Oracle® Audit Vault

Server Installation Guide

Release 10.2.3.2 for Linux x86

E14458-13

February 2012

ORACLE®

Oracle Audit Vault Server Installation Guide, Release 10.2.3.2 for Linux x86

E14458-13

Primary Authors: Rod Ward, Tanaya Bhattacharjee

Contributing Authors: Tammy Bednar, Janet Blowney, Robert Chang, Pat Huey, Sumit Jeloka, Nilima Kapoor, K Karun, Deborah Owens

Contributors: Alan Galbreath, Luann Ho, Donna Keesling, Sarma Namuduri, Mohammed Yunus Qureshi, Trivikrama Samudrala, Vipul Shah, Martin Widjaja

Contents

3 Installing the Oracle Audit Vault Server

4 Upgrading Oracle Audit Vault Server

5 Removing the Oracle Audit Vault Server Software

Index

List of Tables

Preface

Oracle Audit Vault Server Installation Guide for Linux x86 explains how to prepare for, install, and configure Oracle Audit Vault Server (Audit Vault Server). It provides specific instructions for the operating system and Oracle software technology components that the Audit Vault Server requires.

Audience

This document is intended for Oracle database administrator's (DBAs) and system administrators and those who are involved in the installation of Oracle Audit Vault and its related components.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- *Oracle Audit Vault Release Notes*
- *Oracle Audit Vault Collection Agent Installation Guide*
- *Oracle Audit Vault Licensing Information*
- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*

- *Oracle Database Vault Installation Guide for Linux x86*
- *Oracle Database Vault Administrator's Guide*

To download free release notes, installation documentation, updated versions of this guide, white papers, or other collateral, visit the Oracle Technology Network (OTN). You must register online before using OTN. Registration is free. You can register at

http://www.oracle.com/technetwork/community/join/overview/

If you already have a user name and password for OTN, then you can go directly to the Oracle Audit Vault documentation section of the OTN Web site at

http://www.oracle.com/technetwork/database/audit-vault/documentation/auditvault-091754.html

For OTN information specific to Oracle Audit Vault, visit

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

For the Oracle Audit Vault Discussion Forums, visit

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

Conventions

The following text conventions are used in this document:

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

1

Oracle Audit Vault Server Installation Overview

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

This chapter provides an overview of the Oracle Audit Vault Server (Audit Vault Server) installation process. This chapter includes the following sections:

1.1 Deploying Oracle Audit Vault Server

It is recommended that you install Audit Vault Server on its own host computer or a host that contains other repository databases such as Enterprise Manager Grid Control or the Oracle Recovery Manager (RMAN) repository database. This enables Oracle Audit Vault to have high availability to these other databases. For scalability, the Audit Vault Server can implement Real Applications Cluster (Oracle RAC) and Data Guard for disaster recovery.

1.2 Oracle Audit Vault Installation Components

Oracle Audit Vault software installation consists of two parts:

- Audit Vault Server installation that can be either:
  - Single Instance installation
  - Clustered using an Oracle Real Application Clusters (Oracle RAC) installation
- Oracle Audit Vault collection agent installation (see *Oracle Audit Vault Collection Agent Installation Guide*)

1.3 Oracle Audit Vault Installation Methods

You can choose different installation methods to install Audit Vault Server, as follows:

- Interactive Installation Methods
- Automated Installation Methods Using Response Files

1.3.1 Interactive Installation Methods

When you use the interactive method to install Oracle Audit Vault to perform a Basic, Advanced, or Upgrade installation, Oracle Universal Installer displays a series of screens that enable you to specify all of the required information to install the Oracle Audit Vault software.

1.3.2 Automated Installation Methods Using Response Files

Oracle Audit Vault provides a response file template for Audit Vault Server (`av.rsp`) and one for an upgrade installation (`upgrade_av.rsp`). These response template files can be found in the *`AV-installer-location`*`/response` directory on the Audit Vault Server installation media.

When you start Oracle Universal Installer and specify a response file, you can automate all of the Audit Vault Server installation. These automated installation methods are useful if you need to perform multiple installations on similarly configured systems or if the system where you want to install the software does not have X Window system software installed.

For Audit Vault Server, Oracle Universal Installer can run in silent (noninteractive) mode. For silent mode, specify both the `-silent` and `-responseFile` options followed by the path of the response file on the command line when you invoke Oracle Universal Installer. For example:

```
./runInstaller -silent -responseFile path_of_response_file
```

Oracle Universal Installer runs in silent mode if you use a response file that specifies all required information. None of the Oracle Universal Installer screens are displayed, and all interaction (standard output and error messages) and installation logs appear on the command line.

Prepare the response file by entering values for all parameters that are missing in the first part of the response file, then save the file. Do not edit any values in the second part of either response file.

See Section 3.5 for information about performing an Audit Vault Server silent installation and Section 4.4 for information about performing a silent upgrade installation.

Note: The basic installation is not supported in silent mode. Silent installation is only supported for the advanced installation.

1.4 Audit Vault Server Installation

The Audit Vault Server installation consists of three options:

- Upgrade Existing Audit Vault Server Home – detects upgradable Audit Vault Server homes on the system and enables the upgrade option to the current release. Perform an upgrade on the selected upgradable Audit Vault Server home detected on the system.
- Basic installation – simplifies the installation process and prompts for a minimal set of inputs from the user to perform a full installation. An Oracle RAC

installation is not supported through this option; only a single instance installation is supported.

- Advanced installation – offers the user more control and options for the installation process, including storage options and backup options. This option supports the installation of Audit Vault Server on a cluster and as a single instance.

Communication at the management level between the Audit Vault Server and the Oracle Audit Vault collection agent can be secured after the installation is complete. This is done as part of the postinstallation configuration, in which SSL is configured for the mutual authentication between the Oracle Audit Vault management service on the server side and each collection agent over HTTPS.

After you check the requirements described in Section 1.5, the general steps to install Audit Vault Server include these tasks:

1. Run Oracle Universal Installer to perform Audit Vault Server installation.
2. Run postinstallation and configuration tasks using AVCA.

1.5 Installation Considerations

This section contains information that you should consider before deciding how to install this product. It includes contains the following topics:

- Hardware and Software Considerations
- Multiple Oracle Homes

1.5.1 Hardware and Software Considerations

The platform-specific hardware and software requirements included in this installation guide were current at the time this guide was published. However, because new platforms and operating system versions might be certified after this guide is published, review the certification matrix on the My Oracle Support (formerly Oracle*MetaLink*) Web site for the most up-to-date list of certified hardware platforms and operating system versions. The My Oracle Support Web site is available at

`https://support.oracle.com`

1.5.2 Multiple Oracle Homes

This product supports multiple Oracle homes. This means you can install this release of the software more than once on the same system, in different Oracle home directories. See Section 2.5.3 for more information.

2

Oracle Audit Vault Server Preinstallation Requirements

This chapter describes the following Oracle Audit Vault Server (Audit Vault Server) preinstallation requirements. This chapter includes the following sections:

2.1 Becoming Familiar with the Features of Oracle Audit Vault

To plan the installation process, you must be familiar with the features of Oracle Audit Vault. *Oracle Audit Vault Administrator's Guide* discusses the basic features of Oracle Audit Vault.

2.2 Logging In to the System as the root User

Before you install the Oracle software, you must complete the tasks described in this chapter as the `root` user. Log in to your system as the `root` user.

2.3 Checking the Hardware Requirements

The system must meet the following minimum hardware requirements:

- At least 1024 MB of available physical memory (RAM)
- The following table gives the relationship between the available RAM and the required swap space:

Available RAM	Swap Space Required
Between 1024 MB and 2048 MB	1.5 times the size of RAM
Between 2049 MB and 8192 MB	Equal to the size of RAM
More than 8192 MB	0.75 times the size of RAM

- Audit Vault Server installation disk space requirements
  - 2.6 GB of disk space for the Audit Vault Server software files in the Oracle base directory
  - 1.6 GB of additional disk space for the Audit Vault Server database files in the Oracle base directory. This is only if the database storage option is on the file system. For other storage options, such as Automatic Storage Management (ASM), the database files will be stored elsewhere. Also, this 1.6 GB of disk space is only the starting size. Consider the future growth of the database size, especially as the server collects more and more audit data.

To ensure that the system meets these requirements, perform the following tasks:

1. To determine the physical RAM size, enter the following command:

   ```
   # grep MemTotal /proc/meminfo
   ```

   If the size of the physical RAM installed in the system is less than the required size, then you must install more memory before continuing.

2. To determine the size of the configured swap space, enter the following command:

   ```
   # grep SwapTotal /proc/meminfo
   ```

   If necessary, see your operating system documentation for information about how to configure additional swap space.

3. To determine the available RAM and swap space, enter the following command:

   ```
   # free
   ```

   Note: Oracle recommends that you take multiple readings for the available RAM and swap space before determining a value. This is because the available RAM and swap space keep changing depending on the user interactions with the computer.

4. To determine the amount of disk space available in the `/tmp` directory, enter the following command:

   ```
   # df -k /tmp
   ```

   If there is less than 400 MB of disk space available in the `/tmp` directory, then complete one of the following steps:

   - Delete unnecessary files from the `/tmp` directory to meet the disk space requirement.
   - Set the `TEMP` and `TMPDIR` environment variables when setting the environment of the `oracle` users.
   - Extend the file system that contains the `/tmp` directory. If necessary, contact your system administrator for information about extending file systems.

5. To determine the amount of free disk space on the system, enter the following command:

```
# df -k
```

6. To determine whether the system architecture can run the software, enter the following command:

```
# grep "model name" /proc/cpuinfo
```

Note: This command displays the processor type. Verify that the processor architecture matches the Oracle software release that you want to install. If you do not see the expected output, then you cannot install the software on this system.

2.4 Checking the Operating System Requirements

If Oracle Validated RPM is available for your distribution and installed, the RPM downloads the minimum number of packages required to run Oracle Clusterware and Oracle Database. The RPM also sets and verifies system parameters based on recommendations from the Oracle Validated Configurations program.

Unbreakable Linux Network (ULN) customers can obtain the Oracle Validated RPM by using up2date. If you are not a ULN customer, and you are running Red Hat Enterprise Linux or Oracle Linux, then you can obtain the Oracle Validated RPM at the following URLs:

Oracle Linux 4: http://oss.oracle.com/el4/oracle-validated/

Oracle Linux 5: http://oss.oracle.com/el5/oracle-validated/

If you are not a member of ULN or RHN (Red Hat support network) and you are an Oracle support customer, then you can download instructions to configure a script that replicates Oracle Validated RPM package downloads at the following URL:

https://support.oracle.com

Search for "minimal Linux"

If Oracle Validated RPM is not installed and depending on the products that you intend to install, verify that the software is installed on the system listed in Table 2–1. The procedure following Table 2–1 describes how to verify whether these requirements are addressed.

Note: Oracle Universal Installer checks your system to verify that it meets the listed requirements. To ensure that your system passes these checks, verify the requirements before you start Oracle Universal Installer.

The platform-specific hardware and software requirements included in this installation guide were current at the time this guide was published. However, because new platforms and operating system versions might be certified after this guide is published, review the certification matrix on the My Oracle Support (formerly Oracle*MetaLink*) Web site for the most up-to-date list of certified hardware platforms and operating system versions. The My Oracle Support Web site is available at

https://support.oracle.com

Table 2–1 Operating System, Kernel Version, and Packages Requirements

Item	Requirement
Operating system	One of the following operating system versions: ■ Oracle Enterprise Linux 4/Oracle VM ■ Oracle Enterprise Linux 5/Oracle VM ■ Red Hat Enterprise Linux AS/ES 3.0 (Update 3 or later) ■ Red Hat Enterprise Linux AS/ES 4.0/Oracle VM ■ Red Hat Enterprise Linux AS/ES 5.0/Oracle VM ■ SUSE Linux Enterprise Server 9.0 ■ SUSE Linux Enterprise Server 10.0 ■ SUSE Linux Enterprise Server 11.0 The operating system requirements are the same as those for Oracle Database 10*g* release 2. If Oracle Database 10*g* release 2 is installed, then your system automatically meets these requirements.
Kernel version	The system must be running the following kernel version (or a later version): **Red Hat Enterprise Linux AS/ES 3.0:** 2.4.21-27.EL **Note:** This is the default kernel version. **Red Hat Enterprise Linux AS/ES 4.0/Oracle VM, Oracle Enterprise Linux 4/Oracle VM:** 2.6.9-5.0.5.EL **Red Hat Enterprise Linux AS/ES 5.0/Oracle VM, Oracle Enterprise Linux 5/Oracle VM:** 2.6.9 **SUSE Linux Enterprise Server 9.0:** 2.6.5-7.97 **SUSE Linux Enterprise Server 10.0:** 2.6.9 **SUSE Linux Enterprise Server 11.0:** 2.6.27.19 The kernel version requirements are the same as those for Oracle Database 10*g* release 2. If Oracle Database 10*g* release 2 is installed, then your system automatically meets the kernel version requirements.

Table 2–1 (Cont.) Operating System, Kernel Version, and Packages Requirements

Item	Requirement
Packages	The following packages (or later versions) must be installed: **Red Hat Enterprise Linux 3.0:** make-3.79.1 binutils-2.14 gcc-3.2.3-34 glibc-2.3.2-95.20 compat-db-4.0.14-5 compat-gcc-7.3-2.96.128 compat-gcc-c++-7.3-2.96.128 compat-libstdc++-7.3-2.96.128 compat-libstdc++-devel-7.3-2.96.128 openmotif21-2.1.30-8 setarch-1.3-1 libaio-0.3.96 **Red Hat Enterprise Linux 4.0, Oracle Enterprise Linux 4:** binutils-2.15.92.0.2-13.EL4 compat-libstdc++296-2.96-132.7.2 compat-db-4.1.25-9 control-center-2.8.0-12 gcc-3.4.3-22.1.EL4 gcc-c++-3.4.3-22.1.EL44 glibc-2.3.4-2.9 glibc-common-2.3.4-2.9 gnome-libs-1.4.1.2.90-44.1 libstdc++-3.4.3-22.1 libstdc++-devel-3.4.3-22.1 make-3.80-5 numactl-0.6.4.i386 pdksh-5.2.14-30 sysstat-5.0.5-1 xscreensaver-4.18-5.rhel4.2 setarch-1.6-1 **Red Hat Enterprise Linux 5.0, Oracle Enterprise Linux 5:** binutils-2.17.50.0.6-2.el5 compat-libstdc++-33-3.2.3-61 elfutils-libelf-0.125-3.el5 elfutils-libelf-devel-0.125 gcc-4.1.1-52 gcc-c++-4.1.1-52 glibc-2.5-12 glibc-common-2.5-12 glibc-devel-2.5-12 glibc-headers-2.5-12 libaio-0.3.106 libaio-devel-0.3.106 libgcc-4.1.1-52 libstdc++-4.1.1 libstdc++-devel-4.1.1-52.e15 make-3.81-1.1 numactl-devel-0.9.8.i386 sysstat-7.0.0 unixODBC-2.2.11 unixODBC-devel-2.2.11

Table 2–1 (Cont.) Operating System, Kernel Version, and Packages Requirements

Item	Requirement
Packages	The following packages (or later versions) must be installed: **SUSE Linux Enterprise Server 9:** binutils-2.15.90.0.1.1-32.5 gcc-3.3.3-43.24 gcc-c++-3.3.3-43.24 glibc-2.3.3-98.28 gnome-libs-1.4.1.7-671.1 libstdc++-3.3.3-43.24 libstdc++-devel-3.3.3-43.24 make-3.80-184.1 pdksh-5.2.14-780.1 sysstat-5.0.1-35.1 xscreensaver-4.16-2.6 **SUSE Linux Enterprise Server 10:** binutils-2.16.91.0.5 compat-libstdc++-5.0.7 gcc-4.1.0 glibc-2.4-31.63 glibc-devel-2.4-31.63 ksh-93r-12.9 libaio-0.3.104 libaio-devel-0.3.104 libelf-0.8.5 libgcc-4.1.0 libstdc++-4.1.0 libstdc++-devel-4.1.0 make-3.80 sysstat-6.0.2 unixODBC-2.2.11 unixODBC-devel-2.2.11 **SUSE Linux Enterprise Server 11:** binutils-2.19 gcc-4.3 gcc-c++-4.3 glibc-2.9 glibc-devel-2.9 ksh-93t libaio-0.3.104 libaio-devel-0.3.104 libgcc43-4.3.3_20081022 libstdc++33-3.3.3 libstdc++43-4.3.3_20081022 libstdc++43-devel-4.3.3_20081022 libstdc++-devel-4.3 make-3.81 sysstat-8.1.5
Packages	The package requirements are the same as those for Oracle Database 10*g* release 2. If Oracle Database 10*g* release 2 is installed, then your system automatically meets the package requirements.

To ensure that the system meets these requirements, perform the following tasks:

1. To determine which distribution and version of Linux is installed, enter the following command:

```
# cat /etc/issue
```

> **Note:** Only the distributions and versions listed in the previous table are supported. Do not install the software on other versions of Linux.

2. To determine whether the required kernel is installed, enter the following command:

```
# uname -r
```

For example, the following output appears for Red Hat Enterprise Linux 3.0:

```
2.4.21-15.EL
```

In this example, the output shows the kernel version (`2.4.21`) and errata level (`15.EL`) on the system.

If the kernel version does not meet the requirement specified in Table 2–1, then contact your operating system vendor for information about obtaining and installing kernel updates.

3. To determine whether the required packages are installed, enter commands similar to the following:

```
# rpm -q package_name
```

If a package is not installed, then install it from your Linux distribution media or download the required package version from the Web site of your Linux vendor.

2.5 Checking the Network Setup

Typically, the computer on which you want to install Oracle Audit Vault is connected to the network, has local storage to contain the Oracle Audit Vault installation, has a display monitor, and has a CD-ROM or DVD drive.

This section describes how to install Audit Vault Server on computers that do not meet the typical scenario. It covers the following cases:

- Configuring Name Resolution
- Installing on DHCP Computers
- Installing on Multi-homed Computers
- Installing on Computers with Multiple Aliases

2.5.1 Configuring Name Resolution

When you run Oracle Universal Installer, an error might occur if name resolution is not set up. To avoid this error, before you begin an installation, you must ensure that host names are resolved only through the `/etc/hosts` file.

To ensure that host names are resolved only through the `/etc/hosts` file:

1. Verify that the `/etc/hosts` file is used for name resolution. You can do this by checking the hosts file entry in the `nsswitch.conf` file as follows:

```
# cat /etc/nsswitch.conf | grep hosts
```

The output of this command should contain an entry for files.

2. Verify that the host name has been set by using the `hostname` command as follows:

```
# hostname
```

The output of this command should be similar to the following:

```
myhost.us.example.com
```

3. Verify that the domain name has not been set dynamically by using the `domainname` command as follows:

```
# domainname
```

This command should not return any results.

4. Verify that the hosts file contains the fully qualified host name by using the following command:

```
# cat /etc/hosts | grep `eval hostname`
```

The output of this command should contain an entry for the fully qualified host name and for the `localhost`.

For example:

```
192.0.2.1         myhost.us.example.com     myhost
127.0.0.1         localhost                 localhost.localdomain
```

If the hosts file does not contain the fully qualified host name, then open the file and make the required changes in it.

2.5.2 Installing on DHCP Computers

Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses on a network. Dynamic addressing enables a computer to have a different IP address each time it connects to the network. In some cases, the IP address can change while the computer is still connected. You can have a mixture of static and dynamic IP addressing in a DHCP system.

In a DHCP setup, the software tracks IP addresses, which simplifies network administration. This lets you add a new computer to the network without having to manually assign that computer a unique IP address.

Do not install Audit Vault Server in an environment where the IP addresses of the Audit Vault Server or the Oracle Audit Vault collection agent can change. If your environment uses DHCP, ensure that all Oracle Audit Vault systems use static IP addresses.

2.5.3 Installing on Multi-homed Computers

You can install Audit Vault Server on a multi-homed computer. A multi-homed computer has multiple network cards, which in turn, allows it to have multiple IP addresses. Each IP address is associated with a host name. In addition, you can set up aliases for the host name. By default, Oracle Universal Installer uses the `ORACLE_HOSTNAME` environment variable setting to find the host name. If the `ORACLE_HOSTNAME` environment variable is not set and you are installing Audit Vault Server

on a computer that has multiple network cards, then Oracle Universal Installer determines the host name by using the first entry in the `/etc/hosts` file.

Clients must be able to access the computer either by using this host name or by using aliases for this host name. To verify this, ping the host name from the client computers using the short name (host name only) and the full name (host name and domain name). Both tests must be successful.

Setting the ORACLE_HOSTNAME Environment Variable

Use the following procedure to set the `ORACLE_HOSTNAME` environment variable.

For example, if the fully qualified host name is `myhost.us.example.com`, then enter one of the following commands:

Bourne, Bash, or Korn shell:

```
$ ORACLE_HOSTNAME=myhost.us.example.com
$ export ORACLE_HOSTNAME
```

C shell:

```
% setenv ORACLE_HOSTNAME myhost.us.example.com
```

2.5.4 Installing on Computers with Multiple Aliases

A computer with multiple aliases is registered with the naming service under a single IP address. The naming service resolves all of those aliases to the same computer. Before installing Audit Vault Server on a computer with multiple aliases, set the `ORACLE_HOSTNAME` environment variable to the computer whose host name you want to use.

2.6 Creating the Required Operating System Groups and Users

When it is installed, Oracle Validated Configuration RPM creates an oracle software owner (oracle), and the OSDBA group (dba) and Oracle Inventory group (oinstall), and completes most tasks discussed in this section. The RPM also updates `sysctl.conf` settings, system startup parameters, user limits, and driver parameters to values tested for performance. See Section 2.6.5 to verify that the unprivileged user `nobody` exists. See Section 2.4 for more information about Oracle Validated Configuration RPM.

If Oracle Validated Configuration RPM is not installed, then depending on whether you are installing Oracle software for the first time on this system and the products that you are installing, you may need to create several operating system groups and users. Log in to your system as the `root` user before you attempt to create these operating system groups and users.

If you are installing Audit Vault Server, it requires the following operating system groups and user:

- The OSDBA group (`dba`)

  You must create this group the first time you install Audit Vault Server software on the system. It identifies operating system user accounts that have database administrative privileges (the `SYSDBA` privilege). The default name for this group is `dba`.

- The OSOPER group (`oper`)

This is an optional group. Create this group if you want a separate group of operating system users to have a limited set of administrative privileges (the SYSOPER privilege). By default, members of the OSDBA group also have the SYSOPER privilege.

- An unprivileged user

  Verify that the unprivileged user nobody exists on the system. The nobody user must own the external jobs (extjob) executable after the installation.

The following operating system group and user are required for all installations:

- The Oracle Inventory group (oinstall)

  You must create this group the first time you install Oracle software on the system. The usual name chosen for this group is oinstall. This group owns the Oracle inventory, which is a catalog of all Oracle software installed on the system.

  Note: If Oracle software is already installed on the system, then the existing Oracle Inventory group must be the primary group of the operating system user that you use to install new Oracle software. The following topics describe how to identify an existing Oracle Inventory group.

- The Oracle software owner user (typically, oracle)

  You must create this user the first time you install Oracle software on the system. This user owns all software installed during the installation. This user must have the Oracle Inventory group as its primary group. It must also have the OSDBA and OSOPER groups as secondary groups.

  Note: In Oracle documentation, this user is referred to as the oracle user.

All installations of Oracle software on the system require a single Oracle Inventory group. After the first installation of Oracle software, you must use the same Oracle Inventory group for all subsequent Oracle software installations on that system. However, you can choose to create different Oracle software owner users, OSDBA groups, and OSOPER groups (other than oracle, dba, and oper) for separate installations. By using different groups for different installations, members of these different groups have DBA privileges only on the associated databases, rather than on all databases on the system.

See Also: *Oracle Database Administrator's Guide* for more information about the OSDBA group and the SYSDBA and SYSOPER privileges

Note: The following topics describe how to create local users and groups. As an alternative to creating local users and groups, you could create the appropriate users and groups in a directory service, for example, Network Information Services (NIS). For information about using directory services, contact your system administrator or see your operating system documentation.

The following topics describe how to create the required operating system users and groups:

- Creating the Oracle Inventory Group
- Creating the OSDBA Group
- Creating an OSOPER Group (Optional)
- Creating the Oracle Software Owner User

2.6.1 Creating the Oracle Inventory Group

You must create the Oracle Inventory group if it does not already exist. The following topics describe how to determine the Oracle Inventory group name, if it exists, and how to create it if necessary.

Determining Whether the Oracle Inventory Group Exists

When you install Oracle software on the system for the first time, Oracle Universal Installer creates the `oraInst.loc` file. This file identifies the name of the Oracle Inventory group and the path of the Oracle Inventory directory.

To determine whether the Oracle Inventory group exists, enter the following command:

```
# more /etc/oraInst.loc
```

If the output of this command shows the `oinstall` group name, then the group already exists.

If the `oraInst.loc` file exists, then the output from this command is similar to the following:

```
inventory_loc=/u01/app/oracle/oraInventory
inst_group=oinstall
```

The `inst_group` parameter shows the name of the Oracle Inventory group, `oinstall`.

Creating the Oracle Inventory Group

If the `oraInst.loc` file does not exist, then create the Oracle Inventory group by entering the following command:

```
# /usr/sbin/groupadd oinstall
```

2.6.2 Creating the OSDBA Group

You must create an OSDBA group in the following circumstances:

- An OSDBA group does not exist, for example, if this is the first installation of Oracle software on the system
- An OSDBA group exists, but you want to give a different group of operating system users database administrative privileges in a new Oracle installation

If the OSDBA group does not exist or if you need a new OSDBA group, then create it as follows. In the following command, use the group name `dba` unless a group with that name already exists.

```
# /usr/sbin/groupadd dba
```

2.6.3 Creating an OSOPER Group (Optional)

Create an OSOPER group only if you want to identify a group of operating system users with a limited set of database administrative privileges (SYSOPER operator privileges). For most installations, it is sufficient to create only the OSDBA group. If you want to use an OSOPER group, then you must create it in the following circumstances:

- If an OSOPER group does not exist, for example, if this is the first installation of Oracle software on the system
- If an OSOPER group exists, but you want to give a different group of operating system users database operator privileges in a new Oracle installation

If you need a new OSOPER group, then create it as follows. In the following command, use the group name `oper` unless a group with that name already exists.

```
# /usr/sbin/groupadd oper
```

2.6.4 Creating the Oracle Software Owner User

You must create an Oracle software owner user in the following circumstances:

- If an Oracle software owner user does not exist, for example, if this is the first installation of Oracle software on the system
- If an Oracle software owner user exists, but you want to use a different operating system user, with a different group membership, to give database administrative privileges to those groups in a new Oracle installation

2.6.4.1 Determining Whether an Oracle Software Owner User Exists

To determine whether an Oracle software owner user named `oracle` exists, enter the following command:

```
# id oracle
```

If the `oracle` user exists, then the output from this command is similar to the following:

```
uid=440(oracle) gid=200(oinstall) groups=201(dba),202(oper)
```

If the user exists, then determine whether you want to use the existing user or create another Oracle software owner (`oracle`) user. If you want to use the existing user, then ensure that the primary group of the user is the Oracle Inventory group and that it is a member of the appropriate OSDBA and OSOPER groups.

Note: If necessary, contact your system administrator before using or modifying an existing user.

See one of the following sections for more information:

- To modify an existing Oracle software owner user, see Section 2.6.4.3.
- To create an Oracle software owner user, see the following section.

2.6.4.2 Creating an Oracle Software Owner User

If the Oracle software owner user does not exist or if you need a new Oracle software owner user, then create it as follows. In the following procedure, use the user name `oracle` unless a user with that name already exists.

1. To create the `oracle` user, enter a command similar to the following:

   ```
   # /usr/sbin/useradd -g oinstall -G dba[,oper] oracle
   ```

   In this command:

   - The `-g` option specifies the primary group, which must be the Oracle Inventory group, for example, `oinstall`.
   - The `-G` option specifies the secondary groups, which must include the OSDBA group and, if required, the OSOPER group (for example, `dba` or `dba`, `oper`).

2. Set the password of the `oracle` user:

   ```
   # passwd oracle
   ```

See Section 2.6.5 to continue.

2.6.4.3 Modifying an Oracle Software Owner User

If the `oracle` user exists, but its primary group is not `oinstall` or it is not a member of the appropriate OSDBA or OSOPER groups, then enter a command similar to the following to modify it. Specify the primary group using the `-g` option and any required secondary group using the `-G` option:

```
# /usr/sbin/usermod -g oinstall -G dba[,oper] oracle
```

2.6.5 Verifying That the User nobody Exists

Before installing the software, perform the following procedure to verify that the `nobody` user exists on the system:

1. To determine whether the user exists, enter the following command:

   ```
   # id nobody
   ```

   If this command displays information about the `nobody` user, then you do not have to create that user.

2. If the `nobody` user does not exist, then enter the following command to create it:

   ```
   # /usr/sbin/useradd nobody
   ```

2.7 Checking the Kernel Parameters

> **Note:** The kernel parameter and shell limit values shown in the following section are recommended minimum values only or the value checked at the time of the installation. For production database systems, Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

When it is installed, Oracle Validated Configuration RPM sets and verifies system parameters based on recommendations from the Oracle Validated Configurations program following an operating system installation. See Section 2.4 for more information about Oracle Validated Configuration RPM.

If Oracle Validated Configuration RPM is not installed, verify that the kernel parameters shown in the following table are set to values greater than or equal to the

recommended minimum value shown or the value checked at the time of the installation.

Parameter	Value	File
semmsl	250	/proc/sys/kernel/sem
semmns	32000	
semopm	100	
semmni	128	
shmall	2097152	/proc/sys/kernel/shmall
shmmax	Half the size of physical memory (in bytes)	/proc/sys/kernel/shmmax
shmmni	4096	/proc/sys/kernel/shmmni
file-max	65536	/proc/sys/fs/file-max
ip_local_port_range	Minimum:1024 Maximum: 65000	/proc/sys/net/ipv4/ip_local_port_range
rmem_default	262144	/proc/sys/net/core/rmem_default
rmem_max	262144	/proc/sys/net/core/rmem_max
wmem_default	262144	/proc/sys/net/core/wmem_default
wmem_max	262144	/proc/sys/net/core/wmem_max

Note: If the current value for any parameter is higher than the value listed in this table, then do not change the value of that parameter.

To view the current values specified for these kernel parameters, and to change them if necessary:

1. Enter the commands shown in the following table to view the current values of the kernel parameters:

Note:

- You will need root privileges to run the commands.
- Make a note of the current parameter values and identify any values that you must change.

Parameter	Command
semmsl, semmns, semopm, and semmni	`# /sbin/sysctl -a | grep sem` This command displays the value of the semaphore parameters in the order listed.
shmall, shmmax, and shmmni	`# /sbin/sysctl -a | grep shm` This command displays the details of the shared memory segment sizes.

Parameter	Command
file-max	`# /sbin/sysctl -a | grep file-max` This command displays the maximum number of file handles.
ip_local_port_range	`# /sbin/sysctl -a | grep ip_local_port_range` This command displays a range of port numbers.
rmem_default	`# /sbin/sysctl -a | grep rmem_default`
rmem_max	`# /sbin/sysctl -a | grep rmem_max`
wmem_default	`# /sbin/sysctl -a | grep wmem_default`
wmem_max	`# /sbin/sysctl -a | grep wmem_max`

2. If the value of any kernel parameter is different from the recommended minimum value, then complete the following procedure:

   Using any text editor, create or edit the `/etc/sysctl.conf` file, and add or edit lines similar to the following:

   Note: Include lines only for the kernel parameter values that you want to change. For the semaphore parameters (`kernel.sem`), you must specify all four values. However, if any of the current values are larger than the recommended value, then specify the larger value. You should set the value of `kernel.shmmax` to 536870912; however, Oracle recommends that you set kernel.shmmax to 2 GB, as shown in the following example. Do not set it lower than 536870912.

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 262144
net.core.rmem_max = 262144
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

   If you specify the values in the `/etc/sysctl.conf` file, they persist when you restart the system.

   On SUSE systems only, enter the following command to ensure that the system reads the `/etc/sysctl.conf` file when it restarts:

```
# /sbin/chkconfig boot.sysctl on
```

Setting Shell Limits for the Oracle User

To improve the performance of the software on Linux systems, you must increase the following shell limits for the `oracle` user:

Shell Limit	Item in limits.conf	Hard Limit
Maximum number of open file descriptors	`nofile`	65536

Shell Limit	Item in limits.conf	Hard Limit
Maximum number of processes available to a single user	nproc	16384

To increase the shell limits:

1. Add the following lines to the /etc/security/limits.conf file:

```
oracle              soft    nproc   2047
oracle              hard    nproc   16384
oracle              soft    nofile  1024
oracle              hard    nofile  65536
```

2. Add or edit the following line in the /etc/pam.d/login file, if it does not already exist:

```
session    required     /lib/security/pam_limits.so
```

3. Depending on the default shell of the oracle user, make the following changes to the default shell startup file:

   - For a Bourne, Bash, or Korn shell, add the following lines to the /etc/profile file (or the /etc/profile.local file on SUSE systems):

```
if [ $USER = "oracle" ]; then
        if [ $SHELL = "/bin/ksh" ]; then
              ulimit -p 16384
              ulimit -n 65536
        else
              ulimit -u 16384 -n 65536
        fi
fi
```

   - For a C shell (csh or tcsh), add the following lines to the /etc/csh.login file (or the /etc/csh.login.local file on SUSE systems):

```
if ( $USER == "oracle" ) then
        limit maxproc 16384
        limit descriptors 65536
endif
```

2.8 Identifying the Required Software Directories

You must identify or create the following directories for the Oracle software:

- Oracle Base Directory
- Oracle Inventory Directory
- Oracle Home Directory

2.8.1 Oracle Base Directory

The Oracle base directory is a top-level directory for Oracle software installations. On Linux systems, the Optimal Flexible Architecture (OFA) guidelines recommend that you use a path similar to the following for the Oracle base directory:

/mount_point/app/*oracle_sw_owner*

In this example:

- *mount_point* is the mount point directory for the file system that will contain the Oracle software.

  The examples in this guide use /u01 for the mount point directory. However, you could choose another mount point directory, such as /oracle or /opt/oracle.

- *oracle_sw_owner* is the operating system user name of the Oracle software owner, for example, oracle.

You can use the same Oracle base directory for more than one installation or you can create separate Oracle base directories for different installations. If different operating system users install Oracle software on the same system, then each user must create a separate Oracle base directory. The following example Oracle base directories could all exist on the same system:

```
/u01/app/oracle
/u01/app/orauser
/opt/oracle/app/oracle
```

The following topics describe how to identify existing Oracle base directories that might be suitable for your installation and how to create an Oracle base directory if necessary.

Regardless of whether you create an Oracle base directory or decide to use an existing one, you must set the ORACLE_BASE environment variable to specify the full path to this directory.

2.8.2 Oracle Inventory Directory

The Oracle Inventory directory (oraInventory) stores an inventory of all software installed on the system. It is required by, and shared by, all Oracle software installations on a single system. The first time you install Oracle software on a system, Oracle Universal Installer prompts you to specify the path to this directory. Oracle recommends that you choose the following path:

oracle_base/oraInventory

Oracle Universal Installer creates the directory that you specify and sets the correct owner, group, and permissions for it. You do not need to create it.

Note: All Oracle software installations rely on this directory. Ensure that you back it up regularly.

Do not delete this directory unless you have completely removed all Oracle software from the system.

2.8.3 Oracle Home Directory

The Oracle home directory is the directory where you choose to install the software for a particular Oracle product. You must install different Oracle products, or different releases of the same Oracle product, in separate Oracle home directories. When you run Oracle Universal Installer, it prompts you to specify the path to this directory and a name that identifies it. The directory that you specify must be a subdirectory of the Oracle base directory. Oracle recommends that you specify a path similar to the following for the Oracle home directory:

oracle_base/product/10.2.3/av_1

Oracle Universal Installer creates the directory path that you specify under the Oracle base directory. It also sets the correct owner, group, and permissions on it. You do not need to manually create this directory on your system.

2.9 Identifying or Creating an Oracle Base Directory

Before starting the installation, you must either identify an existing Oracle base directory or if required, create one. This section contains the following topics:

- Identifying an Existing Oracle Base Directory
- Creating an Oracle Base Directory

Note: You can choose to create an Oracle base directory, even if other Oracle base directories exist on the system.

2.9.1 Identifying an Existing Oracle Base Directory

Existing Oracle base directories might not have paths that comply with Optimal Flexible Architecture (OFA) guidelines. However, if you identify an existing Oracle Inventory directory or existing Oracle home directories, then you can usually identify the Oracle base directories, as follows:

- To identify an existing Oracle Inventory directory

  Enter the following command to view the contents of the `oraInst.loc` file:

  ```
  # more /etc/oraInst.loc
  ```

  If the `oraInst.loc` file exists, then the output from this command is similar to the following:

  ```
  inventory_loc=/u01/app/oracle/oraInventory
  inst_group=oinstall
  ```

  The `inventory_loc` parameter identifies the Oracle Inventory directory (`oraInventory`). The parent directory of the `oraInventory` directory is typically an Oracle base directory. In the previous example, `/u01/app/oracle` is an Oracle base directory.

- To identify existing Oracle home directories

  Enter the following command to view the contents of the `oratab` file:

  ```
  # more /etc/oratab
  ```

  If the `oratab` file exists, then it contains lines similar to the following:

  ```
  *:/u03/app/oracle/product/1.0.0/db_1:N
  *:/opt/orauser/infra_904:N
  *:/oracle/9.2.0:N
  ```

  The directory paths you specify on each line identify Oracle home directories. Directory paths that end with the user name of the Oracle software owner that you want to use are valid choices for an Oracle base directory. If you intend to use the `oracle` user to install the software, then you could choose one of the following directories from the previous example:

  ```
  /u03/app/oracle
  /oracle
  ```

Note: If possible, choose a directory path similar to the first (`/u03/app/oracle`). This path complies with the OFA guidelines.

Before deciding to use an existing Oracle base directory for this installation, ensure that it satisfies the following conditions:

- It should not be on the same file system as the operating system.
- It must have sufficient free disk space as described in the table in Section 2.3.

  To determine the free disk space on the file system where the Oracle base directory is located, enter the following command:

  ```
  # df -h oracle_base_path
  ```

If an Oracle base directory does not exist on the system or if you want to create an Oracle base directory, then complete the steps in Section 2.9.2.

2.9.2 Creating an Oracle Base Directory

Before you create an Oracle base directory, you must identify an appropriate file system with sufficient free disk space, as indicated in the table in Section 2.3.

To identify an appropriate file system:

1. Use the `df -k` command to determine the free disk space on each mounted file system.
2. From the display, identify a file system that has appropriate free space.
3. Note the name of the mount point directory for the file system that you identified.

To create the Oracle base directory and specify the correct owner, group, and permissions for it:

1. Enter commands similar to the following to create the recommended subdirectories in the mount point directory that you identified, and set the appropriate owner, group, and permissions on them:

   ```
   # mkdir -p /mount_point/app/oracle_sw_owner
   # chown -R oracle:oinstall /mount_point/app/oracle_sw_owner
   # chmod -R 775 /mount_point/app/oracle_sw_owner
   ```

   For example, if the mount point you identify is `/u01` and `oracle` is the user name of the Oracle software owner, then the recommended Oracle base directory path is:

   ```
   /u01/app/oracle
   ```

2. When you configure the environment of the `oracle` user (see Section 2.6.4), set the `ORACLE_BASE` environment variable to specify the Oracle base directory that you created.

2.10 Creating Directories for Oracle Audit Vault Database Files

If you choose to place the Oracle Audit Vault database files on a file system, then use the following guidelines when deciding where to place them:

- The default path suggested by Oracle Universal Installer for the database file directory is a subdirectory of the Oracle base directory.

- You can choose either a single file system or more than one file system to store the database files:
  - If you want to use a single file system, then choose a file system on a physical device that is dedicated to the database.

    For best performance and reliability, choose a redundant arrays of independent disks (RAID) device or a logical volume on more than one physical device and implement the stripe-and-mirror-everything (SAME) methodology.
  - If you want to use more than one file system, then choose file systems on separate physical devices that are dedicated to the database.

    This method enables you to distribute physical I/O and create separate control files on different devices for increased reliability. It also enables you to fully implement the OFA guidelines.
- For optimum performance, the file systems that you choose should be on physical devices that are used only by the database.
- The `oracle` user must have write permissions to create the files in the path that you specify.

2.11 Setting the DISPLAY Environment Variable

Before you begin the Audit Vault Server installation, you should check to see that the `DISPLAY` environment variable is set to a proper value. For example, for the Bourne, Bash, or Korn shell, you would enter the following commands, where `myhost.us.example.com` is your host name:

```
$ DISPLAY=myhost.us.example.com:1.0
$ export DISPLAY
```

For example, for the C shell, you would enter the following command, where `myhost.us.example.com` is your host name:

```
% setenv DISPLAY myhost.us.example.com:1.0
```

2.12 Setting the Correct Locale

Ensure that the `NLS_LANG` environment variable is not set.

For example, for C shell:

```
unsetenv NLS_LANG
```

For example, for Bourne, Bash, or Korn shells:

```
unset NLS_LANG
```

3

Installing the Oracle Audit Vault Server

This chapter includes an overview of the major steps required to install single instance Oracle Audit Vault Server (Audit Vault Server) and to install Audit Vault Server with Oracle Real Application Clusters (Oracle RAC).

This chapter includes the following sections:

3.1 Accessing the Server Installation Software

The Audit Vault Server software is available:

- On digital video disc (DVD)
- For download on Oracle Technology Network, `http://www.oracle.com/technology/index.html`

3.2 Basic Installation – Performing the Single Instance Server Installation

For an overview of requested information specific to the Audit Vault Server installation, see Section 3.6.

See Section 2.12 for important information about setting the correct locale.

To perform Audit Vault Server single instance basic installation:

1. Invoke Oracle Universal Installer (OUI) to install Oracle Audit Vault as an Oracle Database 10*g* release 2 (10.2.0.3) database.

   Log in as the `oracle` user. Alternatively, switch the user to `oracle` using the `su -` command. Change your current directory to the directory containing the installation files. Start Oracle Universal Installer from the Oracle Audit Vault package.

   ```
   cd directory-containing-the-Oracle-Audit-Vault-installation-files
   ```

```
./runInstaller
```

Oracle Universal Installer starts up by first checking the following installation requirements and displaying the results. For example, it shows what the value should be or must be greater than or at least equal to, then the actual value for each check and the check result status: Passed or Failed.

- Checking operating system version: must be redhat-3, SuSE-9, SuSE-10, redhat-4, redhat-5, UnitedLinux-1.0, asiaunx-1, asianux-2, enterprise-4 or enterprise-5 Passed
- Checking temp space: must be greater than 80MB. Actual 15412 MB Passed
- Checking swap space: must be greater than 150MB. Actual 3931 MB Passed
- Checking monitor: must be configured to display at least 256 colors. Actual 65536 Passed

Then Oracle Universal Installer prepares to launch itself.

2. On the **Select Installation Type** page, select the **Basic Installation** option, then click **Next**.
3. Enter the following information on the **Basic Installation Details** page. See Section 3.6 for more information about each of these topics.
   a. **Audit Vault Name** – A unique name for the Oracle Audit Vault database. The Oracle Audit Vault name is required. The name will be used as the database SID, and will be the first portion (*db_name*) of the database service name.
   b. **Audit Vault Home** – Specify or browse to find the path to the Oracle Audit Vault home where you want to install Audit Vault Server. Install the Audit vault Server into a new home directory.
   c. **Audit Vault Administrator** and **Audit Vault Auditor** – The account name of the Oracle Audit Vault Administrator and a separate, optional Oracle Audit Vault Auditor, respectively. The Oracle Audit Vault administrator and Oracle Audit Vault auditor account names must not be the same. The Oracle Audit Vault Administrator account name is required. Accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Oracle Audit Vault Auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Oracle Audit Vault Auditor user name and password. The Oracle Audit Vault Administrator in this case will also be granted the role of Oracle Audit Vault Auditor.

      The Oracle Audit Vault Administrator user name will also be used for the following Oracle Database Vault users that are created to facilitate the separation of duties:

      *AV_ADMIN*dvo – The Oracle Database Vault Owner (granted DV_OWNER role) to manage Database Vault roles and configuration, where *AV_ADMIN* represents the Oracle Audit Vault Administrator user name.

      *AV_ADMIN*dva – The Oracle Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts, where *AV_ADMIN* represents the Oracle Audit Vault administrator user name.
   d. **Administrator Password** and **Auditor Password** – The password for the Oracle Audit Vault administrator account and the Oracle Audit Vault auditor account, respectively.

      There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist

of at least one alphabetic character, one numeric character, and one of the special characters shown in Table 3–3.

The password entered for the Oracle Audit Vault administrator account will also be used for the standard database accounts (`sys`, `system`, `sysman`, `dbsnmp`).

The Oracle Audit Vault administrator password will also be used for the Oracle Database Vault users (Database Vault Owner and the Database Vault Account Manager users) that are created to facilitate the separation of duties.

e. **Confirm Password** – The confirming password for the Oracle Audit Vault Administrator account and the Oracle Audit Vault auditor account, respectively.

Each password must be identical to its corresponding password confirmation.

After entering the required information, click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information is performed on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

4. If this is the first installation of an Oracle product on the system, the Oracle Universal Installer displays the **Specify inventory directory and credentials** page, where you must enter the Inventory directory location and the OS group name, then click **Next**.

5. Review the installation prerequisite checks on the **Prerequisite Check** page. This is when all installation prerequisite checks are performed and the results are displayed. Verify that all prerequisite checks succeed, then click **Next**.

   Oracle Universal Installer checks the system to verify that it is configured correctly to run Oracle software. If you have completed all of the preinstallation steps in this guide, all of the checks should pass.

   If a check fails, then review the cause of the failure listed for that check on the screen. If possible, rectify the problem and rerun the check. Alternatively, if you are satisfied that your system meets the requirements, then you can select the check box for the failed check to manually verify the requirement.

6. Review the installation summary information on the **Basic Installation Summary** page. After reviewing this installation information, click **Install** to begin the installation procedure. The installation will copy files, link binaries, apply patches, run configuration assistants, including DBCA to create and start the Audit Vault Server, DVCA to secure the server, and AVCA to configure and start Oracle Audit Vault Console.

   At the end of running DBCA to configure the software and create the database, a message displays, click **OK** to continue.

7. Provide information or run scripts as the `root` user when prompted by Oracle Universal Installer. The `root.sh` script adds your environment variable settings to scripts, such as `coraenv`, that you can later use to set your environment variables. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file is located in the `cfgtoollogs/oui` directory, in the following location:

   $ORACLE_HOME`/cfgtoollogs/oui/installActions`*date_time*`.log`

8. After the installation completes, take note of the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL. On the **Exit** page, click **Exit**. Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

See Section 3.7.7 for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

After you have completed the installation, proceed to Section 3.7 to perform the postinstallation tasks.

3.3 Advanced Installation – Prerequisite Information for Installing in an Oracle Real Application Clusters Environment

This section assumes that you performed the initial installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC). These initial installation procedures are described in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*. These tasks include preinstallation tasks, configuring Oracle Clusterware and Oracle Database storage, and installing Oracle Clusterware. You are now ready to install Oracle Audit Vault in an Oracle RAC environment.

This section describes the remaining installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC).

Verifying System Readiness for Installing Oracle Audit Vault with CVU

To help verify that your system is prepared to install Oracle Audit Vault with Oracle RAC successfully, use the Cluster Verification Utility (CVU) runcluvfy command. See "Verifying System Readiness for Installing Oracle Database with CVU " in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux* for more information.

If the cluster verification check fails, then review and correct the relevant system configuration steps, and run the test again. Use the system configuration checks described in "Troubleshooting Installation Setup for Linux" in Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux to assist you.

3.4 Advanced Installation – Installing Single Instance and Installing in an Oracle Real Application Clusters Environment

For an overview of requested information specific to the Audit Vault Server installation, see Section 3.6.

See Section 2.12 for important information about setting the correct locale.

This section describes the advanced installation for both the single instance installation and the Oracle RAC installation.

Perform the following procedures to install Oracle Audit Vault.

1. Run Oracle Universal Installer (OUI) to install Audit Vault Server.

   Log in as the `oracle` user. Alternatively, switch user to `oracle` using the `su -` command. Change your current directory to the directory containing the installation files. Start Oracle Universal Installer from the Oracle Audit Vault package.

```
cd directory-containing-the-Oracle-Audit-Vault-installation-files
./runInstaller
```

Oracle Universal Installer starts up by first checking the following installation requirements and displaying the results. For example, it shows what the value should be or must be greater than or at least equal to, then the actual value for each check and the check result status: Passed or Failed.

- Checking operating system version: must be redhat-3, SuSE-9, SuSE-10, redhat-4, redhat-5, UnitedLinux-1.0, asiaunx-1, asianux-2, enterprise-4 or enterprise-5 Passed
- Checking temp space: must be greater than 80MB. Actual 14773 MB Passed
- Checking swap space: must be greater than 150MB. Actual 3970 MB Passed
- Checking monitor: must be configured to display at least 256 colors. Actual 65536 Passed

Then Oracle Universal Installer prepares to launch itself.

2. On the **Select Installation Type** screen, select the **Advanced Installation** option, then click **Next**.
3. Enter the following information on the **Advanced Installation Details** screen. See Section 3.6 for more information about each of these topics.

   a. **Audit Vault Name** – A unique name for the Oracle Audit Vault database. The Oracle Audit Vault name is required. For single instance installation, the name will be used as the database SID, and will be the first portion (*db_name*) of the database service name. For an Oracle RAC installation, the name will be used to derive the Oracle RAC database SID of each Oracle RAC node, and will be the first portion (*db_name*) of the database service name.

   b. **Audit Vault Home** – Specify or browse to find the path to the Oracle Audit Vault home where you want to install Oracle Audit Vault.

   Note: The Oracle home name and path that you provide during Audit Vault Server installation *must be different* from the home that you used during the Oracle Clusterware installation. You **cannot** install Audit Vault Server with Oracle RAC software into the same home in which you installed the Oracle Clusterware software.

   c. **Audit Vault Administrator** and **Audit Vault Auditor** – the account name of the Oracle Audit Vault administrator and a separate, optional Oracle Audit Vault auditor, respectively. The Oracle Audit Vault administrator and Oracle Audit Vault auditor account names cannot be the same. The Oracle Audit Vault Administrator account name is required. Accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Oracle Audit Vault auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Oracle Audit Vault auditor user name and password. The Oracle Audit Vault administrator in this case will also be granted the role of Oracle Audit Vault Auditor.

   d. **Administrator Password** and **Auditor Password** – The password for the Oracle Audit Vault administrator account and the Oracle Audit Vault auditor account, respectively.

      There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist

of at least one alphabetic character, one numeric character, and one of the special characters shown in Table 3–3.

e. **Confirm Password** – The confirming password for the Oracle Audit Vault Administrator account and the Oracle Audit Vault Auditor account, respectively.

Each password must be identical to its corresponding password confirmation.

After entering the required information, click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information is performed on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

4. If this is the first installation of an Oracle product on the system, the Oracle Universal Installer displays the **Specify inventory directory and credentials** page, where you must enter the Inventory directory location and the OS group name, then click **Next**.

5. Enter the following information on the **Database Vault User Credentials** screen. See Section 3.6.2 for more information about each of these topics.

a. **Database Vault Owner** and **Database Vault Account Manager** – The account name of the Oracle Database Vault Owner and a separate, optional Oracle Database Vault Account Manager, respectively. The Database Vault Owner, Database Vault Account Manager, Oracle Audit Vault Administrator, and Oracle Audit Vault Auditor account names must not be the same (applicable when a separate Oracle Audit Vault Auditor or Database Vault Account Manager account is created). The Database Vault Owner name is required. Accept the selected **Create a Separate Database Vault Account Manager** check box to choose to create the Database Vault Account Manager account name. The check box is selected by default. Deselecting the check box disables the text fields for the Database Vault Account Manager user name and password. The Database Vault Owner in this case will also be granted the role of Database Vault Account Manager.

b. **Database Vault Owner Password** and **Database Vault Account Manager Password** – The password for the Oracle Database Vault Owner account and the Oracle Database Vault Account Manager account, respectively.

There cannot be repeating characters and space characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in Table 3–3.

c. **Confirm Password** – The confirming password for the Oracle Database Vault Owner account and the Oracle Database Vault Account Manager account, respectively.

Each password must be identical to its corresponding password confirmation.

After entering the required information, click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information is performed on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

6. If you are installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), the **Node Selection** screen appears from which to select the nodes on which Oracle Audit Vault will be installed. Local node will

always be selected by default. If you are installing Oracle Audit Vault single instance on this local node only, select the **Local Only Installation** option, then click **Next**.

If you are installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), select the nodes on which on which Oracle Audit Vault must be installed, then click **Next**.

7. Review the installation prerequisite checks on the **Prerequisite Check** screen. This is when all installation prerequisite checks are performed and the results are displayed. Verify that all prerequisite checks succeed, then click **Next**.

   Oracle Universal Installer checks the system to verify that it is configured correctly to run Oracle Database software. If you have completed all of the preinstallation steps in this guide, all of the checks should pass.

   If a check fails, then review the cause of the failure listed for that check on the screen. If possible, rectify the problem and rerun the check. Alternatively, if you are satisfied that your system meets the requirements, then you can select the check box for the failed check to manually verify the requirement.

8. On the **Specify Database Storage Options** screen, you can select one of the following storage options: **File system**, **Automatic Storage Management (ASM)**, or **Raw Devices**.

   If you select the **File System**, specify or browse to the database file location for the data files. If you select **Raw Devices**, specify the path or browse to the Raw Devices mapping file. If you select **Automated Storage Management (ASM)**, you must have already installed ASM. Make a selection and click **Next**.

9. On the **Specify Backup and Recovery Options** screen, you can choose either to not enable automated backups or to enable automated backups.

   If you select the **Do not enable Automated backups** option, click **Next**.

   If you select the **Enable Automated backups** option, then you must specify a **Recovery Area Storage**. You can choose either to use the **File System** option or the **Automatic Storage Management** option.

   If you select the **File System** option, specify a path or browse to the recovery area location. Next, for **Backup Job Credentials**, enter the operating system credentials (user name and password) of the user account with administrative privileges to be used for the backup jobs, then click **Next**.

   If you select the **Automatic Storage Management** option, then for **Backup Job Credentials**, enter the operating system credentials (user name and password) of the user account with administrative privileges to be used for the backup jobs, then click **Next**.

   Next, select the disk group from the existing disk groups. This screen lets you select the disk groups. If the disk group selected has enough free space, by clicking **Next**, the **Specifying Database Schema Password** screen is displayed (see Step 9). If the disk group selected does not have enough free space, the **Configure Automatic Storage Management** page is displayed.

   On the **Configure Automatic Storage Management** screen, you can select the disks to add from the **Add Member Disks** table by selecting the check box in the **Select** column for the corresponding disks.

   On Linux systems, the default path for discovering eligible disks is `/dev/raw/*`. If your disks are located elsewhere, you must change the disk discovery path for

the disks to be discovered by Oracle Universal Installer. To change the path, click **Change Disk Discovery Path**.

10. On the **Specify Database Schema Passwords** screen, you can choose to enter different passwords for each privileged database account or select the **Use the same passwords for all accounts** option. If you choose to enter a set of valid passwords for each privileged database account, enter these passwords. If you select the **Use the same passwords for all accounts** option, then enter a single valid password. When you are finished, click **Next**.
11. Review the installation summary information on the **Advanced Installation Summary** screen. After reviewing this installation information, click **Install** to begin the installation procedure. The installation will copy files, link binaries, apply patches, run configuration assistants, including DBCA to create and start the Audit Vault Server, DVCA to secure the server, and AVCA to configure and start Oracle Audit Vault Console.

    At the end of running DBCA to configure the software and create the database, a message displays, click **OK** to continue.
12. Run scripts as the `root` user when prompted by Oracle Universal Installer. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file is located in the `cfgtoollogs/oui` directory in the following location:

    `$ORACLE_HOME``/cfgtoollogs/oui/installActions`*`date_time`*`.log`

    The following is a list of additional information to note about installation:

    - If you are not using the ASM library driver (ASMLIB), and you select Automatic Storage Management (ASM) during installation, then ASM default discovery finds all disks that ASMLIB marks as ASM disks.
    - If you are not using ASMLIB, and you select ASM during installation, then ASM default discovery finds all disks marked `/dev/raw/*` for which the Oracle software owner user has read/write permission. You can change the disk discovery string during the installation if the disks that you want to use for ASM are located elsewhere.
    - On the Select Database Management Option page, if you have already completed the Grid Control Management Agent installation, then you can select either Grid or Local Database control. Otherwise, only Local Database control for database management is supported for Oracle RAC. When you use the local Database Control, you can choose the e-mail option and enter the outgoing SMTP server name and e-mail address.

      See Also: *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for details about installing Grid Control with Oracle Universal Installer, and *Oracle Enterprise Manager Advanced Configuration Guide* for details about installing Database Control with the Database Configuration Assistant (DBCA) and Enterprise Manager Configuration Assistant (EMCA)

13. After the installation completes, take note of the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL. On the **Exit** page, click **Exit.** Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

See Section 3.7.7 for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

After you have completed the part of the installation, proceed to Section 3.7 to perform the postinstallation tasks.

3.5 Performing a Silent Installation Using a Response File

Note: The Basic installation option is not supported in silent mode. Silent installation is only supported for the Advanced installation option.

For an overview of requested information specific to the Audit Vault Server installation, see Section 3.6.

Follow these brief steps to perform a silent installation using a response file:

1. Make sure all prerequisites are met for the installation of Audit Vault Server.
2. Prepare the Audit Vault Server response file. A template response file can be found at *AV-installer-location*`/response/av.rsp` on the Audit Vault Server installation media.

   Prepare the response file by entering values for all parameters that are missing in the first part of the response file, then save the file. Note that for single instance installations, RAW storage is not used. Also note that the `CLUSTER_NODES` parameter must be specified for installing Audit Vault Server in an Oracle RAC environment. Do not edit any values in the second part of either response file.
3. Set the `DISPLAY` environment variable to an appropriate value before proceeding with the silent installation. See Section 2.11 for more information.
4. Invoke Oracle Universal Installer using the following options:

   ```
   ./runInstaller -silent -responseFile path_of_response_file
   ```

For more information about these options, see Section 1.3.2. For general information about how to complete a database installation using response files, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*.

3.6 Audit Vault Server Installation Details

This section provides an overview of requested information specific to the Audit Vault Server installation.

An Audit Vault Server installation consists of three options:

- **Upgrade Existing Audit Vault Server Home** – Detects the existence of upgradable Audit Vault Server homes on the system and enables the upgrade option to the current release. Performs an upgrade on the selected upgradable Audit Vault Server home when this option is selected. See Chapter 4 for more information on performing an upgrade.
- **Basic Installation** – Simplifies the installation process and prompts for a minimal set of inputs, including the name of the Oracle Audit Vault database, the Oracle Audit Vault administrator and optionally the Oracle Audit Vault auditor user names and passwords. An Oracle RAC installation is not supported through the **Basic Installation** option.

- **Advanced Installation** – Offers the user more control and options for the installation process, including storage options and backup options. The **Advanced Installation** option supports the installation of Audit Vault Server on a cluster.

This section covers the following topics:

3.6.1 Basic and Advanced Installation Details Screens

This section describes the required fields in the **Basic Installation Details** screen and the **Advanced Installation Details** screen.

3.6.1.1 Audit Vault Name

The Oracle Audit Vault Name must be a unique name for the Oracle Audit Vault database. The name will be used for the database SID, and will be the first portion (*db_name*) of the database service name.

The name cannot exceed 8 characters and must begin with an alphabetic character.

The Oracle Audit Vault name cannot contain any of the characters shown in Table 3–1.

Table 3–1 Invalid Oracle Audit Vault Name and Oracle Audit Vault Account Name Characters

Symbol	Character Name
!	Exclamation point
@	At sign
%	Percent sign
^	Circumflex
&	Ampersand
*	Asterisk
(	Left parenthesis
)	Right parenthesis
-	Minus sign
+	Plus sign
=	Equal sign
"	Double quotation mark
|	Vertical bar
`	grave
~	tilde
[	Left bracket
{	Left brace

Table 3–1 (Cont.) Invalid Oracle Audit Vault Name and Oracle Audit Vault Account Name Characters

Symbol	Character Name
]	Right bracket
}	Right brace
;	Semicolon
:	Colon
'	Single quotation mark
<	Less than sign
>	Greater than sign
/	Slash
\	Backslash
?	Question mark
,	Comma
.	Period
#	Number sign
_	Underscore
$	Dollar sign
	Space character

3.6.1.2 Oracle Audit Vault Home

The Oracle Audit Vault Home is the path that you must specify or browse to find the Oracle Audit Vault home where you want to install Oracle Audit Vault. The path can contain only alphanumeric characters (letters and numbers).

In addition, the special characters shown in Table 3–2 are allowed.

Table 3–2 Special Characters Allowed in the Oracle Audit Vault Home Name

Symbol	Character Name
\	Backslash
/	Slash
-	hyphen
_	Underscore
.	Period
:	Colon

3.6.1.3 Oracle Audit Vault Server Accounts

The Oracle Audit Vault Server installation software prompts you for user names and passwords for the Oracle Audit Vault Administrator user and the separate, optional Oracle Audit Vault Auditor user. In addition, the installation creates an Oracle Database Vault Owner user and a separate, Oracle Database Vault Account Manager for you (basic installation) or the installation prompts you for these user names and passwords (advanced installation). Finally, the installation creates `sys`, `system`,

sysman, and dbsnmp standard database users for you (basic installation) or the installation prompts for passwords for these users (advanced installation).

You must supply a user name and password for the Oracle Audit Vault administrator user and optionally for the Oracle Audit Vault auditor user during installation. The **Create a Separate Audit Vault Auditor** check box is selected by default, which means that a separate Oracle Audit Vault Auditor account will be created (and the corresponding user name and password are required). The Oracle Audit Vault Administrator user will be granted the AV_ADMIN role and the Oracle Audit Vault Auditor user will be granted the AV_AUDITOR role. Deselecting this check box means that the Oracle Audit Vault Administrator user will be granted both roles, because the separate Oracle Audit Vault Auditor user will not be created.

Audit Vault Administrator and Audit Vault Auditor Accounts

The Oracle Audit Vault Administrator account is granted the AV_ADMIN role. The user granted the AV_ADMIN role can manage the postinstallation configuration. This role accesses Oracle Audit Vault services to administer, configure, and manage a running Oracle Audit Vault system. This role registers audit sources. This role has the ability to configure parameters that assist in populating the Oracle Audit Vault data warehouse. For the basic installation, the Oracle Audit Vault Administrator user name is used to generate the following Oracle Database Vault users to facilitate the separation of duties:

- *AV_ADMIN*dvo – The Oracle Database Vault Owner (granted DV_OWNER role) to manage Database Vault roles and configuration
- *AV_ADMIN*dva – The Oracle Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts

For the advanced installation, a **Database Vault User Credentials** page prompts for the Database Vault Owner account name and password and a separate, optional Database Vault Account Manager account name and password.

The Oracle Audit Vault Auditor account is granted the AV_AUDITOR role. The user granted the AV_AUDITOR role accesses Oracle Audit Vault Reporting and Analysis services to monitor components, detect security risks, create and evaluate alert scenarios, create detail and summary reports of events across systems, and manage the reports. This role manages central audit settings. This role can use the data warehouse services to further analyze the audit data to assist in looking for trends, intrusions, anomalies, and other areas of interest.

The Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, and Oracle Database Vault Account Manager user names must not be the same. For the basic installation, the Oracle Audit Vault Administrator user name must be between 2 and 27 characters because the characters "dvo" and "dva" are appended to the Administrator name making the normal upper limit of 30 characters for the user names that are allowed to be 27 characters. For the advanced installation, the Oracle Audit Vault Administrator user name must be between 2 and 30 characters.

The length of the Oracle Audit Vault Auditor user name must be between 2 and 30 characters. Each user name must not be one of the following reserved names.

Names	Names	Names	Names	Names
ACCESS	ADD	ALL	ALTER	AND
ANONYMOUS	ANY	AQ_ADMINISTRATOR_ROLE	AQ_USER_ROLE	ARRAYLEN
AS	ASC	AUDIT	AUTHENTICATEDUSER	AV_ADMIN

Names	Names	Names	Names	Names
AV_AGENT	AV_ARCHIVER	AV_AUDITOR	AV_SOURCE	AVSYS
BETWEEN	BY	CHAR	CHECK	CLUSTER
COLUMN	COMMENT	COMPRESS	CONNECT	CREATE
CTXAPP	CTXSYS	CURRENT	DATE	DBA
DBSNMP	DECIMAL	DEFAULT	DELETE	DELETE_CATALOG_ROLE
DESC	DIP	DISTINCT	DM_CATALOG_ROLE	DMSYS
DMUSER_ROLE	DROP	DV_ACCTMGR	DV_ADMIN	DVF
DV_OWNER	DV_PUBLIC	DV_REALM_OWNER	DV_REALM_RESOURCE	DV_SECANALYST
DVSYS	EJBCLIENT	ELSE	EXCLUSIVE	EXECUTE_CATALOG_ROLE
EXFSYS	EXISTS	EXP_FULL_DATABASE	FILE	FLOAT
FOR	FROM	GATHER_SYSTEM_ STATISTICS	GLOBAL_AQ_USER_ ROLE	GRANT
GROUP	HAVING	HS_ADMIN_ROLE	IDENTIFIED	IMMEDIATE
IMP_FULL_ DATABASE	IN	INCREMENT	INDEX	INITIAL
INSERT	INTEGER	INTERSECT	INTO	IS
JAVA_ADMIN	JAVADEBUGPRIV	JAVA_DEPLOY	JAVAIDPRIV	JAVASYSPRIV
JAVAUSERPRIV	LBAC_DBA	LBACSYS	LEVEL	LIKE
LOCK	LOGSTDBY_ ADMINISTRATOR	LONG	MAXEXTENTS	MDDATA
MDSYS	MGMT_USER	MGMT_VIEW	MINUS	MODE
MODIFY	NOAUDIT	NOCOMPRESS	NOT	NOTFOUND
NOWAIT	NULL	NUMBER	OEM_ADVISOR	OEM_MONITOR
OF	OFFLINE	OLAP_DBA	OLAPSYS	OLAP_USER
ON	ONLINE	ONT	OPTION	OR
ORDER	ORDPLUGINS	ORDSYS	OUTLN	OWF_MGR
PCTFREE	PRIOR	PRIVILEGES	PUBLIC	RAW
RECOVERY_ CATALOG_ OWNER	RENAME	RESOURCE	REVOKE	ROW
ROWID	ROWLABEL	ROWNUM	ROWS	SCHEDULER_ADMIN
SCOTT	SELECT	SELECT_CATALOG_ROLE	SESSION	SET
SHARE	SI_INFORMTN_ SCHEMA	SIZE	SMALLINT	SQLBUF
START	SUCCESSFUL	SYNONYM	SYS	SYSDATE
SYSMAN	SYSTEM	TABLE	THEN	TO
TRIGGER	TSMSYS	UID	UNION	UNIQUE
UPDATE	USER	VALIDATE	VALUES	VARCHAR
VARCHAR2	VIEW	WHENEVER	WHERE	WITH
WKPROXY	WKSYS	WK_TEST	WKUSER	WM_ADMIN_ROLE
WMSYS	XDB	XDBADMIN		

Each account name cannot contain any of the characters shown in Table 3–1.

Audit Vault Administrator and Audit Vault Auditor Passwords

For the basic installation, the Oracle Audit Vault Administrator password you enter for the Oracle Audit Vault Administrator account is also used for the standard database accounts (`sys`, `system`, `sysman`, `dbsnmp`). For the basic installation **Details** page, the Oracle Audit Vault Administrator user password is also used for the Oracle Database Vault Owner and Oracle Database Vault Account Manager user passwords.

For the advanced installation, the installer can choose individual passwords for each of these database accounts (`sys`, `system`, `sysman`, `dbsnmp`) or select to use the same password as the Oracle Audit Vault Administrator for all of these accounts. In addition, a **Database Vault User Credentials** page prompts for the Oracle Database Vault Owner user password and for a separate, optional Oracle Database Vault Account Manager user password if that user is created.

The Oracle Audit Vault Administrator and Oracle Audit Vault Auditor password cannot be the name of the Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, or Oracle Database Vault Account Manager. The Oracle Audit Vault Administrator user password is required, while the Oracle Audit Vault Auditor user password is only required when creating the separate, optional Oracle Audit Vault Auditor user.

There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in Table 3–3.

Table 3–3 Valid Oracle Audit Vault Administrator and Auditor Password Characters

Symbol	Character Name
%	Percent sign
^	Circumflex
-	Hyphen
[	Left bracket
+	Plus sign
~	Tilde
,	Comma
#	Number sign
]	Right bracket
.	Period
_	Underscore

Each password must be identical to its corresponding password confirmation.

3.6.2 Advanced Server Installation: Database Vault User Credentials Screen

The Audit Vault Server installation software prompts you for two accounts that you create during installation. These are the Oracle Database Vault Owner account and the separate, optional Oracle Database Vault Account Manager account. You must supply an account name and password for the Database Vault Owner account, and optionally for the Database Vault Account Manager account during installation.

The **Create a Separate Database Vault Account Manager** check box is selected by default, which means that a separate Oracle Database Vault Account Manager account will be created (and the corresponding user name and password are required). The Oracle Database Vault Owner user will be granted the `DV_OWNER` role and the Oracle Database Vault Account Manager user will be granted the `DV_ACCTMGR` role. Deselecting this check box means that the Database Vault Owner user will be granted both roles, because the separate Database Vault Account Manager user will not be created.

3.6.2.1 Database Vault Owner and Database Vault Account Manager Accounts

The Oracle Database Vault Owner, Oracle Database Vault Account Manager, Oracle Audit Vault Administrator, and Oracle Audit Vault Auditor account names must be different from each other (applicable when a separate Oracle Audit Vault Auditor or Oracle Database Vault Account Manager account is created). The Oracle Database Vault Owner name is required.

The length of each account name must be between 2 and 30 characters.

Each account name must not be one of the reserved names shown in the table in Section 3.6.1.3.

Each account name cannot contain any of the characters shown in Table 3–1.

3.6.2.2 Database Vault Owner and Database Vault Account Manager Passwords

The Oracle Database Vault Owner or Oracle Database Vault Account Manager password must not be the name of the Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, or Oracle Database Vault Account Manager. The Database Vault Owner user password is required, while the Database Vault Account Manager user password is only required when creating the separate, optional Database Vault Account Manager user.

There must be no repeating characters in each password. There must be no space characters in the password.

The length of each password must be between 8 and 30 characters.

Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in Table 3–3. All other characters are not allowed.

Each password must be identical to its corresponding password confirmation.

3.6.3 Advanced Server Installation: Node Selection Screen

The **Node Selection** screen will appear if you are installing Oracle Audit Vault in an Oracle RAC environment and a clustered system (Oracle Clusterware) is installed and the system is already part of a cluster. On this screen, users can select the nodes on which they want to install Oracle Audit Vault, or they can select a local installation to install Oracle Audit Vault single instance. See *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux* for more information.

3.6.4 Advanced Server Installation: Specify Database Storage Options Screen

On the **Specify Database Storage Options** screen, you can select **File System**, **Automatic Storage Management**, or **Raw Storage**.

File System

If you choose the **File System** option, then Database Configuration Assistant creates the database files in a directory on a file system mounted on the computer. Oracle recommends that the file system you choose be separate from the file systems used by the operating system or the Oracle software. The file system that you choose can be any of the following:

- A file system on a disk that is physically attached to the system

  If you are creating a database on basic disks that are not logical volumes or redundant arrays of independent disks (RAID) devices, then Oracle recommends that you follow the Optimal Flexible Architecture (OFA) recommendations and distribute the database files over more than one disk.

- A file system on a logical volume manager (LVM) volume or a RAID device

  If you are using multiple disks in an LVM or RAID configuration, then Oracle recommends that you use the stripe and mirror everything (SAME) methodology to increase performance and reliability. Using this methodology, you do not need to specify more than one file system mounting point for database storage.

- A network file system (NFS) mounted from a certified network attached storage (NAS) device

  You can store database files on NAS devices provided that the NAS device is certified by Oracle. See "Using Network Attached Storage or NFS File Systems" section in *Oracle Database Installation Guide for Linux x86* for more information about certified NAS and NFS devices.

Automatic Storage Management

Automatic Storage Management (ASM) is a high-performance storage management solution for Oracle Audit Vault database files. It simplifies the management of a dynamic database environment, such as creating and laying out databases and managing disk space.

Note: An existing ASM instance must be installed to select the ASM option for database storage.

Automatic Storage Management can be used with a single instance Oracle Audit Vault installation, multiple Oracle Audit Vault installations, and in an Oracle Real Application Clusters (Oracle RAC) environment. Automatic Storage Management manages the storage of all Oracle Audit Vault database files, such as redo logs, control files, data pump export files, and so on.

See: *Oracle Database Administrator's Guide* for more information.

Raw Devices

Raw devices are disk partitions or logical volumes that have not been formatted with a file system. When you use raw devices for database file storage, Oracle Database writes data directly to the partition or volume, bypassing the operating system file system layer. For this reason, you can sometimes achieve performance gains by using raw devices. However, because raw devices can be difficult to create and administer, and because the performance gains over more modern file systems are minimal, Oracle recommends that you choose Automatic Storage Management or file system storage instead of raw devices.

3.6.5 Advanced Server Installation: Specify Backup and Recovery Option Screen

On the **Specify Backup and Recovery** screen, you can choose **Enable Automated Backups** or **Do Not Enable Automated Backups**.

If you choose **Enable Automated Backups**, then Oracle Enterprise Manager schedules a daily backup job that uses Oracle Recovery Manager (RMAN) to back up all of the database files to an on-disk storage area called the flash recovery area. The first time that the backup job runs, it creates a full backup of the database. Subsequent backup jobs perform incremental backups, which enable you to recover the database to its state at any point during the preceding 24 hours.

To enable automated backup jobs during installation, you must specify the following information:

- The location of the flash recovery area

  You can choose to use either a file system directory or an Automatic Storage Management disk group for the flash recovery area. The default disk quota configured for the flash recovery area is 2 GB. For Automatic Storage Management disk groups, the required disk space depends on the redundancy level of the disk group that you choose. See *Oracle Database Installation Guide for Linux x86* for more information about how to choose the location of the flash recovery area and to determine its disk space requirements.

- An operating system user name and password for the backup job

  Oracle Enterprise Manager uses the operating system credentials that you specify when running the backup job. The user name that you specify must belong to the Linux group that identifies database administrators (the OSDBA group, typically `dba`). The Oracle software owner user name (typically `oracle`) that you use to install the software is a suitable choice for this user. Section 2.6 describes the requirements for the OSDBA group and Oracle software owner user and explains how to create them.

Backup Job Default Settings

If you enable automated backups after choosing one of the preconfigured databases during the installation, then automated backup is configured with the following default settings:

- The backup job is scheduled to run nightly at 2:00 a.m.
- The disk quota for the flash recovery area is 2 GB.

If you enable automated backups by using Database Configuration Assistant after the installation, then you can specify a different start time for the backup job and a different disk quota for the flash recovery area.

For information about using Oracle Enterprise Manager Database Control to configure or customize automated backups or to recover a backed up database, see *Oracle Database 2 Day DBA*.

For more detailed information about defining a backup strategy and backing up and recovering Oracle databases, see *Oracle Database Backup and Recovery Advanced User's Guide*.

3.6.6 Advanced Server Installation: Specify Database Schema Passwords Screen

On the **Specify Database Schema Passwords** screen, provide the passwords for the four standard database accounts (`sys`, `system`, `sysman`, and `dbsnmp`).

Either enter and confirm passwords for the privileged database accounts, or select the **Use the same passwords for all accounts** option. Make your selection, then click **Next**.

3.7 Postinstallation Server Tasks

Note: The use of the Database Configuration Assistant (DBCA) to configure additional components after an Audit Vault Server installation is not supported. Audit Vault Server installs with all of the components that it requires already configured, so no additional components need to be configured using DBCA.

Creation of additional databases in the Oracle Audit Vault home is not supported.

Cloning of Oracle Audit Vault homes is not supported.

This section includes the following topics:

- Download Patches
- Download Critical Patch Updates
- Reset User Passwords
- Enable or Disable Connections with the SYSDBA Privilege
- Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC Only)
- Download JDBC Driver Files for Source Database Connectivity
- Log in to Oracle Audit Vault Console
- Next Steps to Perform as an Oracle Audit Vault Administrator

3.7.1 Download Patches

You can find mandatory Oracle Audit Vault patchsets on the My Oracle Support Web site.

To find and download patchsets for Audit Vault Server:

1. Log in to My Oracle Support from the following URL:

   `https://support.oracle.com`

2. Click the **Patches & Updates** tab.
3. Under **Patch Search**, click **Product or Family (Advanced Search)**.
4. Enter `Oracle Audit Vault` in the search field.
5. In the first **Select one or more** list, expand the Oracle Audit Vault list and select **Audit Vault 10.2.3.2.0**. Click **Close**.
6. In the second **Select one or more list**, select your specific platform from the list, then click **Close**.
7. Click **Search**. In a moment, the patches associated with your selection appear.
8. Select the patch you want from the list by clicking its Patch ID link.

9. Click **View Read Me** to read about the patch details, and then click **Download** to download the patch to your computer.
10. Repeat Step 8 through Step 9 for each patch listed in the Patch Search Results section.

> **Note:** Do not apply any Oracle Database one-off patches to the Oracle Audit Vault database unless directed to do so by Oracle Support Services.

3.7.2 Download Critical Patch Updates

A critical patch update (CPU) is a collection of patches for security vulnerabilities. It includes non-security fixes required (because of interdependencies) by those security patches. Critical patch updates are cumulative, and they are provided quarterly on the Oracle Technology Network. You should periodically check My Oracle Support for critical patch updates.

To find and download critical patch updates for Oracle Audit Vault:

1. Follow Step 1 through Step 9 in Section 3.7.1 to find the critical patch updates for Oracle Audit Vault.
2. In the list of articles that appears, search for the phrase `Oracle Critical Patch Update`.
3. Select the most recent critical patch update article, and then read its instructions.

   Download the most recent critical patch update for Oracle Audit Vault. In most critical patch update articles, there is section entitled "Patch Download Procedure," which explains how to download the critical patch update.

For more information about critical patch updates, see:

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

For the latest information on whether a specific critical patch update is certified with Oracle Audit Vault, review the certification matrix on the My Oracle Support Web site, at:

`https://support.oracle.com`

3.7.3 Reset User Passwords

Audit Vault Server uses the password you enter for the Oracle Audit Vault administrator as the password for core database accounts such as SYS, SYSTEM, SYSMAN, and DBSNMP in a basic installation. For an advanced installation, the user is given the option of changing the password for each of these accounts.

For a basic installation, Audit Vault Server also uses the same Oracle Audit Vault Administrator password for the *AV_ADMIN*`dvo` account, the Oracle Database Vault Owner (granted `DV_OWNER` role), to manage Database Vault roles and configuration and the *AV_ADMIN*`dva` account, and the Oracle Database Vault Account Manager (granted `DV_ACCTMGR` role), to manage database user accounts. You must change these passwords according to your company policies.

For an advanced installation, Audit Vault Server uses the Database Vault Owner user password and the separate, optional Database Vault Account Manager user password for these users. You must change these passwords according to your company policies.

See Also: *Oracle Audit Vault Administrator's Guide* for specific information about changing Oracle Audit Vault user passwords on a regular basis and how to change each user password

3.7.3.1 Using SQL*Plus to Reset Passwords

To reset user account passwords using SQL*Plus:

1. Start SQL*Plus and log in as *AV_ADMIN*dva account.
2. Enter a command similar to the following, where password is the new password:

   ```
   SQL> ALTER USER account IDENTIFIED BY password;
   ```

   In this example:

   The IDENTIFIED BY *password* clause resets the password.

   See Also: *Oracle Database Security Guide* for more information about:

   - Changing passwords after installation
   - Oracle security procedures
   - Best security practices

3.7.4 Enable or Disable Connections with the SYSDBA Privilege

Oracle Database Vault allows you to disable remote logins with SYSDBA privileges. This enables enhanced security for your database.

To disable remote SYSDBA connections, re-create the password file with the nosysdba flag set to y (Yes). A user can still log in AS SYSDBA locally using Operating System (OS) authentication. However, remote connections AS SYSDBA will fail.

Use the following syntax to run the orapwd utility:

```
orapwd file=filename password=password [entries=users] force=y/n nosysdba=y/n
```

In this example:

- file is the name of password file (mandatory).
- password is the password for SYS (mandatory). Enter at least six alphanumeric characters.
- entries is the maximum number of distinct DBA users.
- force indicates whether to overwrite the existing file (optional). Enter y (for yes) or n (for no).
- nosysdba indicates whether to enable or disable the SYS logon (optional for Oracle Database Vault only). Enter y (to disable SYS login) or n (to enable SYS login).

  The default is no. If you omit this flag, the password file will be created enabling SYSDBA access for Oracle Database Vault instances.

For example:

```
orapwd file=$ORACLE_HOME/dbs/orapworcl password=password force=y nosysdba=n
```

Note: Do not insert spaces around the equal sign (=).

See Also: *Oracle Database Administrator's Guide* for more information about using the `orapwd` utility

Enable or Disable Connecting with SYSDBA on Oracle Real Application Clusters Systems

Under a cluster file system and raw devices, the password file under *$ORACLE_HOME* is in a symbolic link that points to the shared storage location in the default configuration. In this case, the `orapwd` command that you issue affects all nodes.

Enable or Disable Connecting with SYSDBA on Automatic Storage Management Systems

For Automatic Storage Management systems, you must update each node to enable or disable the `SYSDBA` connection privilege by using the `orapwd` utility.

3.7.5 Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC Only)

After installing Oracle Audit Vault for a Oracle Real Application Clusters (Oracle RAC) instance, you must run Database Vault Configuration Assistant (`DVCA`) with the `-action optionrac` switch on all other Oracle RAC nodes. This sets instance parameters and disables `SYSDBA` operating system authentication.

You must run this command on all Oracle RAC nodes other than the node on which the Oracle Audit Vault installation is performed. This step is required to enable the enhanced security features provided by Oracle Database Vault.

Note: The listener and database instance should be running on the nodes on which you run DVCA.

Use the following syntax to run `DVCA`:

```
# dvca -action optionrac -racnode host_name -oh oracle_home
-jdbc_str jdbc_connection_string -sys_passwd sys_password
[-logfile ./dvca.log] [-silent] [-nodecrypt] [-lockout]
```

In this example:

- `action` is the action to perform. The `optionrac` utility performs the action of updating the instance parameters for the Oracle RAC instance and optionally disabling `SYSDBA` operating system access for the instance.
- `racnode` is the host name of the Oracle RAC node on which the action is being performed. Do not include the domain name with the host name.
- `oh` is the Oracle home for the Oracle RAC instance.
- `jdbc_str` is the JDBC connection string used to connect to the database. For example, `"jdbc:oracle:oci:@orcl1"`.
- `sys_password` is the password for the `SYS` user.
- `logfile` is optionally used to specify a log file name and location. You can enter an absolute path or a path that is relative to the location of the *$ORACLE_HOME*`/bin` directory.
- `silent` is required if you are not running DVCA in an Xterm window.
- `nodecrypt` reads plain text passwords as passed on the command line.

- `lockout` is used to disable `SYSDBA` operating system authentication.

> **Note:** You can reenable `SYSDBA` access by re-creating the password file with the `nosysdba` flag set to `n` (No). The `orapwd` utility enables you to do this.

After running DVCA, stop and restart the instance and database listener on all cluster nodes. This step is also applicable to the node on which Oracle Audit Vault was installed. Use the following commands:

```
srvctl stop instance -d sid -i instance_name -q
Connect String: sys as sysdba
Enter password: sysdbapassword
srvctl stop nodeapps -n node_name
srvctl start nodeapps -n node_name
srvctl start instance -d sid -i instance_name -q
Connect String: sys as sysdba
Enter password: sysdbapassword
```

3.7.6 Download JDBC Driver Files for Source Database Connectivity

Oracle Audit Vault enables you to collect audit records from audit trails in Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), and IBM DB2 databases.

To allow connectivity between Audit Vault Server and Microsoft SQL Server databases, Audit Vault Server and Sybase ASE databases, and Audit Vault Server and IBM DB2 databases, you must download and copy the respective JDBC Driver jar files to the designated location.

Section 3.7.6.1, Section 3.7.6.2, and Section 3.7.6.3 describe this download and copy process for each JDBC Driver.

3.7.6.1 Download SQL Server JDBC Driver for SQL Server Connectivity

Because the SQL Server JDBC Driver 1.2 works with SQL Server 2000 and SQL Server 2005, use SQL Server JDBC Driver 1.2.

Download the Microsoft SQL Server JDBC Driver 1.2 from the following link.

`http://www.microsoft.com/downloads/details.aspx?FamilyID=c47053eb-3b64-4794-950d-81e1ec91c1ba&displaylang=en`

This Type 4 JDBC driver (`sqljdbc.jar`) provides highly scalable and reliable connectivity for the enterprise Java environment and provides JDBC access to SQL Server 2000 and SQL Server 2005 through any Java-enabled applet, application, or application server.

Copy the `sqljdbc.jar` file to the Oracle Audit Vault collection agent home location:

ORACLE_HOME`/jlib`

3.7.6.2 Download jConnect JDBC Driver for Sybase ASE Connectivity

Download jConnect for JDBC, which provides high performance native access to Sybase ASE data sources, from the following link:

`http://www.sybase.com/products/allproductsa-z/softwaredeveloperkit/jconnect`

jConnect for JDBC (`jconn3.jar`) is a high performance JDBC Driver from Sybase that communicates directly to Sybase data sources.

Copy the `jconn3.jar` file to the Oracle Audit Vault Server home location:

```
ORACLE_HOME/jlib
```

3.7.6.3 Copy the IBM DB2 Data Server Driver for JDBC and SQLJ to the Audit Vault Homes

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

This driver provides high performance native access to IBM DB2 database data sources. The DB2 collector uses this driver to collect audit data from IBM DB2 databases, so the driver must be present in Oracle Audit Vault OC4J before you can start the agent OC4J.

3.7.7 Log in to Oracle Audit Vault Console

Use the following instructions to log in to the Oracle Audit Vault Console:

1. On the node from which you installed the database, open a Web browser to access the Oracle Audit Vault Console URL, and use the following URL syntax:

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

   In the preceding example:

   - *host* is the name of the computer on which you installed Oracle Audit Vault Database.
   - *port* is the port number reserved for the Oracle Audit Vault Console during installation.

   If you do not know the correct port number to use, then perform the following steps in the Audit Vault Server home shell:

   a. Set the following environment variables: `ORACLE_HOME`, `ORACLE_SID`, and `PATH`. See *Oracle Audit Vault Administrator's Guide* for more information.

   b. Issue the AVCTL `show_av_status` command. The output displays the Oracle Audit Vault Console URL.

   c. On any system, enter this URL in a Web browser and Oracle Enterprise Manager will display the Oracle Audit Vault Console login page.

2. Log in to the Oracle Audit Vault Console using the user name *AV_ADMIN* and the *AV_ADMIN* password that you created during the installation.

3.7.8 Next Steps to Perform as an Oracle Audit Vault Administrator

After Audit Vault Server installation is complete, see *Oracle Audit Vault Collection Agent Installation Guide* for information about installing Oracle Audit Vault collection agents and the collectors.

After an Oracle Audit Vault collection agent installation is complete, see *Oracle Audit Vault Administrator's Guide* for some Oracle Audit Vault Administration tasks to perform. These tasks include:

1. For Linux and UNIX platforms only: Check and set environment variables in the shells in which you will be interacting with the Audit Vault Server and the Oracle Audit Vault collection agent (see the information about checking and setting Linux and UNIX environment variables).
2. For collecting audit records from Oracle Database audit sources, see the information about registering Oracle Database sources and collectors.
3. For collecting audit records from SQL Server Database audit sources, see the information about registering Microsoft SQL Server sources and collector.
4. For collecting audit records from Sybase ASE Database audit sources, see the information about registering Sybase ASE database sources and collector.
5. For collecting audit records from IBM DB2 database audit sources, see the information about registering IBM DB2 sources and collector.
6. To start collecting audit records from a database audit source, see the information about starting collection agents and collectors.
7. To perform other Oracle Audit Vault configuration tasks, see the information about performing additional Oracle Audit Vault configuration tasks.
8. To manage and monitor an Oracle Audit Vault system, see the information about managing Oracle Audit Vault.
9. Before going into production be sure to secure management communications, see the information about Oracle advanced security and secure management communication.

4

Upgrading Oracle Audit Vault Server

This chapter describes the procedure to upgrade an Oracle Audit Vault Server (Audit Vault Server) installation from release 10.2.2.1.0 or earlier to release 10.2.3.0.0. This chapter covers the following topics:

4.1 Back Up and Recovery of Audit Vault Server

You cannot roll back the Audit Vault Server upgrade installation. Back up the current installation before performing the upgrade.

Back Up the Database

After cleanly shutting down the instance following the analysis of the database, you should perform a full backup of the database. Complete the following steps:

1. Sign on to RMAN:

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

2. Issue the following RMAN commands:

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

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

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

Back Up Audit Vault Server Home

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

Abandon the Upgrade

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

1. Copy (Restore) the 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;
}
```

4.2 Upgrade Requirements

The only requirement to perform an upgrade to Audit Vault Server 10.2.3.0.0 is that Oracle Universal Installer detects an older release of an Audit Vault Server (release 10.2.2.1.0 or earlier) installed on your system.

4.3 Upgrade Procedure

To upgrade to Audit Vault Server release 10.2.3.0.0, you must follow this sequence of steps to shut down Oracle Audit Vault components, perform the server upgrade, perform the collection agent upgrade, then start up Oracle Audit Vault components:

- Step 1: Ensure the NLS_LANG Environment Variable Is Not Set
- Step 2: Stop All Collectors
- Step 3: Stop All Collection Agents
- Step 4: Stop the Agent OC4J
- Step 5: Stop the Oracle Audit Vault Console
- Step 6: Shut Down the Oracle Audit Vault Database
- Step 7: Stop the Listener
- Step 8: Perform the Upgrade to Audit Vault Server Release 10.2.3.0.0 in the Audit Vault Server Home

- Step 9: Perform the Upgrade to Oracle Audit Vault Collection Agent Release 10.2.3.0.0 in the Oracle Audit Vault Collection Agent Homes

  See the information about upgrading an Oracle Audit Vault collection agent in *Oracle Audit Vault Collection Agent Installation Guide* for more information.
- Step 10: Start All Collection Agents
- Step 11: Start All Collectors
- Step 12: Monitor the Oracle Audit Vault System

Details of each of these steps follows.

Step 1: Ensure the NLS_LANG Environment Variable Is Not Set

The `NLS_LANG` environment variable must not be set.

For example, for C shell:

```
unsetenv NLS_LANG
```

For example, for Bourne, Bash, or Korn shells:

```
unset NLS_LANG
```

Step 2: Stop All Collectors

You must stop all collectors associated with the Audit Vault Server to which this upgrade installation is being applied.

From the Audit Vault Server home with `ORACLE_HOME`, `ORACLE_SID`, and `PATH` environment variables properly set for the Audit Vault Server home, use the following command syntax to stop each collector.

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

Step 3: Stop All Collection Agents

You must stop all collection agents associated with the Audit Vault Server to which this upgrade installation is being applied.

From the Audit Vault Server home with `ORACLE_HOME`, `ORACLE_SID`, and `PATH` environment variables properly set for the Audit Vault Server home, use the following command syntax to stop each collection agent.

```
avctl stop_agent -agentname agent-name
```

Step 4: Stop the Agent OC4J

You must stop all agent OC4J associated with the Audit Vault Server to which this upgrade installation is being applied. There is one agent OC4J associated with each collection agent.

From each Oracle Audit Vault collection agent home with `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables properly set for the Oracle Audit Vault collection agent home, use the following command syntax to stop each agent OC4J.

```
avctl stop_oc4j
```

Step 5: Stop the Oracle Audit Vault Console

From the Audit Vault Server home with `ORACLE_HOME`, `ORACLE_SID`, and `PATH` environment variables properly set for the Audit Vault Server home, use the following command syntax to stop the Oracle Audit Vault Console.

```
avctl stop_av
```

In an Oracle RAC environment, run the command on all nodes where Audit Vault Server is installed.

> **Note:** In an Oracle RAC environment, do not shut down Enterprise Manager on the remote nodes; otherwise, you will have to manually start up Enterprise Manager on these remote nodes following an upgrade to Audit Vault Server release 10.2.3.0.0.

Step 6: Shut Down the Oracle Audit Vault Database

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

```
sqlplus /nolog
SQL*Plus: Release 10.2.0.3.0 - Production on Thu Dec 13 22:51:56 2007
Copyright (c) 1982, 2007, Oracle.  All Rights Reserved.
SQL> connect sys as sysoper
Enter password:
Connected.
SQL>
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
```

Step 7: Stop the Listener

From the Audit Vault Server home, use the following command to stop the listener. The listener name is usually LISTENER. Perform the `lsnrctl status` command to determine the name of the listener.

```
$ORACLE_HOME/bin/lsnrctl stop Listener-name
```

In an Oracle RAC environment, run the command on all nodes where Audit Vault Server is installed.

Step 8: Perform the Upgrade to Audit Vault Server Release 10.2.3.0.0 in the Audit Vault Server Home

Perform the following steps to perform the upgrade installation to Audit Vault Server release 10.2.3.0.0 in the Audit Vault Server home:

1. Locate the Audit Vault Server release 10.2.3 media and mount the media.
2. Start Oracle Universal Installer (OUI) from the directory where the runInstaller program is located.

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

3. On the **Oracle Audit Vault Server Installation Select Installation Type** window, when the installer detects an upgradable release, it automatically selects the **Upgrade Existing Audit Vault Server Home** option and displays the upgradeable home path specifications. If there is more than one upgradable path to upgrade, review the path names, and select the path specification to upgrade. Then click **Next**.
4. The **Summary Page** screen is displayed. Check the space requirements. Note that 662 MB of space is required to upgrade to Audit Vault Server 10.2.3.0.0, which includes 117 MB of temporary space. Next, review each of the items that are about to be installed. Click **Install**.
5. The **Configuration Assistants** screen appears and proceeds to apply Audit Vault Server one-off patches and then the Oracle Audit Vault Upgrade Assistant runs some AVCA scripts to continue the release 10.2.3 upgrade installation.
6. On the **End of Installation** screen, you should see a message indicating a successful installation. Take note of the URL for the Oracle Audit Vault Console 10.2.3.0.0. Click **Exit** to exit the Oracle Universal Installer. Then on the **Exit** confirmation screen for the prompt "Do you really want to exit?", click **Yes** to confirm the exit operation.

See *Oracle Audit Vault Collection Agent Installation Guide* for information on upgrading all Oracle Audit Vault collection agent release 10.2.2.1.0 or earlier collection agents that are associated with your recently upgraded Audit Vault Server installation to release 10.2.3.0.0.

Step 9: Perform the Upgrade to Oracle Audit Vault Collection Agent Release 10.2.3.0.0 in the Oracle Audit Vault Collection Agent Homes

> **Note:** All release 10.2.2.1.0 or earlier Oracle Audit Vault collection agents associated with the recently upgraded Audit Vault Server to release 10.2.3.0.0 can now be upgraded to Oracle Audit Vault collection agent release 10.2.3.0.0 to maintain compatibility with this most current release of the Audit Vault Server. See the information about upgrading an Oracle Audit Vault collection agent in *Oracle Audit Vault Collection Agent Installation Guide* for more information.

Step 10: Start All Collection Agents

From the Audit Vault Server home with `ORACLE_HOME`, `ORACLE_SID`, and `PATH` environment variables properly set for the Audit Vault Server home, use the following command syntax to start each collection agent.

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

Step 11: Start All Collectors

From the Audit Vault Server home with `ORACLE_HOME`, `ORACLE_SID`, `PATH`, and `LD_LIBRARY_PATH` environment variables properly set for the Audit Vault Server home, use the following command syntax to start each collector.

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

Step 12: Monitor the Oracle Audit Vault System

This step is a reminder to monitor the Oracle Audit Vault system to ensure all Oracle Audit Vault components are running and the system is operational. See the *Oracle Audit Vault Administrator's Guide* for more information.

4.4 Performing a Silent Upgrade Installation Using a Response File

Note: The basic installation is not supported in silent mode. Silent installation is only supported for the advanced upgrade installation.

Follow these brief steps to perform a silent upgrade installation using a response file:

1. Make sure all prerequisites are met for the installation of Audit Vault Server and Oracle Audit Vault collection agent.
2. Prepare the Audit Vault Server response file. A template response file can be found at *AV-installer-location*`/response/upgrade_av.rsp` on the Audit Vault Server installation media.

   Prepare the response file by entering values for all parameters that are missing in the first part of the response file, then save the file. Note that for single instance installations, RAW storage is not used. Also note that the `CLUSTER_NODES` parameter must be specified for installing Audit Vault Server in an Oracle RAC environment. Do not edit any values in the second part of either response file.
3. Set the `DISPLAY` environment variable to an appropriate value before proceeding with the silent installation. See Section 2.11 for more information.
4. Invoke Oracle Universal Installer using the following options:

   ```
   ./runInstaller -silent -responseFile path_of_response_file
   ```

For more information about these options, see Section 1.3.2. For general information about how to complete a database installation using response files, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*.

4.5 Post Upgrade Information

Note that after performing an Oracle Audit Vault Server upgrade, because the upgrade is an inplace upgrade, the original directory structure is still in use. This means the `ORACLE_HOME`, `PATH`, and `LD_LIBARARY_PATH` environment variables are the same as they were before the upgrade.

See Section 3.7 for any additional post upgrade installation tasks.

5

Removing the Oracle Audit Vault Server Software

This chapter describes the process of removing the Oracle Audit Vault Server (Audit Vault Server) software.

To remove Audit Vault Server software, all Oracle Audit Vault collection agents must be stopped if the Oracle Audit Vault collection agent software is installed on the same system as the Audit Vault Server software. See *Oracle Audit Vault Collection Agent Installation Guide* for more information.

Then, use the following procedure to uninstall the Audit Vault Server software.

1. Stop the Oracle Audit Vault Console using the `avctl stop_av` command.

   This command performs an emctl stop dbconsole operation. For example:

   ```
   $ avctl stop_av
   ```

   In an Oracle RAC environment, run that command on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

2. Start the Database Configuration Assistant to delete the Oracle Audit Vault database and then stop the listener.

   Perform the following steps:

   a. Start the Database Configuration Assistant from the command-line.

      ```
      $ dbca
      ```

      The Welcome window appears.

   b. Click **Next**.

      The Operations window appears.

   c. Select **Delete a Database**, then click **Next**.

   d. Select the Oracle Audit Vault database that you want to delete, then click **Finish**.

   e. In the window that appears, confirm that you want to delete the Oracle Audit Vault database.

   f. When the Database Configuration Assistant removes the Audit Vault database, you are prompted to choose whether you want to perform another operation. Click **No** to exit from the Database Configuration Assistant.

In an Oracle RAC environment, run the Database Configuration Assistant on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

g. Stop the listener.

Look in the `listener.ora` file to check the name of the listener. It might be `LISTENER1` or some other name, but usually it is `LISTENER`. For example:

```
$ lsnrctl stop listener-name
```

In an Oracle RAC environment, run that stop listener command on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

3. Uninstall the Audit Vault Server by running the following command in the Audit Vault Server home directory. For example:

```
$ $ORACLE_HOME/oui/bin/runInstaller
```

Note: Before removing the Audit Vault Server software, first use the DBCA "Delete a database" option to select and delete the database. See *Oracle Database 2 Day DBA* and *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide* for more information about using DBCA to delete a database.

---

4. Click **Deinstall Products** to bring up the Oracle Inventory screen.

Select the Oracle homes and the products that you want to remove by selecting the desired check boxes, then click **Remove**.

5. Clean up the old Oracle directories.

On systems where Oracle Audit Vault is the only Oracle software installed, go to the directory for `oracle`, and remove the directory using the `rm -r` command. Otherwise, delete the Audit Vault Server home.

Issue the following command to confirm there is no other Oracle home installed.

```
$ grep 'HOME NAME' OraInventory/ContentsXML/inventory.xml
```

In an Oracle RAC environment, perform these operations on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

Index

P

R

S

T

U

W

X