Oracle® Audit Vault

Server Installation Guide

10*g* Release 2 (10.2.2) for Linux x86

B25322-01

April 2007

ORACLE®

Oracle Audit Vault Server Installation Guide, 10*g* Release 2 (10.2.2) for Linux x86

B25322-01

Primary Author: Rod Ward and Prakash Jashnani

Contributing Author: Sumit Jeloka, Nilima Kapoor, Robert Chang, K Karun

Contributor: Vipul Shah, Jack Brinson, Tammy Bednar, Donna Keesling, Martin Widjaja, Mayur Mundada, Trivikrama Samudrala, Sarma Namuduri, Luann Ho, Dineshsing Patil, Alan Galbreath

Contents

Preface vii

Audience vii
Documentation Accessibility vii
Related Documents viii
Conventions viii

1 Oracle Audit Vault Server Installation Overview

1.1 Overview of Oracle Audit Vault 1-1
1.2 Overview of the Oracle Audit Vault Installation Process 1-5
1.3 Audit Vault Installation Components 1-5
1.4 Audit Vault Installation Methods 1-6
1.4.1 Interactive Installation Methods 1-6
1.4.2 Automated Installation Methods Using Response Files 1-6
1.5 Audit Vault Server Installation 1-6
1.6 Installation Considerations 1-7
1.6.1 Hardware and Software Considerations 1-7
1.6.2 Multiple Oracle Homes 1-8

2 Oracle Audit Vault Server Preinstallation Requirements

2.1 Becoming Familiar with the Features of Oracle Audit Vault 2-1
2.2 Logging In to the System as the root User 2-1
2.3 Checking the Hardware Requirements 2-1
2.4 Checking the Operating System Requirements 2-3
2.5 Checking the Network Setup 2-4
2.5.1 Configuring Name Resolution 2-5
2.5.2 Installing on DHCP Computers 2-5
2.5.3 Installing on Computers with Multiple Homes 2-6
2.5.4 Installing on Computers with Multiple Aliases 2-6
2.6 Creating Required Operating System Groups and Users 2-6
2.6.1 Creating the Oracle Inventory Group 2-8
2.6.2 Creating the OSDBA Group 2-8
2.6.3 Creating an OSOPER Group (Optional) 2-9
2.6.4 Creating the Oracle Software Owner User 2-9
2.6.4.1 Determining Whether an Oracle Software Owner User Exists 2-9
2.6.4.2 Creating an Oracle Software Owner User 2-10

2.6.4.3 Modifying an Oracle Software Owner User 2-10
2.6.5 Verifying that the User nobody Exists 2-10
2.7 Checking the Kernel Parameters 2-10
2.8 Identifying Required Software Directories 2-13
2.8.1 Oracle Base Directory 2-13
2.8.2 Oracle Inventory Directory 2-14
2.8.3 Oracle Home Directory 2-14
2.9 Identifying or Creating an Oracle Base Directory 2-15
2.9.1 Identifying an Existing Oracle Base Directory 2-15
2.9.2 Creating an Oracle Base Directory 2-16
2.10 Creating Directories for Oracle Audit Vault Database Files 2-16
2.11 Setting the DISPLAY Environment Variable 2-17

3 Installing Audit Vault Server

3.1 Accessing the Server Installation Software 3-1
3.2 Audit Vault Server Installation Details 3-1
3.2.1 Basic and Advanced Installation Details Screens 3-1
3.2.1.1 Audit Vault Name 3-2
3.2.1.2 Audit Vault Home 3-2
3.2.1.3 Audit Vault Server Accounts 3-2
3.2.2 Advanced Server Installation: Database Vault User Credentials Screen 3-5
3.2.2.1 Database Vault Owner and Database Vault Account Manager Accounts 3-5
3.2.2.2 Database Vault Owner and Database Vault Account Manager Passwords 3-6
3.2.3 Advanced Server Installation: Node Selection Screen 3-6
3.2.4 Advanced Server Installation: Specify Database Storage Options Screen 3-6
3.2.5 Advanced Server Installation: Specify Backup and Recovery Option Screen 3-7
3.2.6 Advanced Server Installation: Specify Database Schema Passwords Screen 3-8
3.2.7 Default Audit Policy and Initialization Parameters 3-8
3.3 Basic Installation -- Performing the Single Instance Server Installation 3-8
3.4 Advanced Installation -- Prerequisite Information for Installing in an Oracle Real Application Clusters Environment 3-10
3.4.1 Verifying System Readiness for Installing Oracle Audit Vault with CVU 3-10
3.5 Advanced Installation -- Installing Single Instance and in an Oracle Real Application Clusters Environment 3-11
3.6 Performing a Silent Installation Using a Response File 3-14
3.7 Postinstallation Server Tasks 3-15
3.7.1 Unlocking and Resetting User Passwords 3-15
3.7.1.1 Using SQL*Plus to Unlock Accounts and Reset Passwords 3-16
3.7.2 Enabling or Disabling Connections with the SYSDBA Privilege 3-16
3.7.3 Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC only) 3-17
3.7.4 Logging in to Audit Vault Console 3-18

4 Removing Audit Vault Server Software

4.1 Removing Audit Vault Server Software 4-1

Index

List of Figures

1–1 Oracle Audit Vault Architecture..... 1-2
1–2 Usage Scenario Showing Important Roles of Audit Vault Administrators 1-5

List of Tables

1–1 Audit Vault Administrator Roles and Their Assigned Tasks 1-3
2–1 Operating System, Kernel Version, and Packages Requirements 2-3
3–1 Invalid Audit Vault Name and Audit Vault Account Characters 3-2
3–2 Special Characters Allowed in the Audit Vault Home Name 3-2
3–3 Reserved Names That Cannot Be Used in Audit Vault Account Names 3-3
3–4 Valid Audit Vault Administrator and Audit Vault Auditor Password Characters 3-5

Preface

The Oracle Audit Vault Server Installation Guide explains how to prepare for, install, and configure Oracle Audit Vault Server with specific instructions for the operating system and Oracle software technology components that Audit Vault Server requires.

Audience

This document is intended for Oracle DBAs and System Administrators as well as those who are involved in the installation of Oracle Audit Vault and its related components.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

For more information, refer to the following documents:

- *Oracle Audit Vault Release Notes*
- *Oracle Audit Vault Agent Installation Guide*
- *Oracle Audit Vault Licensing Information*
- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Database Installation 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*

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.

1.1 Overview of Oracle Audit Vault

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

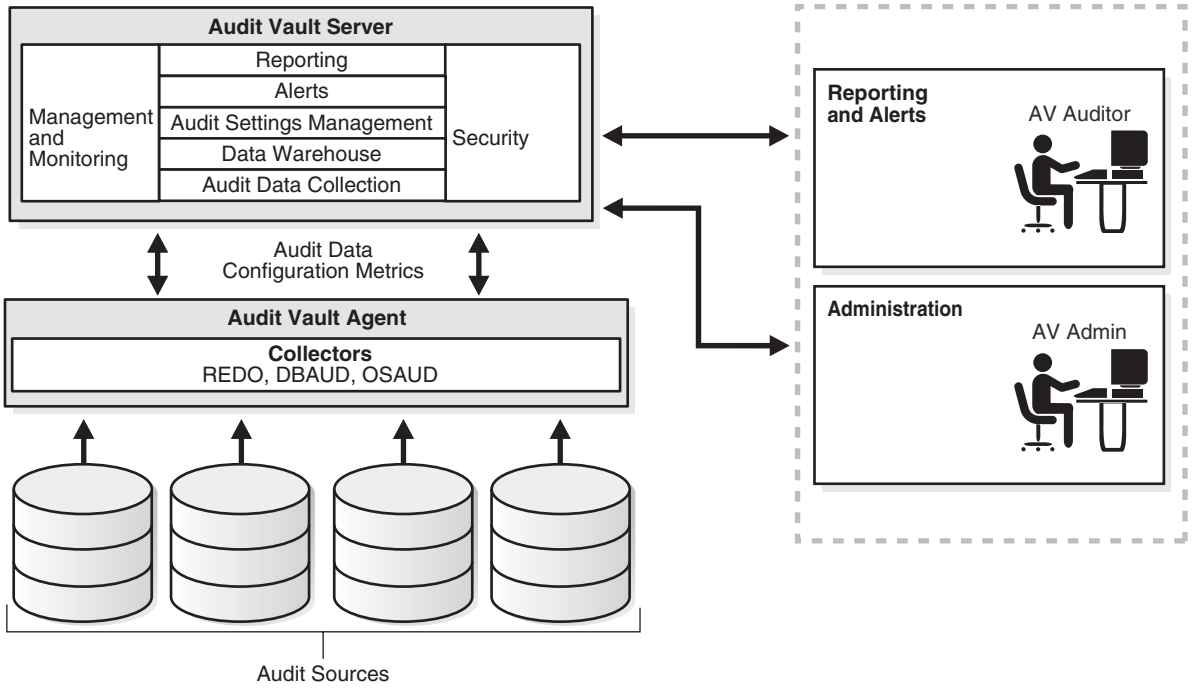
Businesses use a wide variety of systems, databases, and applications that produce vast quantities of audit log data and must consolidate and monitor this data for a holistic view of enterprise data access. Auditors must analyze the audit log data in a timely fashion across disparate and heterogeneous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

Oracle Audit Vault solves these security and audit problems by:

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

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

Figure 1–1 Oracle Audit Vault Architecture



Oracle Audit Vault Components

Oracle Audit Vault consists of:

- Audit Vault Server
- Audit Vault Agents

Audit Vault Server

Audit Vault Server consists of:

- Audit event repository
- Audit Vault Console
- The following services:
  - Audit data collection and storage
  - Creating and managing alerts
  - Managing and monitoring collectors
  - Configuration to assist in defining information about what sources are known to Audit Vault. It stores information (metadata) about the sources of audit data and policy information (database audit settings and alerts).
  - Creating and managing reports
  - Published data warehouse that can be used with reporting tools like Oracle BI Publisher to create customized reports
  - Audit policy management

Audit Vault Agents

Audit Vault Agents consists of:

- Oracle Database client
- Oracle Container for Java (OC4J)
- Audit Vault management services
- Audit data collectors for Oracle Database
- Collecting audit data from Oracle Database operating system (OSAUD) audit logs, database (DBAUD) audit logs, and (REDO) redo logs

Oracle Audit Vault Interfaces and Administrator Access

Oracle Audit Vault provides a GUI interface and the Audit Vault Configuration Assistant (AVCA), Audit Vault Control (AVCTL), and Audit Vault Oracle Database (AVORCLDB) command-line utilities to manage the system. These components provide the ability to manage and monitor agents and collectors, and populate the data warehouse. See *Oracle Audit Vault Administrator's Guide* for information about these interfaces.

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

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

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

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

Role	When Is Role Granted	Role Is Granted To Whom	Description
AV_ADMIN	During Server installation	Audit Vault administrator	Accesses Oracle Audit Vault services to administer, configure, and manage a running Oracle Audit Vault system. A user granted this role configures and manages audit sources, agents, collectors, the set up of the source with the agent, and the warehouse. A user is created and granted this role during the Audit Vault Server installation.
AV_AUDITOR	During Server installation	Audit Vault auditor	Accesses Audit Vault reporting and analysis services to monitor components, detect security risks, create and evaluate alert scenarios, create detail and summary reports of events across systems, and manage the reports. A user granted this role manages central audit settings and alerts. This user also uses the data warehouse services to further analyze the audit data to assist in looking for trends, intrusions, anomalies, and other items of interest. A user is created and granted this role during the Audit Vault Server installation.
AV_AGENT	Before agent installation	Agent software component	Manages agents and collectors by starting, stopping, and resetting them. A user is created and granted this role prior to an agent installation. The Agent software uses this role at run time to query Audit Vault for configuration information
AV_SOURCE	Before source registration	Collector software component	Manages the setting up of the sources for audit data collection. A user is created and granted this role prior to source and collector configuration. The collector software uses this role at run time to send audit data to Audit Vault

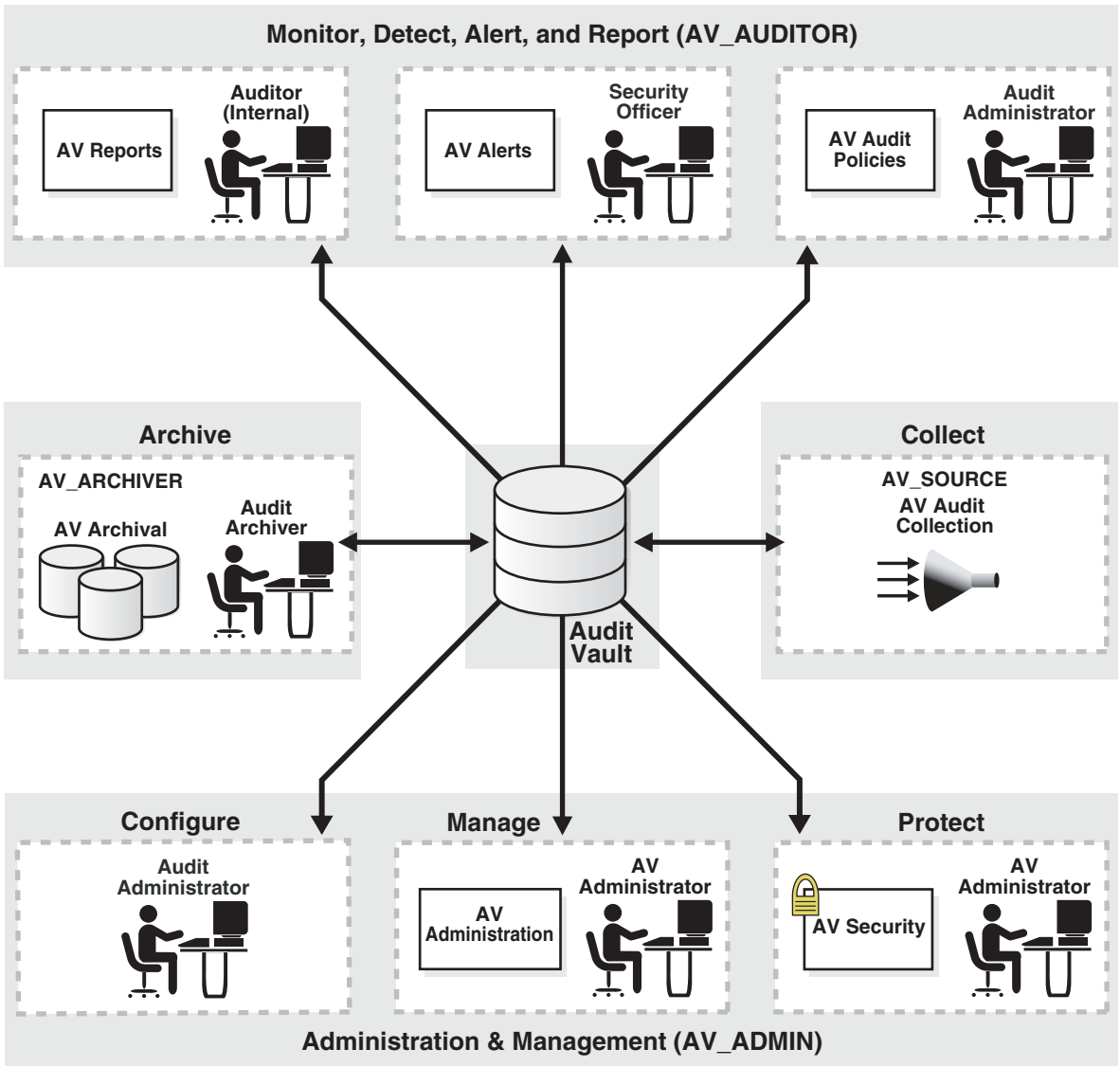
Table 1–1 (Cont.) Audit Vault Administrator Roles and Their Assigned Tasks

Role	When Is Role Granted	Role Is Granted To Whom	Description
AV_ARCHIVER	Before archiving audit data	Audit Vault archiver	Archives and deletes audit data from Audit Vault and cleans up old unused metadata and alerts that have already been processed. A user granted this role can archive raw audit data.
DV_OWNER	During Server installation	Database Vault owner	Manages Database Vault roles and configuration and grants Audit Vault roles.
DV_ACCTMGR	During Server installation	Database Vault account manager	Manages database user accounts.

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

Figure 1–2 shows a detailed view of the various Audit Vault usage scenarios for which each of the Oracle Audit Vault administrator roles described in Table 1–1 plays an important role.

Figure 1–2 Usage Scenario Showing Important Roles of Audit Vault Administrators



1.2 Overview of the Oracle Audit Vault Installation Process

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

- Audit Vault Installation Components
- Audit Vault Installation Methods
- Audit Vault Server Installation
- Installation Considerations

1.3 Audit Vault Installation Components

Oracle Audit Vault software installation consists of two parts:

- Oracle Audit Vault Server installation that can be either:
  - Single Instance installation

  - Clustered using Oracle Real Application Clusters (Oracle RAC) installation
- Oracle Audit Vault Agent installation (see *Oracle Audit Vault Agent Installation Guide*)

1.4 Audit Vault Installation Methods

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

- Interactive Installation Methods
- Automated Installation Methods Using Response Files

1.4.1 Interactive Installation Methods

When you use the interactive method to install Oracle Audit Vault, 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.

1.4.2 Automated Installation Methods Using Response Files

Audit Vault provides a response file template for Audit Vault Server (`av.rsp`). The response template file 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 Oracle 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, Oracle Universal Installer can run in silent or non-interactive mode. In 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 install 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 3.6 for information about performing an Audit Vault silent installation:

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

1.5 Audit Vault Server Installation

The server installation consists of two options:

- 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.

The Audit Vault Console uses a wallet in the `$ORACLE_HOME/network/admin/avwallet` directory. An Oracle wallet is a password-protected container that stores credentials, such as certificates, authentication credentials, and private keys, all of which are used by Secure Sockets Layer (SSL) for strong authentication. Oracle wallets are managed through the Oracle Wallet Manager. The Oracle Wallet Manager can perform tasks such as creating wallets, requesting certificate generation, and importing certificates into the wallet.

The wallet is used to store the user name and password of the user granted the `AV_ADMIN` role. This user name is used by the Audit Vault Console to allow communication with Audit Vault. Audit Vault Console provides the management service that initiates the communication with agents using HTTP. Audit Vault Configuration Assistant (AVCA) modifies the Oracle Enterprise Manager Database Control console `server.xml` file and other related files to enable Audit Vault management through the Audit Vault Console.

If certificate-based authentication is used for communication with any agent, the Audit Vault Administrator must acquire the necessary server-side certificates and set up Oracle Wallet for storing the certificates on the server. This server-side certificate is used for authenticating the Audit Vault Server to the agent. Similarly, agents must each have a certificate to authenticate each agent to the Audit Vault Server.

Communication at the management level between Audit Vault Server and Audit Vault 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 Audit Vault Management Service on the server side and each agent over HTTPS.

After checking the requirements described in Section 1.6, the general steps to install Oracle 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.

1.6 Installation Considerations

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

- Hardware and Software Considerations
- Multiple Oracle Homes

1.6.1 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 Oracle*MetaLink* Web site for the most up-to-date list of certified hardware platforms and operating system versions. The Oracle*MetaLink* Web site is available at:

http://metalink.oracle.com

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

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

1.6.2 Multiple Oracle Homes

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

2

Oracle Audit Vault Server Preinstallation Requirements

This chapter describes the following Oracle Audit Vault Server preinstallation requirements.

- Becoming Familiar with the Features of Oracle Audit Vault
- Logging In to the System as the root User
- Checking the Hardware Requirements
- Checking the Operating System Requirements
- Checking the Network Setup
- Creating Required Operating System Groups and Users
- Checking the Kernel Parameters
- Identifying Required Software Directories
- Identifying or Creating an Oracle Base Directory
- Creating Directories for Oracle Audit Vault Database Files
- Setting the DISPLAY Environment Variable

2.1 Becoming Familiar with the Features of Oracle Audit Vault

Before you plan the installation process, you need to become 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 need to complete several tasks described in the sections that follow as the `root` user. Log into 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 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
  - 1.4 GB of disk space for the Oracle Audit Vault Server software files in the Oracle Base
  - 700 MB of additional disk space for the Audit Vault Server database files in the Oracle Base. This is only if the database storage option is on the file system. For other storage options, such as ASM, the database files will be stored elsewhere. Also, this 700MB disk space is only the starting size. The Audit Vault administrator must take future growth of the database size into consideration, especially as the server collects more and more audit data.

To ensure that the system meets these requirements:

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 freezing on 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 (described later).
   - 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

Depending on the products that you intend to install, verify that the following software is installed on the system. The procedure following Table 2–1 describes how to verify whether these requirements are addressed.

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

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

Item	Requirement
Operating system	One of the following operating system versions: ■ Red Hat Enterprise Linux 3.0 (Update 3 or later) ■ Red Hat Enterprise Linux 4.0 ■ SUSE Linux Enterprise Server 9.0 ■ Asianux 2.0 The operating system requirements are the same as those for Oracle Database 10*g* release 2. If you already have Oracle Database 10*g* release 2 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 3.0:** 2.4.21-27.EL **Note:** This is the default kernel version. **Red Hat Enterprise Linux 4.0 and Asianux 2.0:** 2.6.9-5.0.5.EL **SUSE Linux Enterprise Server 9.0:** 2.6.5-7.97 The kernel version requirements are the same as those for Oracle Database 10*g* release 2. If you already have Oracle Database 10*g* release 2 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 package requirements are the same as those for Oracle Database 10*g* release 2. If you already have Oracle Database 10*g* release 2 installed, then your system automatically meets the package requirements.

To ensure that the system meets these requirements:

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
   ```

   The following is sample output obtained by running this command on a Red Hat Enterprise Linux 3.0 system:

   ```
   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 earlier in this section, 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 Oracle Audit Vault on computers that do not meet the typical scenario. It covers the following cases:

- Configuring Name Resolution
- Installing on DHCP Computers
- Installing on Computers with Multiple Homes

- Installing on Computers with Multiple Aliases

2.5.1 Configuring Name Resolution

When you run Oracle Universal Installer, an error may occur if name resolution is not set up. To avoid this error, before you begin 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.mycomputer.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:

   ```
   192.168.100.16    myhost.us.mycompany.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.

Audit Vault cannot be installed in an environment where the IP addresses of the Audit Vault Server or the Audit Vault Agent can change. If your environment uses DHCP, ensure that all Audit Vault machines use static IP addresses.

2.5.3 Installing on Computers with Multiple Homes

You can install Oracle Audit Vault on a computer that has multiple homes. A multiple-homed computer is associated with multiple IP addresses. This is typically achieved by having multiple network cards on the computer. 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 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 need to 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 (hostname only) and the full name (hostname 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 `somehost.us.acme.com`, then enter one of the following commands:

Bourne, Bash, or Korn shell:

```
$ ORACLE_HOSTNAME=somehost.us.acme.com
$ export ORACLE_HOSTNAME
```

C shell:

```
% setenv ORACLE_HOSTNAME somehost.us.acme.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 Oracle Audit Vault 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 Required Operating System Groups and Users

Depending on whether or not this is the first time Oracle software is being installed on this system and on the products that you are installing, you may need to create several operating system groups and users.

The following operating system groups and user are required if you are installing Oracle Audit Vault:

- The OSDBA group (`dba`)

  You must create this group the first time you install Oracle Audit Vault 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 sections 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 the 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.

A single Oracle Inventory group is required for all installations of Oracle software on the system. 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 Audit Vault Administrator's Guide* for more information about the OSDBA group and the `SYSDBA` and `SYSOPER` privileges

Note: The following sections 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 sections 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 subsections 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 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` 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. Refer to one of the following sections for more information:

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

- If you want to use an existing Oracle software owner user, and the primary group of the user is the Oracle Inventory group, then see Section 2.6.4.1.
- To modify an existing user, see Section 2.6.4.3.
- To create a user, refer to 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 values only. 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.

Verify that the kernel parameters shown in the following table are set to values greater than or equal to the recommended value shown.

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 value 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 need to 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.
file-max	`# /sbin/sysctl -a | grep file-max` This command displays the maximum number of file handles.

Parameter	Command
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 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.

```
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
```

   By specifying 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
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 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 sections describe how to identify existing Oracle base directories that may 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/10.2.2/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 create this directory.

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 information about the following:

- 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 may 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 specified 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 Table 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 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 later in this chapter, 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 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 install, 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.oracle.com` is your host name:

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

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

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

3

Installing Audit Vault Server

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

This chapter includes the following topics:

- Accessing the Server Installation Software
- Audit Vault Server Installation Details
- Basic Installation -- Performing the Single Instance Server Installation
- Advanced Installation -- Prerequisite Information for Installing in an Oracle Real Application Clusters Environment
- Advanced Installation -- Installing Single Instance and in an Oracle Real Application Clusters Environment
- Performing a Silent Installation Using a Response File
- Postinstallation Server Tasks

3.1 Accessing the Server Installation Software

The Oracle Audit Vault Server software is available on digital video disc (DVD).

3.2 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 two options:

- **Basic Installation** -- simplifies the installation process and prompts for a minimal set of inputs, including the name of the Audit Vault database, the Audit Vault Administrator and optionally the 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.

3.2.1 Basic and Advanced Installation Details Screens

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

3.2.1.1 Audit Vault Name

The Audit Vault Name must be a unique name for the 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 Audit Vault name cannot contain any of the characters shown in Table 3–1.

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

Symbol	Character Name	Symbol	Character Name	Symbol	Character Name
!	Exclamation point	"	Double quote mark	<	Less than sign
@	At sign	|	Vertical bar	>	Greater than sign
%	Percent sign	`	grave	/	Slash
^	Circumflex	~	tilde	\	Backslash
&	Ampersand	[	Left bracket	?	Question mark
*	Asterisk	{	Left brace	,	Comma
(	Left parenthesis	]	Right bracket	.	Period
)	Right parenthesis	}	Right brace	#	Number sign
-	Minus sign	;	Semicolon	_	Underscore
+	Plus sign	:	Colon	$	Dollar sign
=	Equal sign	'	Single quotation mark		Space character

3.2.1.2 Audit Vault Home

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

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

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

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

3.2.1.3 Audit Vault Server Accounts

The Audit Vault Server installation software prompts you for user names and passwords for the Audit Vault Administrator user and the separate, optional Audit Vault Auditor user. In addition, a Database Vault Owner user and a separate, optional Database Vault Account Manager user are created for you (basic installation) or the installation prompts you for these user names and passwords (advanced installation). Finally, `sys`, `system`, `sysman`, and `dbsnmp` standard database users are created for you (basic installation) or the installation prompts for passwords for these users (advanced installation).

You need to supply a user name and password for the Audit Vault Administrator and optionally for the Audit Vault Auditor during installation. The **Create a Separate Audit Vault Auditor** check box is selected by default, which means that a separate

Audit Vault Auditor account will be created (and the corresponding user name and password are required). The Audit Vault Administrator user will be granted the AV_ADMIN role and the Audit Vault Auditor user will be granted the AV_AUDITOR role. Deselecting this check box means the Audit Vault Administrator user will be granted both roles because the separate Audit Vault Auditor user will not be created.

Audit Vault Administrator and Audit Vault Auditor Accounts

The 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 manages the audit services including source creation and parameters, and sources and their channels. This role registers audit sources, defines plug-ins for translation, and manages central audit settings. For the basic installation, the Audit Vault Administrator user name is used to generate the following Oracle Database Vault roles to facilitate the separation of duties:

- *AV_ADMIN*dvo-- the Database Vault Owner (granted DV_OWNER role) to manage Database Vault roles and configuration
- *AV_ADMIN*dva -- the 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 Audit Vault Auditor account is granted the AV_AUDITOR role. The user granted the AV_AUDITOR role accesses Audit Vault Reporting and Analysis services to monitor components, detect security risks, create and evaluate alert scenarios, create detail and summary reports of events across systems, and manage the reports. This role has the ability to configure parameters that assist in populating the Audit Vault Data Warehouse. 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 Audit Vault Administrator, Audit Vault Auditor, Database Vault Owner, and Database Vault Account Manager user names must not be the same. For the basic installation, the 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 number of characters allowed to be 27 characters. For the advanced installation, the Audit Vault Administrator user name must be between 2 and 30 characters.

The length of the Audit Vault Auditor user name must be between 2 and 30 characters. Each user name must not be one of the reserved names shown in Table 3–3.

Table 3–3 Reserved Names That Cannot Be Used in Audit Vault Account 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
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

Table 3–3 (Cont.) Reserved Names That Cannot Be Used in Audit Vault Account Names

Names	Names	Names	Names	Names
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 Audit Vault Administrator password entered for the Audit Vault Administrator account is also used for the standard database accounts (`sys`, `system`, `sysman`, `dbsnmp`). For the basic installation **Details** page, the 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 Audit Vault Administrator for all of these accounts. In addition, a **Database Vault User Credentials** page prompts for the Database Vault Owner user password and for a separate, optional Database Vault Account Manager user password if that user is created.

The Audit Vault Administrator and Audit Vault Auditor password cannot be the name of the Audit Vault Administrator, Audit Vault Auditor, Database Vault Owner, or Database Vault Account Manager. The Audit Vault Administrator user password is required, while the Audit Vault Auditor user password is only required when creating the separate, optional 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 following special characters shown in Table 3–4.

Table 3–4 Valid Audit Vault Administrator and Audit Vault Auditor Password Characters

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

Each password must be identical to its corresponding password confirmation.

3.2.2 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 Database Vault Owner account and the separate, optional Database Vault Account Manager account. You need to 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 Database Vault Account Manager account will be created (and the corresponding user name and password are required). The Database Vault Owner user will be granted the `DV_OWNER` role and the Database Vault Account Manager user will be granted the `DV_ACCTMGR` role. Deselecting this check box means the Database Vault Owner user will be granted both roles because the separate Database Vault Account Manager user will not be created.

3.2.2.1 Database Vault Owner and Database Vault Account Manager Accounts

The Database Vault Owner, Database Vault Account Manager, Audit Vault Administrator, and Audit Vault Auditor account names must be different from each other (applicable when a separate Audit Vault Auditor or Database Vault Account Manager account is created). The 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 Table 3–3.

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

3.2.2.2 Database Vault Owner and Database Vault Account Manager Passwords

The Database Vault Owner or Database Vault Account Manager password must not be the name of the Audit Vault Administrator, Audit Vault Auditor, Database Vault Owner, or 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 following special characters shown in Table 3–4. All other characters are not allowed.

Each password must be identical to its corresponding password confirmation.

3.2.3 Advanced Server Installation: Node Selection Screen

The **Node Selection** screen will display when you install Audit Vault on an Oracle RAC environment. On this screen, users can select the nodes on which they want to install Audit Vault, or they can select a local installation to install Audit Vault single instance.

3.2.4 Advanced Server Installation: Specify Database Storage Options Screen

On the **Specify Database Storage Options** screen, you can select either **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 the *Oracle Database Installation Guide* for more information about certified NAS and NFS devices

Automatic Storage Management

Automatic Storage Management 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 Audit Vault installation, multiple Audit Vault installations, and in an Oracle Real Application Clusters (Oracle RAC) environment. Automatic Storage Management manages the storage of all 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.

3.2.5 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 the database files to an on-disk storage area called the flash recovery area. The first time 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 more information on 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 describes 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*.

3.2.6 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 **Use the same passwords for all accounts** option. Make your selection, then click **Next**.

3.2.7 Default Audit Policy and Initialization Parameters

Oracle Audit Vault installs a baseline database auditing policy. This policy covers the access control configuration information stored in Audit Vault database tables, information stored in Oracle Catalog (rollback segments, tablespaces, and so on), the use of system privileges, and Oracle Label Security configuration.

> **See Also:** *Oracle Audit Vault Administrator's Guide* for more information about the database audit policy

When you install Oracle Database Vault, the security-specific, database initialization parameters are initialized with default values. See "Initialization Parameters" appendix in Oracle Database Vault Installation Guide for Linux x86 for more information.

3.3 Basic Installation -- Performing the Single Instance Server Installation

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. You should run the installer as the software owner account that owns the current `ORACLE_HOME` environment. This is normally the `oracle` account.

   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
```

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 3.2 for more information about each of these topics.
   a. **Audit Vault Name** -- a unique name for the Audit Vault database. The 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 Audit Vault Home where you want to install Oracle Audit Vault.
   c. **Audit Vault Administrator** and **Audit Vault Auditor** -- the account name of the Audit Vault Administrator and a separate, optional Audit Vault Auditor, respectively. The Audit Vault Administrator and Audit Vault Auditor account names must not be the same. The Audit Vault Administrator account name is required. Accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Audit Vault Auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Audit Vault Auditor user name and password. The Audit Vault Administrator in this case will also be granted the role of Audit Vault Auditor.

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

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

      *AV_ADMIN*dva -- the Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts, where *AV_ADMIN* represents the Audit Vault Administrator user name.
   d. **Administrator Password** and **Auditor Password** -- the password for the Audit Vault Administrator account and the 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 following special characters shown in Table 3–4.

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

      The Audit Vault Administrator password will also be used for the Oracle Database Vault roles (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 Audit Vault Administrator account and the 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 the required fields. Validation of information is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

4. Review the installation prerequisite checks on the **Prerequisite Check** page. This is when all the installation prerequisite checks are performed and the results display. 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.

5. Review the installation summary information on the **Basic Installation Summary** page. After reviewing this installation information, click **Install** to begin the installation procedure.

6. Provide information or run scripts as root when prompted by OUI. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the OUI 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`

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

3.4 Advanced Installation -- Prerequisite Information for Installing in an Oracle Real Application Clusters Environment

This section assumes you performed phase one of the installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC) as 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 phase two of the installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC). This chapter also describes some of the Oracle Universal Installer (OUI) features. This section contains the following topics:

- Verifying System Readiness for Installing Oracle Audit Vault with CVU

3.4.1 Verifying System Readiness for Installing Oracle Audit Vault with CVU

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

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" section in Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux to assist you.

3.5 Advanced Installation -- Installing Single Instance and in an Oracle Real Application Clusters Environment

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

Perform the following procedures to install the Oracle Audit Vault.

1. Run Oracle Universal Installer (OUI) to install Oracle Audit Vault. You should run the installer as the software owner account that owns the current `ORACLE_HOME` environment. This is normally the `oracle` account.

   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
   ```

2. On the **Select Installation Type** page, select the **Advanced Installation** option, then click **Next**.

3. Enter the following information on the **Advanced Installation Details** page. See Section 3.2 for more information about each of these topics.

   a. **Audit Vault Name** -- a unique name for the Audit Vault database. The 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 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 Audit Vault home where you want to install Oracle Audit Vault.

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

   d. **Administrator Password** and **Auditor Password** -- the password for the Audit Vault Administrator account and the 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 following special characters shown in Table 3–4.

e. **Confirm Password** -- the confirming password for the Audit Vault Administrator account and the 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 the required fields. Validation of information is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

4. Enter the following information on the **Database Vault User Credentials** page. See Section 3.2.2 for more information about each of these topics.

   a. **Database Vault Owner** and **Database Vault Account Manager** -- the account name of the Database Vault Owner and a separate, optional Database Vault Account Manager, respectively. The Database Vault Owner, Database Vault Account Manager, Audit Vault Administrator, and Audit Vault Auditor account names must not be the same (applicable when a separate 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 Database Vault Owner account and the 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 following special characters shown in Table 3–4.

   c. **Confirm Password** -- the confirming password for the Database Vault Owner account and the 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 the required fields. Validation of information is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

5. If installing on a clustered system (Oracle Clusterware (CRS) is installed and the system is already part of a cluster), the **Node Selection** page appears from which to select the nodes on which Audit Vault needs to be installed. Local node will always be selected by default. If you are installing Audit Vault single instance on this local node only, select the **Local Only Installation** option, then click **Next**.

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

6. Review the installation prerequisite checks on the **Prerequisite Check** page. This is when all the installation prerequisite checks are performed and the results display. 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.

7. On the **Specify Database Storage Options** page, one of the following storage options can be selected: **File system**, **Automated Storage Management (ASM)**, or **Raw Devices**.

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

8. On the **Specify Backup and Recovery Options** page, 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** page displays (see Step 9). If the disk group selected does not have enough free space, the **Configure Automatic Storage Management** page displays.

   On the **Configure Automatic Storage Management** page, 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**.

9. On the **Specify Database Schema Passwords** page, you can choose to enter different passwords for each privileged database account or select **Use the same passwords for all accounts** option. If you choose to enter set of valid passwords for each privileged database account, enter these passwords. If you select **Use the same passwords for all accounts** option, then enter a single valid password. When finished, click **Next**.

10. Review the installation summary information on the **Advanced Installation Summary** page. After reviewing this installation information, click **Install** to begin the installation procedure.

11. Run scripts as root when prompted by Oracle Universal Installer. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the OUI 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`

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

    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 user has read/write permission. You can change the disk discovery string during the installation if the disks 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 email 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 OUI, and *Oracle Enterprise Manager Advanced Configuration Guide* for details about installing Database Control with DBCA and EMCA

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

After you have completed the second and final phase of the installation, proceed to Section 3.7 to perform the postinstallation tasks.

3.6 Performing a Silent Installation Using a Response File

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

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

1. Make sure all the pre-requisites are met for the installation of Audit Vault Server and Audit Vault Agent.
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 install. 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 1.4.2. 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*.

3.7 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 installs with all the components it requires already configured, so no additional components need to be configured using DBCA.
>
> Creation of additional databases in the Audit Vault home is not supported.

This section describes the following topics:

- Unlocking and Resetting User Passwords
- Enabling or Disabling Connections with the SYSDBA Privilege
- Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC only)
- Logging in to Audit Vault Console

3.7.1 Unlocking and Resetting User Passwords

The password entered for the Audit Vault Administrator is used as the password for core database accounts such as SYS, SYSTEM, SYSMAN, and DBSNMP in the case of 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, the same Audit Vault Administrator password is also used for the `<AV_ADMIN>dvo` account, the Database Vault Owner (granted `DV_OWNER` role), to manage Database Vault roles and configuration and the `<AV_ADMIN>dva` account, and the 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, the Database Vault Owner user password and the separate, optional Database Vault Account Manager user password are entered for these users. You must change these passwords according to your company policies.

3.7.1.1 Using SQL*Plus to Unlock Accounts and Reset Passwords

To unlock and 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 `account` is the user account that you want to unlock and `password` is the new password:

   ```
   SQL> ALTER USER account [ IDENTIFIED BY password ] ACCOUNT UNLOCK;
   ```

   In this example:

   - The ACCOUNT UNLOCK clause unlocks the account.
   - The IDENTIFED BY password clause resets the password.

   Note: If you unlock an account but do not reset the password, then the password remains expired. The first time someone connects as that user, they must change the password.

   To permit unauthenticated access to your data through HTTP, unlock the ANONYMOUS user account.

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

   - Unlocking and changing passwords after installation
   - Oracle security procedures
   - Best security practices

3.7.2 Enabling or Disabling Connections with the SYSDBA Privilege

In a default Audit Vault installation, the operating system authentication to the database is disabled. In addition, connections to the database using the `SYSDBA` privilege (that is, those that use the `AS SYSDBA` clause) are disabled. This is a security feature and is implemented to prevent misuse of the `SYSDBA` privilege.

If a password file was created using the `orapwd` utility with the `nosysdba` flag set to `y` (Yes), which is the default action of a Database Vault installation, users will not be able to log in to an Oracle Database Vault instance using the `SYS` account or any account with `SYSDBA` privilege using the `AS SYSDBA` clause. You can re-enable the ability to connect with the `SYSDBA` privilege by re-creating the password file with the `nosysdba` flag set to n (No). You might need to re-enable the ability to connect with `SYSDBA` privileges, if certain products or utilities require its use.

When you re-create the password file, any accounts other than `SYS` that were granted the `SYSDBA` or `SYSOPER` privileges will have those privileges removed. You will need to grant again the privileges for these accounts after you have re-created the password file.

Use the following syntax to run the `orapwd` utility:

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

Where:

- `file`: Name of password file (mandatory).
- `password`: Password for `SYS` (mandatory). Enter at least six alphanumeric characters.
- `entries`: Maximum number of distinct DBA users.
- `force`: Whether to overwrite the existing file (optional). Enter `y` (for yes) or `n` (for no).
- `nosysdba`: 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=5hjk99 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

Enabling or Disabling 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 you issue affects all nodes.

Enabling or Disabling Connecting with SYSDBA on Automatic Storage Management Systems

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

3.7.3 Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC only)

After installing Audit Vault for a Oracle Real Application Clusters (Oracle RAC) instance, you need to 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 need to run this command on all Oracle RAC nodes other than the node on which the 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]
```

Where:

- `action`: 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`: 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`: The Oracle home for the Oracle RAC instance.
- `jdbc_str`: The JDBC connection string used to connect to the database. For example, `"jdbc:oracle:oci:@orcl1"`.
- `sys_password`: The password for the `SYS` user.
- `logfile`: Optionally, 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`: Required if you are not running DVCA in an Xterm window.
- `nodecrypt`: Reads plain text passwords as passed on the command line.
- `lockout`: Used to disable `SYSDBA` operating system authentication.

> **Note:** You can re-enable 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 the cluster nodes. This step is also applicable to the node on which Audit Vault was installed. Use the following commands:

```
srvctl stop instance -d sid -i instance_name -c "SYS/password AS SYSDBA"
srvctl stop nodeapps -n node_name
srvctl start nodeapps -n node_name
srvctl start instance -d sid -i instance_name -c "SYS/password AS SYSDBA"
```

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

3.7.4 Logging in to Audit Vault Console

To use Audit Vault Console, you must access it on the node where you installed the Audit Vault database. If you want to log in to Audit Vault Console from another cluster node, then you need to reconfigure Enterprise Manager to start the Audit Vault Console interface on that other node.

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

1. On the node from which you installed the database, open a Web browser to access the 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 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 the "Configuring Audit Vault" chapter in *Oracle Audit Vault Administrator's Guide* for more information.

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

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

2. Log in to the Audit Vault Console using the user name <AV_ADMIN> and the <AV_ADMIN> password you created during the installation.

4

Removing Audit Vault Server Software

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

4.1 Removing Audit Vault Server Software

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

Then, use the following procedure to uninstall the server.

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

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

   ```
   $ avctl stop_av
   ```

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

2. Log into Audit Vault database and shut it down, as follows:

   ```
   sqlplus / as sysoper
   SQL> shutdown immediate;
   SQL> exit
   ```

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

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

3. 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 command on all nodes where Audit Vault is installed if you are removing Audit Vault server from all nodes.

4. 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 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.

5. Click **Deinstall Products** to bring up the Oracle Inventory.

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

6. Clean up the old Oracle directories.

   On systems where Oracle Audit Vault is the only Oracle software installed, navigate 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 Audit Vault is installed if you are removing Audit Vault server from all nodes.

Index

A

aliases, multiple on computers, 2-6
architecture
  checking system architecture, 2-3

B

base directory
  See Oracle base directory

C

certification, hardware and software, 1-7
checking
  operating system distribution and version, 2-4
chmod command, 2-16
chown command, 2-16
Cluster Verification Utility
  verifying readiness for database installation, 3-10
computers with multiple aliases, 2-6

D

data files
  recommendations for file system, 2-16
dba group
  and SYSDBA privilege, 2-6
  creating, 2-8
  description, 2-6
DHCP computers, installing on, 2-5
directory
  database file directory, 2-16
  Oracle base directory, 2-13
  Oracle home directory, 2-14
  Oracle Inventory directory, 2-14
  oraInventory, 2-14
disk space
  checking, 2-3
Dynamic Host Configuration Protocol. *See* DHCP

E

environment variables
  ORACLE_BASE, 2-14, 2-16
  ORACLE_HOSTNAME, 2-6
  TEMP and TMPDIR, 2-2
errata
  Linux kernel, 2-4
examples
  Oracle base directories, 2-14
external jobs
  operating system user required for, 2-7
extjob executable file
  operating system user required for, 2-7

F

file system
  appropriate for Oracle base directory, 2-16
  using for data files, 2-16
file-max parameter file, 2-11
files
  /etc/pam.d/login, 2-13
  /etc/profile.local, 2-13
  /etc/security/limits.so, 2-12
  /etc/sysctl.conf, 2-12
  limits.conf, 2-12
  oraInst.loc, 2-8, 2-15
  oratab, 2-15
  /proc/sys/fs/file-max, 2-11
  /proc/sys/kernel/sem, 2-11
  /proc/sys/kernel/shmall, 2-11
  /proc/sys/kernel/shmmax
    shmmax file, 2-11
  /proc/sys/kernel/shmmni, 2-11
  /proc/sys/net/core/rmem_default, 2-11
  /proc/sys/net/core/rmem_max, 2-11
  /proc/sys/net/core/wmem_default, 2-11
  /proc/sys/net/core/wmem_max, 2-11
  /proc/sys/net/ipv4/ip_local_port_range, 2-11
  profile.local, 2-13
free
  Linux command, 2-2

G

groupadd command, 2-8, 2-9
groups
  creating the dba group, 2-8
  creating the oinstall group, 2-8
  creating the oper group, 2-9

H

hardware and software certifications, 1-7
hardware certification, 1-7
home directory
  See Oracle home directory
host name, setting before installation, 2-6

I

id command, 2-10
installation
  computer aliases, multiple, 2-6
  non-interactive, 3-14
IP addresses, multiple, 2-6
ip_local_port_range file, 2-11

K

kernel
  Linux errata, 2-4
kernel parameters
  changing, 2-12

L

limit command, 2-13
limits.conf file, 2-12
limits.so file, 2-12
Linux
  kernel errata, 2-4
Linux commands
  chmod, 2-16
  chown, 2-16
  free, 2-2
  groupadd, 2-8, 2-9
  id, 2-10
  limit, 2-13
  mkdir, 2-16
  passwd, 2-10
  rpm, 2-4
  sysctl, 2-11
  ulimit, 2-13
  useradd, 2-10
  xhost, 2-1
Linux workstation
  installing from, 2-1
login file, 2-13

M

mkdir command, 2-16
mount point
  for Oracle base directory, 2-13
multihomed computers, installing on, 2-6
multiple aliases, computers with, 2-6
multiple Oracle homes, 1-8

N

network adapters
  See also loopback adapters, primary network adapters
network cards, multiple, 2-6
network setup
  about, 2-4
  computers with multiple aliases, 2-6
network topics
  DHCP computers, 2-5
  multiple network cards, 2-6
nobody user
  checking existence of, 2-10
  description, 2-7

O

oinstall group
  creating, 2-8
  description, 2-7
oper group
  and SYSOPER privilege, 2-7
  creating, 2-9
  description, 2-7
operating system groups
  creating the dba group, 2-8
  creating the oinstall group, 2-8
  creating the oper group, 2-9
  oinstall, 2-7
  OSDBA, 2-6
  OSOPER, 2-7
  osoper, 2-7
  requirements, 2-6
operating system users
  checking existence of the nobody user, 2-10
  creating the oracle user, 2-9
  nobody, 2-7
  oracle, 2-7
  requirements, 2-6
  unprivileged user, 2-7
Optimal Flexible Architecture
  recommendations for Oracle base directory, 2-13
  recommended path for Oracle base directory, 2-13
  recommended path for Oracle home directory, 2-14
  recommended path for Oracle Inventory directory, 2-14
Oracle base directory
  and ORACLE_BASE environment variable, 2-14
  creating, 2-16
  creating new, 2-16
  description, 2-13
  determining disk space on, 2-16
  examples, 2-14
  identifying appropriate file system, 2-16
  identifying existing, 2-15
  mount point for, 2-13
  recommended path, 2-13
  relationship with Oracle software owner user, 2-13
Oracle home directory

description, 2-14
multiple homes, network considerations, 2-6
recommended path, 2-14
requirements, 2-14
using to identify Oracle base directory, 2-15
Oracle home name, 2-14
Oracle homes, multiple, 1-8
Oracle host name, setting before installation, 2-6
Oracle Inventory
description, 2-14
pointer file, 2-8
Oracle Inventory directory
description, 2-14
recommended path, 2-14
Oracle Inventory group
creating, 2-8
description, 2-7
Oracle software owner user
creating, 2-9
description, 2-7
relationship with Oracle base directory, 2-13
setting shell limits for, 2-12
oracle user
creating, 2-9
description, 2-7
relationship with Oracle base directory, 2-13
setting shell limits for, 2-12
ORACLE_BASE environment variable, 2-14, 2-16
ORACLE_HOSTNAME environment variable
about, 2-6
computers multiple homes, 2-6
computers with multiple aliases, 2-6
setting before installation, 2-6
oraInst.loc file, 2-8, 2-15
location, 2-8
oraInventory directory
See Oracle Inventory directory
oratab file, 2-15
formats, 2-15
location of, 2-15
OSDBA group
and SYSDBA privilege, 2-6
creating, 2-8
description, 2-6
OSOPER group
and SYSOPER privilege, 2-7
creating, 2-9
description, 2-7

P

packages, checking, 2-4
passwd command, 2-10
permissions
for Oracle base directory, 2-16
processor
checking system architecture, 2-3
profile.local file, 2-13

R

RAID
using for Oracle data files, 2-16
Red Hat
operating system requirements, 2-3
Red Hat Package Manager
See RPM
redundant array of independent disks
See RAID
removing, Oracle Software, 4-1
rmem_default file, 2-11
rmem_max file, 2-11
root user
logging in as, 2-1
RPM
checking, 2-4
rpm command, 2-4

S

sem file, 2-11
shell limits
setting, 2-12
shmall file, 2-11
shmmni file, 2-11
software and hardware certifications, 1-7
software certification, 1-7
SUSE
operating system requirements, 2-3
swap space
checking, 2-2
sysctl command, 2-11
sysctl.conf file, 2-12
SYSDBA privilege
associated operating system group, 2-6
SYSOPER privilege
associated operating system group, 2-7
system architecture
checking, 2-3

T

TEMP environment variable, 2-2
TMPDIR environment variable, 2-2

U

ulimit command, 2-13
unprivileged user
checking existence of, 2-10
useradd command, 2-10
users
checking existence of the nobody user, 2-10
creating the oracle user, 2-9
operating system nobody user, 2-7
Oracle software owner user, 2-7

W

wmem_default file, 2-11

wmem_max file, 2-11

X

X Window system
  enabling remote hosts, 2-1
xhost command, 2-1