORA-25301 error is returned.

To find this setting, log into SQL*Plus and enter the following command:

```
SQL> SHOW PARAMETER NLS_LANG
```

1.3 Step 3: Stop the Oracle Audit Vault Processes

This section contains:

- Step 3A: Stop All Collectors
- Step 3B: Stop All Agents
- Step 3C: Stop the Oracle Audit Vault Console
- Step 3D: Shut Down the Oracle Audit Vault Database
- Step 3E: Stop the Listener

1.3.1 Step 3A: Stop All Collectors

To stop the collectors:

1. In the server where you installed the Oracle Audit Vault Server, open a shell.
2. Set the appropriate environment variables for the Oracle Audit Vault Server.

   See "Checking and Setting Environment Variables (Linux and UNIX Platforms)" in Chapter 2 of *Oracle Audit Vault Administrator's Guide*.

3. Run the following command:

   ```
   avctl stop_collector -collname collector-name -srcname source_name
   ```

   To find the values that you must enter for this command, in SQL*Plus, query the `ADM_COLLECTORS` data dictionary view.

4. Leave this shell open.

1.3.2 Step 3B: Stop All Agents

To stop the agents:

1. In the shell that you opened in Section 1.3.1, run the following command:

   ```
   avctl stop_agent -agentname agent_name
   ```

   To find the values that you must enter for this command for this command, in SQL*Plus, query the `ADM_AGENTS` data dictionary view.

2. Leave this shell open.

1.3.3 Step 3C: Stop the Oracle Audit Vault Console

To stop the Oracle Audit Vault Console:

1. In the shell that you opened in Section 1.3.1, run the following command:

   ```
   avctl stop_av
   ```

2. In an Oracle RAC environment, run this command on all nodes that include Oracle Audit Vault Server.

3. Leave this shell open.

1.3.4 Step 3D: Shut Down the Oracle Audit Vault Database

From the Oracle Audit Vault Server home, use the following command to shut down the Oracle Audit Vault Database.

```
sqlplus /nolog
SQL> CONNECT SYS/ AS SYSOPER
Enter password: password
Connected.
SQL> SHUTDOWN IMMEDIATE
Database closed.
Database dismounted.
Oracle instance shut down.
SQL> EXIT
```

In an Oracle RAC environment, run the following command from the local node:

```
$ORACLE_HOME/bin/srvctl stop database -d AVdatabase name -q
Connect string:  [/ as sysdba] sys/sys password as sysdba
```

1.3.5 Step 3E: Stop the Listener

From the Oracle Audit Vault Server home, run the following command to stop the listener. The listener name is usually `LISTENER`. You can run the `lsnrctl status` command to determine the name of the listener.

```
$ORACLE_HOME/bin/lsnrctl stop listener_name
```

In an Oracle Real Application Cluster (RAC) environment, run this command on all nodes where Oracle Audit Vault Server is installed.

1.4 Step 4: Install the Oracle Audit Vault Patch Set into the Audit Vault Server Home

Perform the following steps to install the Oracle Audit Vault Patch Set 1 (Release 10.2.3.1.0) in the Oracle Audit Vault Server home. You use the same download executable for both the Audit Vault Server and Audit Vault Agent upgrades.

1. Log in to Oracle*MetaLink* and download Oracle Audit Vault Patch Set 1 (Release 10.2.3.1.0). You can access Oracle*MetaLink* from the following Web site:

   `http://metalink.oracle.com`

2. Start Oracle Universal Installer (OUI) from the directory that contains the `runInstaller` program.

   ```
   cd directory-containing-Oracle-Audit-Vault-Server-Installation-Files
   ./runInstaller
   ```

   Oracle Universal Installer starts. It verifies the operating system version and then presents a summary of the checks it performs.

3. In the Welcome window, click **Installed Products** to display the Inventory window.

   This window indicates the name of the Oracle Audit Vault Server home installed on your computer. For example, it may be named `OraAV10g_home1`.

   Click **Close** to close the Inventory window and return to the Welcome window. Then the click **Next**.

4. In the Specify Home Details window, in the **Name** field, click the down arrow at the end of the field and select the name of the Oracle Audit Vault Server home you found the previous step (Step 3). Then click **Next**.

   For an Oracle RAC installation, a node selection window appears with all fields disabled. This window displays the nodes that this patch set is going to be installed on. Click **Next**.

5. For a first-time installation, go to Step 6.

   For repeat installations only, the Available Product Components window appears, showing a list of product components, some of which have already been installed.

   Click the **Expand All** option to show all the options. Then click the **Select All** option to select all components. To install only certain product components, select the ones you want to install. Click **Next**.

6. In the Summary Page window check the space requirements.

   27 MB of space is required to install Patch Set 1, which includes 13 MB of temporary space. Review each of the items that are about to be installed.

   > **Note:** If the installation fails at the Configuration Assistant step, it might be due to incorrect information entered in Step4 or because the `SYSDBA` privilege was not enabled. See Oracle Audit Vault Server Installation Guide for instructions on enabling the `SYSDBA` privilege.

7. Click **Install**.

   When the installation completes, the Configuration Assistants window appears.

The Configuration Assistants window displays, and the installation continues. When the installation completes, the End of Installation window appears and displays the URL for the Oracle Audit Vault Console. It is the same URL used for the previous Oracle Audit Vault installation.

8. Click **Exit** to exit the Oracle Universal Installer, and then click **Yes** in the confirmation window.

If the Patch Set Upgrade Is Not Successful

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

1. Copy (Restore) the Audit Vault Server Home files back to their original location.
2. If you backed up the database, then restore that backup. Complete the following steps:
   a. Log in to the system as the owner of the Oracle home directory of the previous release.
   b. Sign on to RMAN:

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

   c. Issue the following RMAN commands:

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

1.5 Step 5: Restart the Oracle Audit Vault Server

To restart the Oracle Audit Vault Server:

1. Access the shell that you opened for the Audit Vault Server in Section 1.3.1.
2. Restart the listener.

   ```
   $ORACLE_HOME/bin/lsnrctl start listener_name
   ```

3. Restart Oracle Database.

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

   SQL> STARTUP
   ORACLE instance started
   ```

4. Run the following command:

   ```
   avctl start_av
   ```

2 Installing the Oracle Audit Vault Patch Set on the Audit Vault Agent

This section contains:

- Step 1: Set the NLS_LANG Environment Variable
- Step 2: Stop the Oracle Audit Vault Processes
- Step 3: Install Oracle Audit Vault Patch Set 1 in the Audit Vault Agent Homes
- Step 4: Restart the Oracle Audit Vault Process

2.1 Step 1: Set the NLS_LANG Environment Variable

Set the `NLS_LANG` environment variable to the same value that was used during the base installation of Oracle Audit Vault release 10.2.3.0.0. Otherwise, an ORA-25301 error is returned.

To find this setting, log into SQL*Plus and enter the following command:

```
SQL> SHOW PARAMETER NLS_LANG
```

2.2 Step 2: Stop the Oracle Audit Vault Processes

This section contains:

- Step 2A: Stop All Collectors Running within the Context of the Agent You Are Patching
- Step 2B: Stop the Agent You Are Patching
- Step 2C: Stop the Agent OC4J that Houses the Agent You Are Patching

2.2.1 Step 2A: Stop All Collectors Running within the Context of the Agent You Are Patching

To stop the collectors:

1. Access the shell that you opened in Section 1.3.1.

   If you had closed this shell, then you need to set the appropriate environment variables for the Oracle Audit Vault Server. See "Checking and Setting Environment Variables (Linux and UNIX Platforms)" in Chapter 2 of *Oracle Audit Vault Administrator's Guide*.

2. Run the following command:

   ```
   avctl stop_collector -collname collector-name -srcname source_name
   ```

   To find the values that you must enter for this command, in SQL*Plus, query the `ADM_COLLECTORS` data dictionary view.

3. Leave this shell open.

2.2.2 Step 2B: Stop the Agent You Are Patching

To stop the agents:

1. In the shell that you opened in Section 1.3.1, run the following command:

   ```
   avctl stop_agent -agentname agent_name
   ```

To find the values that you must enter for this command for this command, in SQL*Plus, query the `ADM_AGENTS` data dictionary view.

2. Leave this shell open.

2.2.3 Step 2C: Stop the Agent OC4J that Houses the Agent You Are Patching

To stop the Agent OC4J:

1. Open a shell for the Audit Vault agent.
2. Set the appropriate environment variables for the Oracle Audit Vault agent.

   See "Checking and Setting Environment Variables (Linux and UNIX Platforms)" in Chapter 2 of *Oracle Audit Vault Administrator's Guide*.
3. Run the following command:

   ```
   avctl stop_oc4j
   ```
4. Leave this shell open.

2.3 Step 3: Install Oracle Audit Vault Patch Set 1 in the Audit Vault Agent Homes

Perform the following steps to install the Oracle Audit Vault Patch Set 1 (Release 10.2.3.1.0) in the Oracle Audit Vault Agent home.

1. If you have not done so already, log in to Oracle*MetaLink* and download Oracle Audit Vault Patch Set 1 (Release 10.2.3.1.0). You can access Oracle*MetaLink* from the following Web site:

   `http://metalink.oracle.com`
2. Start Oracle Universal Installer (OUI) from the directory that contains the `runInstaller` program.

   ```
   cd directory-containing-Oracle-Audit-Vault-Agent-Installation-Files
   ./runInstaller
   ```

   Oracle Universal Installer starts. It verifies the operating system version and then presents a summary of the checks it performs.
3. In the Welcome window, click **Installed Products** to display the Inventory window.

   This window indicates the name of the Oracle Audit Vault Agent home installed on your computer. For example, it may be named `OraAV10g_home2` when installed on the same computer as the Oracle Audit Vault Server or `OraAV10g_home1` when installed on a different computer from Oracle Audit Vault Server.

   Click **Close** to close the Inventory window and return to the Welcome window. Then the click **Next**.
4. In the Specify Home Details window, in the **Name** field, click the down arrow at the end of the field and select the name of the Oracle Audit Vault Agent home you determined from the previous step (Step 3)

   Once you select the Oracle Audit Vault Agent home, the **Path** field should display the correct path to the Oracle Audit Vault Agent home. Review the path name. Then click **Next**.
5. For a first time installation, go to Step 6.

For repeat installations only, the Available Product Components window appears, showing a list of product components, some of which have already been installed.

Click the **Expand All** option to show all the options. Then click the **Select All** option. To install only certain components, select the ones you want to install. Then click **Next**.

6. In the Summary Page window, check the space requirements.

   22 MB of space is required to install Patch Set 1, which includes 8 MB of temporary space. Review each of the items that are about to be installed.

7. Click **Install**.

   The **Install** window appears. When the installation completes, the Configuration Assistants window appears and then completes the configuration. Then the end of Installation window appears.

8. Click **Exit** to exit the Oracle Universal Installer, and then click **Yes** in the confirmation window.

If the Patch Upgrade Is Not Successful

If the patch set apply is not successful, to abandon the upgrade, copy (restore) the Audit Vault Collection Agent Home files back to their original location.

2.4 Step 4: Restart the Oracle Audit Vault Process

This section contains:

- Step 4A: Start the Agent OC4j
- Step 4B: Start the Patched Agent
- Step 4C: Start the Collectors that Run in the Patched Agent
- Step 4D: Verify that the Oracle Audit Vault System Components are Running

2.4.1 Step 4A: Start the Agent OC4j

To start the agent OC4J:

1. Access the shell that you opened for the Audit Vault agent in Section 2.2.3.
2. Run the following command:

   ```
   avctl start_oc4j
   ```

3. Close this shell.

2.4.2 Step 4B: Start the Patched Agent

To start the patched agent:

1. In the shell for the Audit Vault Server that you opened in Section 1.3.1, run the following command:

   ```
   avctl start_agent -agentname agent-name
   ```

   To find the values that you must enter for this command for this command, in SQL*Plus, query the `ADM_AGENTS` data dictionary view.

2. Leave this shell open.

2.4.3 Step 4C: Start the Collectors that Run in the Patched Agent

To start the collectors that run in the patched agent:

1. In the shell that you opened in Section 1.3.1, run the following command:

   ```
   avctl start_collector -collname collecctor_name -srcname source_name
   ```

   To find the values that you must enter for this command for this command, in SQL*Plus, query the ADM_COLLECTOR data dictionary view.

2. Leave this shell open.

2.4.4 Step 4D: Verify that the Oracle Audit Vault System Components are Running

To verify that all Oracle Audit Vault components are running and the system is operational:

1. In the shell that you opened in Section 1.3.1, run the following command:

   ```
   avctl show_collector_status -collname collector_name -srcname source_name
   ```

   To find the values that you must enter for this command for this command, in SQL*Plus, query the ADM_COLLECTORS data dictionary view.

2. Close this shell.

3 Postinstallation Tasks

After you install Oracle Audit Vault, check to see if there is a patch set or critical patch update (CPU) available. Before applying any Oracle Audit Vault patch sets, back up your Oracle Audit Vault database, the Oracle Audit Vault Server home, and the Oracle Audit Vault Agent home. See Section 3.1 for more information.

This section describes the following postinstallation tasks if you need to update this patch:

- Back Up and Recovery of Oracle Audit Vault
- Critical Patch Update (CPU)

3.1 Back Up and Recovery of Oracle Audit Vault

Oracle Audit Vault patches cannot be rolled back, therefore you should take precautions to backup the files before the patch is applied until you have tested the patch set. See "Step 1: Back Up Oracle Audit Vault" on page 2 for more information.

3.2 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 10.2.3.1.0 does not include the July 2008 RDBMS CPU for the underlying 10.2.0.3 database, therefore, you need to install this RDBMS CPU. If a later RDBMS CPU is available, then install that. For general information about CPUs, see

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

For specific information about critical patch updates and security alerts, see

http://www.oracle.com/technology/deploy/security/alerts.htm

4 Bugs Fixed in This Release

Table 1 lists bugs that have been fixed for Oracle Audit Vault Patch Set Release 10.2.3.1.

Table 1 Bugs Fixed in Oracle Audit Vault Patch Set Release 10.2.3.1

Bug Number	Description
5874570	PREREQUISITE CHECK ERROR MESSAGE FOR ORACLE HOME NEEDS UPDATE
6902847	ORA-01841 DURING AV WAREHOUSE REFRESH
6918073	AVMSSQLDB ADD_COLLECTOR - BAD ERROR MESSAGE WHEN AGENT NAME IS INVALID
6980485	OSCOLL WRITING GARBAGE VALUE FOR OSAUDIT_CHANNEL_TYPE IN LOG FILE
7000223	DBAUD COLLECTOR COLLECTS INVALID OBJECT FROM DATABASE VAULT
7007428	GLOBAL DEBUGGING AND STACK DUMPING
7008473	OSAUDIT_LOG_LEVEL IS NOT PICK UP FROM SERVER
7017552	DATE FORMAT NEEDS TO BE LOCALIZED
7027265	TIME VALUES IN REPORTS DON'T DISPLAY TIME ZONE
7032087	RECORDS KEEP ON INCREASING FOR DBV COLLECTOR ON 9208 SOURCE
7043940	VALIDATION IN ADVANCED ALERT API WITH COMPOSITE CONDITION
7109942	SOME RECORDS COLLECTED BY SYSLOG COLLECTOR HAVE OLD TIMESTAMP
7151126	SYSLOG COLLECTOR IS DYING INTERMITTENTLY
7164231	TOO MANY CONNECTS/DISCONNECTS TO THE SQL SERVER DATABASE
7164267	POLICY FETCH FAILS WITH INTERNAL ERROR IF SOURCE NOT SETUP ON AGENT
7164835	FAILED TO ADD OSAUD COLLECTOR FOR 9206 NT SOURCE
7172240	AV MULTICOLUMN FGA POLICIES
7218481	DB COLLECTOR DOES NOT START
7235375	DBAUD COLLECTOR CRASHES OCI-22060: ARGUMENT [2] IS AN INVALID
7242648	AUDIT VAULT 10.2.3.0.0 INSTALLATION FAILS INTERMITTENTLY IN SOME ENVIRONMENTS
7245888	NLS:DOWNLOADING ACTIVITY_REPORT.CSV INCLUDED GARBLED WORDS
7256934	OSAUD COLLECTOR NEEDS TO HANDLE THE AUDIT_FILE_DEST PARAMETER CORRECTLY
7311205	AV ALERT DEMO JAR FILE IS MISSING IN INSTALL

Table 1 (Cont.) Bugs Fixed in Oracle Audit Vault Patch Set Release 10.2.3.1

Bug Number	Description
7313180	COLLECTOR REDO_COLLECTOR FOR SOURCE ALREADY EXISTS JAVA.SQL.SQLEXCEPTION:ORA-933
7314693	AV FAILS TO INSTALL UNDER CENTRALIZED TNSNAME CONFIGURATIONS
7317441	JAVA SDK AUTO COMMITS AUDIT RECORDS
7324858	[NLS] OSAUD COLLECTOR CANNOT HANDLE JAPANESE OBJECTNAME
7334760	AVCA FAILING DURING 10.2.3 TO 10.2.3.1 PATCHSET INSTALL
7341268	RESPONSE FILE SHOWS OLD COPYRIGHT YEAR INFORMATION
7342949	LARGE NUMBER OF AUDIT POLICY SETTINGS THROWS VARRAY LIMIT ERRORS
7353816	REDO COLLECTOR DOESN'T COLLECT BEFORE/AFTER VALUES FOR DELETE AND SUP LOG COLUMN
7356241	PLEASE REMOVE REDO COLLECTOR RESTRICTIONS TO FROM 'RECOMMENDED' PARAMETERS
7356965	TYPO IN POLICY SCREENS
7361268	NT AGENT INSTALLER NOT WORKING FOR PATCHSET
7363034	PROVIDE A MECHANISM TO INCREASE AGENT OC4J MAX HEAP SIZE
7364460	INVALID OBJECTS AFTER INSTALLATION OF AV 10.2.3.1 PATCH SET
7368491	AVSYBDB - COMMANDLINE DISABLED IN 10231 BRANCH

5 General Installation Issues

This section contains:

- All Platforms (Single Instance and Oracle RAC)
- All Platforms (RAC) Only
- Linux and UNIX Platforms (Single Instance and Oracle RAC)
- Microsoft Windows Platform

5.1 All Platforms (Single Instance and Oracle RAC)

This section describes known issues and workarounds for single instance and Oracle RAC installations on all platforms.

This section contains:

- The Required Storage Space Calculation Is Not Automatically Updated When Adding Member Disks to the ASM Disk Group
- The Same SYSDBA Password Is Required for Audit Vault and ASM
- Error File Getting Generated During Audit Vault Server Installation
- The -record Option Is Not Supported
- 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
- Manual Cleanup Is Required After Uninstalling the Audit Vault Database
- Audit Vault Server Installer Prints Time Zone on Console When Run for Upgrade
- Deinstalling Upgraded Audit Vault Server Does Not Remove Entry from Oratab File
- Automated Backup Job Not Properly Created with Audit Vault Server Installation
- Errors Appear in Agent Log File After Installing Oracle Audit Vault Agents

5.1.1 The Required Storage Space Calculation Is Not Automatically Updated When Adding Member Disks to the ASM Disk Group

During an Audit Vault Server advanced installation, on the **Configure Automatic Storage Management Configure** page when you select new disks to add from the **Add Member Disks** table, the Required Storage Space area is supposed to automatically adjust the disk sizes displayed to show the amount of required storage space. However, this calculation is not updated.

Workaround: Click the **Change Discovery Path** button and update the discovery path to show the adjusted disk sizes before adding the disks.

This issue is tracked with Oracle bug 5764944.

5.1.2 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:

```
"Supplied ASM SYSDBA password is invalid"
```

Workaround: Provide the same `SYSDBA` password for both ASM and Audit Vault Server.

This issue is tracked with Oracle bug 5845686.

5.1.3 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** window, 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.oiis.OiisVariable.validate(OiisVariable.java:1409)
        at
oracle.sysman.oii.oiis.OiisVariable.validateChildVariables(OiisVariable.java:1836)
        at
oracle.sysman.oii.oiis.OiisVariable.setValue(OiisVariable.java:1124)
        at
oracle.sysman.oii.oiis.OiisVariable.setVariable(OiisVariable.java:2197)
        at
```

```
oracle.sysman.oii.oiis.OiisCompContext.doOperation(OiisCompContext.java:1093)
        at
oracle.sysman.oii.oiif.oiifb.OiifbLinearIterator.iterate(OiifbLinearIterator.java:
147)
        at
oracle.sysman.oii.oiic.OiicCompsWizEngine.doOperation(OiicCompsWizEngine.java:202)
        at
oracle.sysman.oii.oiif.oiifb.OiifbLinearIterator.iterate(OiifbLinearIterator.java:
147)
        at
oracle.sysman.oii.oiic.OiicInstallSession$OiicSelCompsInstall.doOperation(OiicInst
allSession.java:3838)
```

Workaround: You can ignore this error. This exception error 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.

This issue is tracked with Oracle bug 6832669.

5.1.4 The -record Option Is Not Supported

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

Workaround: None.

This issue is tracked with Oracle bug 5841694.

5.1.5 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`.

Workaround: Ensure that you have set the correct value for the `s_dbSid` option in the response file before running the silent installation.

This issue is tracked with Oracle bug 5739374.

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

If you perform a silent installation of the Audit Vault Agent, Oracle Universal 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.

Workaround: Use any of the following methods:

- 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.

This issue is tracked with Oracle bug 5747235.

5.1.7 Silent Installation May Not Report on a Failed DVCA Command

If you perform a silent installation, the `DVCA` command may fail to run. However, the silent installer will report that it ran successfully.

Workaround: Check the installation logs after running silent installation. The log files are located in the *ORACLE_HOME*/cfgtoollogs/oui/installActionsdate_time.log file.

This issue is tracked with Oracle bug 5892119.

5.1.8 Silent Installation Proceeds Even When Variables Are Not Populated

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

On Linux and UNIX systems:

```
./runInstaller -silent -responseFile absolute_path_to_av.rsp_file
```

On Windows systems:

```
setup.exe -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 occured.
Please provide the following files to Oracle Support :'.
```

Workaround: Check the silent installation response file and ensure that you have provided proper input for all the required variables.

This issue is tracked with Oracle bug 5859406.

5.1.9 Manual Cleanup Is Required After Uninstalling the Audit Vault Database

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

Workaround: Manually delete the Audit Vault home directory after you uninstall the Audit Vault database.

This issue is tracked with Oracle bug 5768129.

5.1.10 Audit Vault Server Installer Prints Time Zone on Console When Run for Upgrade

During an Audit Vault server upgrade, Oracle Universal Installer prints the time zone in UTC format in the console in which you invoke `./runInstaller`. This time zone format also appears in the `.out` installation log file.

Workaround: None. You can disregard this message on console and in the `.out` installation log file.

This issue is tracked with Oracle bug 6829132.

5.1.11 Deinstalling Upgraded Audit Vault Server Does Not Remove Entry from Oratab File

If you de-install the Audit Vault Server and even after the de-installation successfully completes, the `/etc/oratab` file still shows the entry for an upgraded Audit Vault server.

Workaround: After the deinstallation completes, manually update the `/etc/oratab` file to remove the corresponding Audit Vault server entry.

This issue is tracked with Oracle bug 6833273.

5.1.12 Automated Backup Job Not Properly Created with Audit Vault Server Installation

When you install Oracle Audit Vault, the automated back-up jobs do not work and fail with a `No such file or directory` error.

Workaround: Use customized back-ups to schedule any back-up jobs.

This issue is tracked with Oracle bug 6844843.

5.1.13 Errors Appear in Agent Log File After Installing Oracle Audit Vault Agents

After you install the Oracle Audit Vault agents, the following validation errors appear in the `$AGENTHOME/av/log/agent_client-0.log` file:

```
2008/04/29 13:03:38 Thread-10 level of detail(low): error invoking validtion
for input=agent2 method=validateName
java.lang.NoClassDefFoundError: javax/servlet/ServletRequest
    at java.lang.Class.getDeclaredMethods0(Native Method)
    at java.lang.Class.privateGetDeclaredMethods(Class.java:1655)
    at java.lang.Class.getMethod0(Class.java:1901)
    at java.lang.Class.getMethod(Class.java:984)
    at oracle.av.util.BeanValidator.invoke(BeanValidator.java:49)
    at oracle.av.util.BeanValidator.validate(BeanValidator.java:97)
    at
@ oracle.av.avca.CommandArguments.validateArguments(CommandArguments.java:170)
    at oracle.av.avca.Avca.startCA(Avca.java:106)
    at oracle.av.avca.Avca.main(Avca.java:448)
2008/04/29 13:03:38 Thread-10 level of detail(low): validationg getAgentName
```

Workaround: You can ignore these errors. The Audit Vault agent should start successfully.

This issue is tracked with Oracle bug 7007105.

5.2 All Platforms (RAC) Only

This section describes known issues and workarounds for Oracle RAC installations on all platforms.

This section contains:

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

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

If you install 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
```

Workaround: Ignore the errors, and after the installation is complete, edit the pfile using the following information:

```
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
```

Afterwards, restart the database.

By default, the PFILE location is in the *ORACLE_HOME*/admin/*db_name*/pfile directory.

This issue is tracked with Oracle bug 6131570.

5.3 Linux and UNIX Platforms (Single Instance and Oracle RAC)

This section describes installation and uninstallation issues in Linux and UNIX platforms for single instance and Oracle Real Application Clusters (RAC) installations.

This section contains:

- Oracle Audit Vault Installation Creates an Error Log File
- Accessing Help Displays a Blank Window

5.3.1 Oracle Audit Vault Installation Creates an Error Log File

If you install Oracle Audit Vault, an error log similar to the following is created:

```
EM Configuration issue.
@ /oracle/av/10.2.3/AV01/av_oh/mycompany.us.oracle.com_ not found.
```

Workaround: None. Oracle Enterprise Manager should be correctly working. You can disregard this error log file.

This issue is tracked with Oracle bug 6780876.

5.3.2 Accessing Help Displays a Blank Window

On AIX 5L Based Systems, if you perform an Audit Vault Server or Agent installation using Simplified Chinese (zh_CN) or Japanese (ja_JP) languages, then accessing help on the installer window will display a blank help window.

Workaround: None.

This issue is tracked with Oracle bug 7016874.

5.4 Microsoft Windows Platform

This section contains:

- Special Message for Security Patch Installation in Audit Vault Agent Upgrade

5.4.1 Special Message for Security Patch Installation in Audit Vault Agent Upgrade

During the upgrade from Oracle Audit Vault release 10.2.2 Audit Vault agent to a release 10.2.3 Audit Vault agent on Microsoft Windows, the following special message appears in the installation log file:

```
ATTENTION                                    **
**
**
** Please note that the Security Patch Installation (Patch Deinstallation) is
**
** not complete until all the Post Installation (Post Deinstallation)
**
** instructions noted in the Readme accompanying this patch, have been
**
** successfully completed.
```

Workaround: Review the readme and other documentation that accompanies the security patch to ensure that you have completed all the required steps.

This issue is tracked with Oracle bug 6979619.

6 General Administration and Configuration Issues

This section contains:

- Audit Vault Source Database Audit Trail Clean-Up Feature Patch
- Garbled Multi-byte User Name Is Displayed on the Login Page
- Subpools for Streams Can Become Too Large
- Need to Enable DV_SECANALYST to Access the DVSYS.AUDIT_TRAIL$ Table
- Time Values in Reports Do Not Display the Time Zone
- Audit Vault Duplicates FGA Policies if Policy Name Is Lower Case
- SQL Server avmssqldb Command Returns Incorrect Warning Message
- AVSYBDB setup Command Failure Results in Help Being Thrown on the Console

6.1 Audit Vault Source Database Audit Trail Clean-Up Feature Patch

New for this release of Oracle Audit Vault is the integration with a new PL/SQL package, `DBMS_AUDIT_MGMT` in Oracle Database. The package provides a set of PL/SQL procedures that you can use to perform audit trail clean-up tasks. In addition to this package, four audit trail clean-up related data dictionary views are provided. This functionality will be available in upcoming versions of Oracle Database. To use this functionality in an existing Oracle 10.2.0.3.0 database, you must download and install Patch 6989148 on the Audit Vault source database.

To download and install Patch 6989148:

1. Log in to Oracle*MetaLink* from the following URL:

   `http://metalink.oracle.com`

2. In Quick Find, select **Patch Number** from the list of categories. In the second Quick Find field, enter `6989148` for the patch number. Then, click **Go**.
3. On the Patch 6989148 page, download and install the patch onto the Audit Vault source database, using the instructions in the provided readme file.

This issue is tracked with Oracle bug 6989148.

6.2 Garbled Multi-byte User Name Is Displayed on the Login Page

If you enter an invalid multi-byte 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 multi-byte user name and then click **Login**.

Workaround: None.

This issue is tracked with Oracle bug 5899718.

6.3 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 an ORA-4031 error.

Workaround: Use one of the following:

- Find what allocations made a particular duration subpool too large and change their durations, for example, from `session` to `cursor` or `execution`.
- Combine the durations into one pool using the following initialization parameter in the `init.ora` initialization file:

  ```
  _enable_shared_pool_durations = false
  ```

  However, be aware that setting this parameter prevents the Streams pool from shrinking.

This issue is tracked with Oracle bug 5919096.

6.4 Need to Enable DV_SECANALYST to Access the DVSYS.AUDIT_TRAIL$ Table

Audit Vault extracts the Oracle Database Vault audit trail records by using the `DV_ADMIN` or `DV_OWNER` role to read the contents of the `DVSYS.AUDIT_TRAIL$` table for Oracle Database 11*g* Release 1 (11.1). For better security, Audit Vault should be able to use the `DV_SECANALYST` role to read the `DVSYS.AUDIT_TRAIL$` table.

Workaround:

1. Log in to SQL*Plus as a user who has been granted the `DV_OWNER` role.

2. Grant the DV_ADMIN role to the user account that was created on the source database for Audit Vault.

This issue is tracked with Oracle bug 7022650.

6.5 Time Values in Reports Do Not Display the Time Zone

The time values displayed in the Oracle Audit Vault reports do not display the time zone. Oracle Audit Vault bases the time zone value the TZ environment variable setting on Linux32 (other platforms vary) that was in place when you start the Audit Vault database. The Home page and all other pages in the Audit Vault Console explicitly use Coordinated Universal Time (UTC) and display the time zone. Therefore, if you start the Audit Vault database in a time zone other than UTC, the timestamps between different parts of the Audit Vault Console are different.

When you install Oracle Audit Vault, Oracle Universal Installer starts the database in UTC. If you then shut down and subsequently restart Audit Vault, time values in the reports can be different. As a result, you cannot determine which time zone in which the report was generated.

Workaround: Always start Oracle Audit Vault using the UTC. For example:

1. In a shell window, set the TZ environment variable to UTC.

```
setenv TZ UTC
```

2. Start the listener.

```
lsnrctl start
```

3. Start the Audit Vault database.

```
sqlplus sys/as sysoper
Enter password: password
Connected.
SQL> startup
```

4. Start the Audit Vault console.

```
avctl start_av
```

This issue is tracked with Oracle bug 7027265.

6.6 Audit Vault Duplicates FGA Policies if Policy Name Is Lower Case

If an auditor creates a fine-grained audit policy and then specifies the policy name using lower-case letters, then Oracle Audit Vault creates a duplicate fine-grained audit policy. The duplicate policy uses upper-case letters for the policy name.

Workaround: Use one of the following solutions:

- Choose a different policy name.
- Delete the fine-grained audit policy and then create a new one having same policy name with previous fine-grained audit policy.

This issue is tracked with Oracle bug 6975309.

6.7 SQL Server avmssqldb Command Returns Incorrect Warning Message

When you run the `avmssqldb verify` or `avmssqldb setup` command, and if the source user you specify does not have `SYSADMIN` privilege, then the `avmssqldb` command returns an error message claiming that you need the `SYSADMIN` privilege.

This error message is correct for SQL Server 2000 but incorrect for SQL Server 2005. For SQL Server 2005, you do not need the `SYSADMIN` privilege.

Workaround: You can ignore this message. The command succeeds in spite of the error message.

This issue is tracked with Oracle bug 7122168.

6.8 AVSYBDB setup Command Failure Results in Help Being Thrown on the Console

When configuring a Sybase ASE source database, if you incorrectly run the `AVSYBDB setup` command, such as specifying an incorrect `-srcname` value, Oracle Audit Vault displays help output on the console.

Workaround: None.

This issue is tracked with Oracle bug 7037146.

7 Source Configuration Issues

This section contains:

- Long Source Database Name Is Garbled in Top Five Audit Sources by Number of Alerts Graph
- Sybase ASE and SQL Server Source and Audit Vault Event Times Differ

7.1 Long Source Database Name Is Garbled in Top Five Audit Sources by Number of Alerts Graph

If the source database has a long name and appears on the Y-axis of the graph Top Five Audit Sources by Number of Alerts, the graph is squeezed to the point that the X-axis becomes one dimensional and does not show the two-dimensional aspect of the graph.

Workaround: Create a reasonably short source name, about 15 characters long, using the `-srcname` *`srcname`* argument when you add the source to Oracle Audit Vault.

This issue is tracked with Oracle bug 6837441.

7.2 Sybase ASE and SQL Server Source and Audit Vault Event Times Differ

The source database event time and Audit Vault event times differ for Sybase ASE and SQL Server. This time difference is small, however.

Table 2 demonstrates this problem. In the values listed in the Audit Vault Timestamp column, there is a trailing, recurring last digit followed by zeros. For some cases, the leading zero is dropped. This could pose problems because the `event_time` value is usually used as a basis for co-relating events.

Table 2 Timestamp Differences Between the Source and Audit Vault Event Times

Source DB Timestamp	Audit Vault Timestamp
2008-03-13 15:27:44.773	2008-03-13 15:27:44.773333000
2008-03-13 15:28:48.056	2008-03-13 15:28:48.56667000
2008-03-13 15:28:55.103	2008-03-13 15:28:55.103333000
2008-03-13 15:28:57.76	2008-03-13 15:28:57.760000000
2008-03-13 15:29:00.086	2008-03-13 15:29:0.86667000
2008-03-13 15:29:52.883	2008-03-13 15:29:52.883333000

Workaround: None.

This issue is tracked with Oracle bug 6890264.

8 Collector Configuration Issues

This section contains:

- Collector Startup Can Be Slow
- SQL Server Collector Status Not Updated
- Invalid Path Error Appears in SQL Server Collector Log File
- Audit Records from SYSLOG Have the Wrong Date
- XML and SYSLOG Audit Files Are Garbled When Collected by the OSAUD Collector
- SYBDB Collector Hangs if the sybsecurity Database Is Dropped With the Collector Running

8.1 Collector Startup Can Be Slow

After several restarts, a collector can take a while to start. In most cases, when the `avctl start_collector` command is successful, the `avctl show_collector_status` command and Audit Vault Console 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.

Workaround: Wait until the startup completes. Operations should be normal after the collector has finished starting. Before re-performing a collector status query, wait a bit longer. The collector status will eventually indicate a running state.

This issue is tracked with Oracle bug 5937597.

8.2 SQL Server Collector Status Not Updated

If you run the Audit Vault SQL Server `avmssqldb` command on the source database, and then try to start the SQL Server collector, the command succeeds but the collector status remains unchanged. It should show a status indicating that the SQL Server collector has started. To find if this error has occurred, check the `$ORACLE_HOME/av/log` directory of the Agent and see if the SQL Collector log file has a Generic Wallet Error. If this wallet error is present, then it is most likely this bug.

Typically, you follow these steps:

1. On the Audit Vault Server side, you add the source and collectors as follows:

   ```
   avmssqldb add_source -srcname src_name ...
   avmssqldb add_collector -collname collector_name ...
   ```

2. On the Audit Vault Agent side, you run the following set-up command:

   ```
   avmssqldb setup -srcname src_name
   ```

3. Then, on the Audit Vault Server side, you run these commands:

   ```
   avctl start_collector -srcname src_name -collname collector_name
   avctl show_collector_status -srcname src_name -collname collector_name
   ```

If you omit Step 2, then no error displays when you run the `avctl start_collector` command in Step 3. When you run the `avctl show_collector_status` command next, then the status displays a `not running` message.

Workaround: Run the `avmssqldb setup` command on the agent, and then restart the collector.

This issue is tracked with Oracle bug 7010699.

8.3 Invalid Path Error Appears in SQL Server Collector Log File

The SQL Server collector log file erroneously states that the directory path specified by the `C2_TRACE_FILEPATH` attribute setting is incorrect.

Workaround: Specify the complete file name, with the wildcard asterisk (`*`) instead of `.trc` in the `C2_TRACE_FILEPATH` parameter. For example, if the file name is `C:\MyTrace.trc`, then specify the value `C:\MyTrace*`.

This issue is tracked with Oracle bug 7030424.

8.4 Audit Records from SYSLOG Have the Wrong Date

Some records collected by the OSAUD collector from SYSLOG have the Event Time field set to a value one year in the past. This happens because of a bug in Oracle Audit Vault and because the SYSLOG file format does not contain year and time zone information for the timestamp. As a result, the SYSLOG audit records do not record the debug level. The records are sent to the Audit Vault repository, but the activity graph does not display the records. There are no errors in the OS collector log. This problem occurs if you set the `AUDIT_TRAIL` initialization parameter to `OS` and the `AUDIT_SYSLOG_LEVEL` to `syslog.info` in the source database. It does not occur for the DB collector, REDO collector, OS Collector (XML), or OS Collector (Aud).

Workaround: None.

This issue is tracked in Oracle bug 7109942.

8.5 XML and SYSLOG Audit Files Are Garbled When Collected by the OSAUD Collector

Multi-bye words collected by the XML collector and SYSLOG audit files are garbled if you do the following in the source database:

- **XML:** If the source database is configured to send the audit trail to `XML` or `XML, EXTENDED` audit files, and the audit trail contains multi-byte characters in non-UTF8 encodings, those characters are garbled in the Audit Vault repository.
- **SYSLOG:** If the source database is configured to send the audit trail to SYSLOG, and the audit trail contains multi-byte characters in non-UTF8 encodings, those characters are garbled in the Audit Vault repository.

Afterwards, data in the Audit Vault Repository is garbled. This problem occurs even if you start the agent and collector with the correct `NLS_LANG` set.

Workaround: None.

This issue is tracked with Oracle bug 7045602.

8.6 SYBDB Collector Hangs if the sybsecurity Database Is Dropped With the Collector Running

Deleting the Sybase ASE `sybsecurity` database results in the following message in the Collector log:

```
sysaudits_01 not found. Specify owner.objectname or use sp_help to check whether
the object exists (sp_help may produce lots of output)
```

However, after you add the Sybsecurity database and then generate audit records, the Sybase collector fails to collect them. The collector status shows that it is running, but there is no subsequent data in Oracle Audit Vault.

Workaround: Shut down the SYBDB collector before dropping the `sybsecurity` database and then restart the SYBDB collect after the `sybsecurity` database has been recreated. Alternately, if the database is indeed dropped while the collector is running, stop the collector using the `avctl stop_collector` command and then restart the collector.

This issue is tracked with Oracle bug 7037266.

9 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, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Oracle Audit Vault Release Notes, Patch Set 1 Release 10.2.3.1.0
E10512-05