Oracle® Audit Vault

Server Installation Guide

10*g* Release 2 (10.2.2) for AIX 5L Based Systems (64-Bit)

E10120-02

August 2007

ORACLE®

Oracle Audit Vault Server Installation Guide, 10*g* Release 2 (10.2.2) for AIX 5L Based Systems (64-Bit)

E10120-02

Primary Author: Rod Ward and Prakash Jashnani

Contributing Author: Sumit Jeloka, Nilima Kapoor, Robert Chang, K Karun, Deborah Owens, Janet Blowney

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

Contents

List of Tables

Preface

Oracle Audit Vault Server Installation Guide for AIX 5L Based Systems (64-Bit) explains how to prepare for, install, and configure Oracle Audit Vault Server. It provides specific instructions for the operating system and Oracle software technology components that the Audit Vault Server requires.

Audience

This document is intended for Oracle database administrator's (DBAs) and system administrators 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. Outside the United States, call +1.407.458.2479.

Related Documents

For more information, see 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 Oracle Clusterware and Oracle Real Application Clusters Installation Guide for AIX Based Systems*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Database Vault Installation Guide for AIX 5L Based Systems (64-Bit)*
- *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.

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

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

1.2 Audit Vault Installation Methods

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

1.2.1 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.

1.2.2 Automated Installation Methods Using Response Files

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

```
./runInstaller -silent -responseFile Path of response file
```

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

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

See Section 3.6 for information about performing an Audit Vault Server silent installation:

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

1.3 Audit Vault Server Installation

The Audit Vault 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 Oracle Wallet Manager. 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 Oracle Audit Vault. The Audit Vault Console provides the

management service that initiates the communication with agents using HTTP. The 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 the Audit Vault Server and the 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 you check the requirements described in Section 1.4, 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.

1.4 Installation Considerations

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

- Hardware and Software Considerations
- Multiple Oracle Homes

1.4.1 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

`https://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`

1.4.2 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. See Section 2.5.3 for more information.

2

Oracle Audit Vault Server Preinstallation Requirements

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

2.1 Becoming Familiar with the Features of Oracle Audit Vault

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

2.2 Logging In to the System as the root User

Before you install the Oracle software, you must complete several tasks (described in the sections that follow) as the `root` user. Log in to your system as the `root` user.

2.3 Checking the Hardware Requirements

The system must meet the following minimum hardware requirements:

- At least 1024 MB of physical RAM.
- The following table describes the relationship between installed RAM and the configured swap space requirement.

RAM	Swap Space
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

- 400 MB of disk space in the `/tmp` directory.
- 5.3 GB of disk space for the Oracle Audit Vault Server software.
- 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:

   ```
   # /usr/sbin/lsattr -E -l sys0 -a realmem
   ```

   If the size of the physical RAM 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:

   ```
   # /usr/sbin/lsps -a
   ```

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

3. 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 free 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 `TMP` and `TMPDIR` environment variables when setting the `oracle` user's environment.
   - Extend the file system that contains the `/tmp` directory. If necessary, contact your system administrator for information about extending file systems.

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

   ```
   # df -k
   ```

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

   ```
   # /usr/bin/getconf HARDWARE_BITMODE
   64
   ```

Note: The expected output of this command is 64. 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 the table 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.

Item	Requirement
Operating system	The following operating system versions and maintenance level are required: AIX 5L version 5.2, Maintenance Level 04 or later AIX 5L version 5.3, Maintenance Level 02 or later

Operating system filesets:	The following operating system filesets are required:
	`bos.adt.base`
	`bos.adt.lib`
	`bos.adt.libm`
	`bos.perf.libperfstat`
	`bos.perf.perfstat`
	`bos.perf.proctools`
	`xlC.aix50.rte:7.0.0.4 or later`
	`xlC.rte:7.0.0.1 or later`

PL/SQL native compilation	One of the following: ■ IBM XL C/C++ Enterprise Edition V7.0 for AIX PTF (7.0.0.2) ■ gcc 3.3.2 **Note:** If you do not install install the IBM XL C/C++ Enterprise Edition V7.0 compiler, you need to install the IBM XL C/C++ Enterprise Edition V7.0 for AIX Runtime Environment Component. The runtime environment file sets can be downloaded with no license requirements from the following link: `http://www-1.ibm.com/support/docview.wss?uid=swg24009788`

Item	Requirement
Pro*C/C++, Oracle Call Interface, Oracle C++ Call Interface, Oracle XML Developer's Kit (XDK)	■ May 2005 XL C/C++ Enterprise Edition V7.0 for AIX PTF (7.0.0.2) You can download this software from the following link: http://www-1.ibm.com/support/docview.wss?uid=swg24009787 **Note:** If you do not install install the IBM XL C/C++ Enterprise Edition V7.0 compiler, you need to install the IBM XL C/C++ Enterprise Edition V7.0 for AIX Runtime Environment Component. The runtime environment file sets can be downloaded with no license requirements from the following link: http://www-1.ibm.com/support/docview.wss?uid=swg24009788
Oracle JDBC/OCI Drivers	You can use the following optional IBM JDK versions with the Oracle JDBC/OCI drivers, however they are not required for the installation: ■ JDK 1.4.2 (64-bit) ■ JDK 1.3.1.11 (32-bit) ■ JDK 1.2.2.18 **Note:** IBM JDK 1.4.2 (32-bit) is installed with this release.

Oracle Messaging Gateway	IBM WebSphere MQ V5.3, client and server:
	`mqm.Client.Bnd`
	`mqm.Server.Bnd`

To ensure that the system meets these requirements:

1. To determine the version of AIX installed, enter the following command:

   ```
   # oslevel -r
   ```

   If the operating system version is lower than AIX 5.2.0.0 Maintenance Level 1 (5200-01), then upgrade your operating system to this level. AIX 5L version 5.2 maintenance packages are available from the following Web site:

   http://www-912.ibm.com/eserver/support/fixes/

2. To determine whether the required filesets are installed and committed, enter a command similar to the following:

   ```
   # lslpp -l bos.adt.base bos.adt.lib bos.adt.libm bos.perf.perfstat \
    bos.perf.libperfstat bos.perf.proctools
   ```

   If a fileset is not installed and committed, then install it. Refer to your operating system or software documentation for information about installing filesets.

In addition, you need to verify that the following patches are installed on the system. The procedure following the table describes how to check these requirements.

Note: There may be more recent versions of the patches listed installed on the system. If a listed patch is not installed, then determine whether a more recent version is installed before installing the version listed.

Installation Type or Product	Requirement
All installations	Authorized Problem Analysis Reports (APARs) for AIX 5L v5.2 ML 04: ■ IY63133: large percentage of CPU time spent in ldata_balance routine ■ IY64978: deadlock with concurrent renaming and unlinking under JFS ■ IY63366: dlsym returns null even for valid symbol in AIX520 ML-4 ■ IY64691: chvg -b can cause corruption and crash ■ IY64737: AIO can hang in knotunlock ■ IY65001: mklvcopy on a striped lv is failing to update lvcb
All installations	Authorized Problem Analysis Reports (APARs) for AIX 5L v5.3 ML 02: ■ IY58143: REQUIRED UPDATE FOR AIX 5.3 ■ IY59386: libdepend.mk files are all empty ■ IY60930: Unable to delete network routes ■ IY66513: LDR_CNTRL turns on undesirable option when initialized with incorrect value ■ IY70159: krtl relocation problem ■ IY68989: eFix for write to mmapped space hangs
PL/SQL native compilation, Pro*C/C++, Oracle Call Interface, Oracle C++ Call Interface, Oracle XML Developer's Kit (XDK)	May 2005 XL C/C++ Enterprise Edition V7.0 for AIX PTF (7.0.0.2): ■ IY64361: Exception in putdiag_no_handler() when -O is specified ■ IY65361: May 2005 XL C Enterprise Edition V7.0 for AIX PTF ■ IY65362: MAY 2005 XL C/C++ Enterprise Edition V7 for AIX
Oracle JDBC/OCI Drivers	**Note:** These APARs are required only if you are using the associated JDK version. APAR required for JDK 1.4.2 (64-bit): ■ IY63533: DK 1.4.2 64-bit SR1 caix64142-20040917 APARs required for JDK 1.3.1.11 (32-bit): ■ IY58350: SDK 1.3.1 32-BIT SR7P : CA131IFX-20040721A ■ IY65305: JAVA142 32-BIT PTF : CA142IFX-20041203 APAR required for JDK 1.2.2.18: ■ IY40034: SDK 1.2.2 PTF: CA122-20030115
Oracle Messaging Gateway	Corrective service diskettes (CSDs) for WebSphere MQ: CSD03 or later for WebSphere MQ V5.3 FP 9

To ensure that the system meets these requirements:

1. To determine whether an APAR is installed, enter a command similar to the following:

```
# /usr/sbin/instfix -i -k "IY63133 IY64978 IY63366 IY64691 IY65001 IY64737 \
  IY64361 IY65305 IY58350 IY63533"
```

   If an APAR is not installed, then download it from the following Web site and install it:

http://www-912.ibm.com/eserver/support/fixes/

2. If you require a CSD for WebSphere MQ, then refer to the following Web site for download and installation information:

   http://www.ibm.com/software/integration/wmq/support/

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 might 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 `netsvc.conf` file as follows:

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

   Ensure that the hosts keyword is configured properly for hostname resolution in the environment.

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

Setting the ORACLE_HOSTNAME Environment Variable

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

For example, if the fully qualified host name is `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 the 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 topics describe how to identify an existing Oracle Inventory group.

- The Oracle software owner user (typically, oracle)

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

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

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 Database Administrator's Guide* for more information about the OSDBA group and the `SYSDBA` and `SYSOPER` privileges

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

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

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

2.6.1 Creating the Oracle Inventory Group

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

Determining Whether the Oracle Inventory Group Exists

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

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

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

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

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

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

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

Creating the Oracle Inventory Group

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

1. Enter the following command:

   ```
   # smit security
   ```

2. Choose the appropriate menu items to create the `oinstall` group.
3. Press **F10** to exit.

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 procedure, use the group name `dba` unless a group with that name already exists.

1. Enter the following command:

   ```
   # smit security
   ```

2. Choose the appropriate menu items to create the `dba` group.
3. Press **F10** to exit.

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 procedure, use the group name `oper` unless a group with that name already exists.

1. Enter the following command:

   ```
   # smit security
   ```

2. Choose the appropriate menu items to create the `oper` group.
3. Press **F10** to exit.

2.6.4 Creating the Oracle Software Owner User

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

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

2.6.4.1 Determining Whether an Oracle Software Owner User Exists

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

```
# id oracle
```

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

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

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

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

See one of the following sections for more information:

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

2.6.4.2 Creating an Oracle Software Owner User

If the Oracle software owner user does not exist or if you require 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. Enter the following command:

   ```
   # smit security
   ```

2. Choose the appropriate menu items to create the `oracle` user, specifying the following information:
   - In the **Primary GROUP** field, specify the Oracle Inventory group, for example `oinstall`.
   - In the **Group SET** field, specify the OSDBA group and if required, the OSOPER group. For example, `dba` or `dba,oper`.

   > **Note:** The UID for the `oracle` user must be less than 65536.

3. Press **F10** to exit.

4. 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 you can modify it as follows:

1. Enter the following command:

```
# smit security
```

2. Choose the appropriate menu items to modify the `oracle` user.
3. In the **Primary GROUP** field, specify the Oracle Inventory group, for example `oinstall`.
4. In the **Group SET** field, specify the required secondary groups, for example `dba` and `oper`.
5. Press **F10** to exit.

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:

```
# smit security
```

   Specify the appropriate options to create an unprivileged `nobody` user, then press **F10** to exit.

2.7 Configure Shell Limits and System Configuration Parameters

> **Note:** The parameter and shell limit values shown in this 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.

Oracle recommends that you set shell limits and system configuration parameters as described in the following sections:

- Configure Shell Limits
- Configure System Configuration Parameters

2.7.1 Configure Shell Limits

Verify that the shell limits shown in the following table are set to the values shown. The procedure following the table describes how to verify and set the values.

Shell Limit (As Shown in smit)	Recommended Value
Soft FILE size	-1 (Unlimited)
Soft CPU time	-1 (Unlimited) **Note:** This is the default value.
Soft DATA segment	-1 (Unlimited)
Soft STACK size	-1 (Unlimited)

To view the current value specified for these shell limits, and to change them if necessary:

1. Enter the following command:

   ```
   # smit chuser
   ```

2. In the **User NAME** field, enter the user name of the Oracle software owner, for example `oracle`.
3. Scroll down the list and verify that the value shown for the soft limits listed in the previous table is -1.

   If necessary, edit the existing value.
4. When you have finished making changes, press F10 to exit.

2.7.2 Configure System Configuration Parameters

Verify that the maximum number of processes allowed for each user is set to 2048 or greater:

> **Note:** For production systems, this value should be at least 128 plus the sum of the `PROCESSES` and `PARALLEL_MAX_SERVERS` initialization parameters for each database running on the system.

1. Enter the following command:

   ```
   # smit chgsys
   ```

2. Verify that the value shown for **Maximum number of PROCESSES allowed for each user** is greater than or equal to 2048.

   If necessary, edit the existing value.
3. When you have finished making changes, press **F10** to exit.

2.8 Identifying the Required Software Directories

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

- Oracle Base Directory
- Oracle Inventory Directory

- Oracle Home Directory

2.8.1 Oracle Base Directory

The Oracle base directory is a top-level directory for Oracle software installations. On AIX 5L Based Systems (64-Bit) systems, the Optimal Flexible Architecture (OFA) guidelines recommend that you use a path similar to the following for the Oracle base directory:

/mount_point/app/*oracle_sw_owner*

In this example:

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

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

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

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

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

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

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

2.8.2 Oracle Inventory Directory

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

oracle_base/oraInventory

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

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

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

2.8.3 Oracle Home Directory

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

```
oracle_base/product/10.2.2/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 the following topics:

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

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

2.9.1 Identifying an Existing Oracle Base Directory

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

- To identify an existing Oracle Inventory directory

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

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

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

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

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

- To identify existing Oracle home directories

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

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

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

  ```
  *:/u03/app/oracle/product/1.0.0/db_1:N
  ```

```
*:/opt/orauser/infra_904:N
*:/oracle/9.2.0:N
```

The directory paths 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 the table in Section 2.3.

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

  ```
  # df -k oracle_base_path
  ```

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

2.9.2 Creating an Oracle Base Directory

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

To identify an appropriate file system:

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

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

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

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

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

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

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

2.10 Creating Directories for Oracle Audit Vault Database Files

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

- The default path suggested by Oracle Universal Installer for the database file directory is a subdirectory of the Oracle base directory.
- You can choose either a single file system or more than one file system to store the database files:
  - If you want to use a single file system, then choose a file system on a physical device that is dedicated to the database.

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

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

2.11 Setting the DISPLAY Environment Variable

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

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

This chapter includes the following sections:

3.1 Accessing the Server Installation Software

The Oracle Audit Vault Server software is available on digital video disk (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
!	Exclamation point
@	At sign
%	Percent sign
^	Circumflex
&	Ampersand
*	Asterisk
(	Left parenthesis
)	Right parenthesis
-	Minus sign
+	Plus sign
=	Equal sign
"	Double quotation mark
|	Vertical bar
`	grave
~	tilde
[	Left bracket
{	Left brace
]	Right bracket
}	Right brace
;	Semicolon
:	Colon
'	Single quotation mark
<	Less than sign
>	Greater than sign
/	Slash
\	Backslash
?	Question mark
,	Comma
.	Period
#	Number sign
_	Underscore

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

Symbol	Character Name
$	Dollar sign
	Space character

3.2.1.2 Audit Vault Home

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

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

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

Symbol	Character Name
\	Backslash
/	Slash
-	hyphen
_	Underscore
.	Period
:	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 must supply a user name and password for the Audit Vault administrator user and optionally for the Audit Vault auditor user 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 that 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 service 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 user names that are 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 following reserved names.

Names	Names	Names	Names	Names
ACCESS	ADD	ALL	ALTER	AND
ANONYMOUS	ANY	AQ_ADMINISTRATOR_ ROLE	AQ_USER_ROLE	ARRAYLEN
AS	ASC	AUDIT	AUTHENTICATEDUSER	AV_ADMIN
AV_AGENT	AV_ARCHIVER	AV_AUDITOR	AV_SOURCE	AVSYS
BETWEEN	BY	CHAR	CHECK	CLUSTER
COLUMN	COMMENT	COMPRESS	CONNECT	CREATE
CTXAPP	CTXSYS	CURRENT	DATE	DBA
DBSNMP	DECIMAL	DEFAULT	DELETE	DELETE_CATALOG_ROLE
DESC	DIP	DISTINCT	DM_CATALOG_ROLE	DMSYS
DMUSER_ROLE	DROP	DV_ACCTMGR	DV_ADMIN	DVF
DV_OWNER	DV_PUBLIC	DV_REALM_OWNER	DV_REALM_RESOURCE	DV_SECANALYST
DVSYS	EJBCLIENT	ELSE	EXCLUSIVE	EXECUTE_CATALOG_ ROLE
EXFSYS	EXISTS	EXP_FULL_DATABASE	FILE	FLOAT
FOR	FROM	GATHER_SYSTEM_ STATISTICS	GLOBAL_AQ_USER_ ROLE	GRANT
GROUP	HAVING	HS_ADMIN_ROLE	IDENTIFIED	IMMEDIATE
IMP_FULL_ DATABASE	IN	INCREMENT	INDEX	INITIAL
INSERT	INTEGER	INTERSECT	INTO	IS
JAVA_ADMIN	JAVADEBUGPRIV	JAVA_DEPLOY	JAVAIDPRIV	JAVASYSPRIV
JAVAUSERPRIV	LBAC_DBA	LBACSYS	LEVEL	LIKE

Names	Names	Names	Names	Names
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 special characters shown in Table 3–3.

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

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

Each password must be identical to its corresponding password confirmation.

3.2.2 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 must supply an account name and password for the Database Vault Owner account, and optionally for the Database Vault Account Manager account during installation.

The **Create a Separate Database Vault Account Manager** check box is selected by default, which means that a separate 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 that 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 the table in Section 3.2.1.3.

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 special characters shown in Table 3–3. 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 appear when you install Oracle Audit Vault in an Oracle RAC environment. On this screen, users can select the nodes on which they want to install Oracle Audit Vault, or they can select a local installation to install Oracle Audit Vault single instance.

3.2.4 Advanced Server Installation: Specify Database Storage Options Screen

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

File System

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

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

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

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

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

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

  You can store database files on NAS devices provided that the NAS device is certified by Oracle.

  > **See Also:** "Using Network Attached Storage or NFS File Systems" section in the *Oracle Database Installation Guide for AIX 5L Based Systems (64-Bit)* for more information about certified NAS and NFS devices.

Automatic Storage Management

Automatic Storage Management (ASM) is a high-performance storage management solution for Oracle Audit Vault database files. It simplifies the management of a

dynamic database environment, such as creating and laying out databases and managing disk space.

> **Note:** An existing ASM instance must be installed in order 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 Also:** *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 of the database files to an on-disk storage area called the flash recovery area. The first time that the backup job runs, it creates a full backup of the database. Subsequent backup jobs perform incremental backups, which enable you to recover the database to its state at any point during the preceding 24 hours.

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

- The location of the flash recovery area

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

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

  Oracle Enterprise Manager uses the operating system credentials that you specify when running the backup job. The user name that you specify must belong to the AIX 5L Based Systems (64-Bit) group that identifies database administrators (the OSDBA group, typically dba). The Oracle software owner user name (typically oracle) that you use to install the software is a suitable choice for this user.

Section 2.6 describes the requirements for the OSDBA group and Oracle software owner user and explains how to create them.

Backup Job Default Settings

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

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

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

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

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

3.2.6 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 the **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 Auditor'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 AIX 5L Based Systems (64-Bit)* 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 special characters shown in Table 3–3.

      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 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 installation prerequisite checks are performed and the results are displayed. Verify that all prerequisite checks succeed, then click **Next**.

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

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

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 the `root` user when prompted by Oracle Universal Installer. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file is located in the `cfgtoollogs/oui` directory, in the following location:

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

7. After the installation completes, take note of the Oracle Enterprise Manager Database Control URL and the Audit Vault Console URL. 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 AIX Based Systems*. These tasks include preinstallation tasks, configuring Oracle Clusterware and Oracle Database storage, and installing Oracle Clusterware. You are now ready to install Oracle Audit Vault in an Oracle RAC environment.

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

Verifying System Readiness for Installing Oracle Audit Vault with CVU

To help to verify that your system is prepared to install Oracle Audit Vault with Oracle RAC successfully, use 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 AIX Based Systems*.

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" section in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for AIX Based Systems* to assist you.

3.5 Advanced Installation – Installing Single Instance and Installing 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 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** screen, select the **Advanced Installation** option, then click **Next**.

3. Enter the following information on the **Advanced Installation Details** screen. 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 an Oracle RAC installation, the name will be used to derive the Oracle RAC database SID of each Oracle RAC node, and will be the first portion (`db_name`) of the database service name.

   b. **Audit Vault Home** – Specify or browse to find the path to the 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 special characters shown in Table 3–3.

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 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** screen. 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 special characters shown in Table 3–3.

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

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

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

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

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

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

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

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

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

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

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

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

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

   On AIX 5L Based Systems (64-Bit) 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** screen, you can choose to enter different passwords for each privileged database account or select the **Use the same passwords for all accounts** option. If you choose to enter a set of valid passwords for each privileged database account, enter these passwords. If you select the **Use the same passwords for all accounts** option, then enter a single valid password. When you are finished, click **Next**.

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

11. Run scripts as the `root` user when prompted by Oracle Universal Installer. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file is located in the `cfgtoollogs/oui` directory in the following location:

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

    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. 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 software owner user has read/write permission. You can change the disk discovery string during the installation if the disks that you want to use for ASM are located elsewhere.
    - On the Select Database Management Option page, if you have already completed the Grid Control Management Agent installation, then you can select either Grid or Local Database control. Otherwise, only Local Database control for database management is supported for Oracle RAC. When you use the local Database Control, you can choose the e-mail option and enter the outgoing SMTP server name and e-mail address.

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

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

After you have completed the part 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 installation using a response file:

1. Make sure all prerequisites 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 installation. See Section 2.11 for more information.
4. Invoke Oracle Universal Installer using the following options:

   ```
   ./runInstaller -silent -responseFile Path of response file
   ```

For more information about these options, see Section 1.4.2. 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 AIX Based Systems*.

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 of the components that 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 includes the following topics:

- Unlocking and Resetting User Passwords
- Enabling or Disabling Connections with the SYSDBA Privilege
- Running 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 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_ADMINdvo* account, the Database Vault Owner (granted DV_OWNER role), to manage Database Vault roles and configuration and the *AV_ADMINdva* 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_ADMINdva* 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 IDENTIFIED 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 an Oracle 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 reenable the ability to connect with the SYSDBA privilege by recreating the password file with the nosysdba flag set to n (No). You might need to reenable 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
```

In this example:

- `file` is the name of password file (mandatory).
- `password` is the password for `SYS` (mandatory). Enter at least six alphanumeric characters.
- `entries` is the maximum number of distinct DBA users.
- `force` indicates whether or not to overwrite the existing file (optional). Enter `y` (for yes) or `n` (for no).
- `nosysdba` indicates whether or not 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 that you issue affects all nodes.

Enabling or Disabling Connecting with SYSDBA on Automatic Storage Management Systems

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

3.7.3 Running 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 must run Database Vault Configuration Assistant (DVCA) with the `-action optionrac` switch on all other Oracle RAC nodes. This sets instance parameters and disables `SYSDBA` operating system authentication.

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

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

Use the following syntax to run DVCA:

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

In this example:

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

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

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

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

3.7.4 Logging In to Audit Vault Console

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

Use the following instructions to log in to the 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 will display 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 that you created during the installation.

4

Removing the Oracle Audit Vault Server Software

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

4.1 Removing the Audit Vault Server Software

To remove Audit Vault Server software, all Audit Vault Agents must be stopped if the 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 Audit Vault server software.

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

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

   ```
   $ avctl stop_av
   ```

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

2. Log in to the 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 -q
   Connect String: sys as sysdba
   Enter password: <sysdbapassword>
   ```

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

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

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

6. Clean up the old Oracle directories.

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

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

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

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

Index

P

R

S

T

U

W

X