Oracle® Audit Vault

Server Installation Guide

Release 10.3 for Linux x86-64

E23565-07

January 2012

ORACLE®

Oracle Audit Vault Server Installation Guide, Release 10.3 for Linux x86-64

E23565-07

Primary Authors: Rod Ward, Tanaya Bhattacharjee

Contributing Authors: Tammy Bednar, Namrata Bhakthavatsalam, Janet Blowney, Pat Huey, Prakash Jashnani, K Karun, Reema Khosla, Deborah Owens, Mohammed Yunus Qureshi, Trivikrama Samudrala, Vipul Shah

Contributors: Luis Edgardo Argote Bolio, Alan Galbreath, Diego Iglesias, Donna Keesling, Aneesh Khandelwai, Sarma Namuduri, Gowri Suserla, Wei You

Contents

3 Oracle Grid Infrastructure

4 Installing the Oracle Audit Vault Server

5 Removing the Oracle Audit Vault Server Software

A Installing and Configuring Oracle Products Using Response Files

List of Tables

Preface

The Oracle Audit Vault Server Installation Guide 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 and those who are involved in the installation of Oracle Audit Vault and its related components.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- *Oracle Audit Vault Release Notes*
- *Oracle Audit Vault Licensing Information*
- *Oracle Audit Vault Collection Agent Installation Guide*
- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Real Application Clusters Installation Guide for Linux and UNIX*
- *Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Database Vault Installation Guide for Linux x86-64*

- *Oracle Database Vault Administrator's Guide*

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

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

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

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

For OTN information specific to Oracle Audit Vault, visit

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

For the Oracle Audit Vault Discussion Forums, visit

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

Conventions

The following text conventions are used in this document:

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

1

Oracle Audit Vault Server Installation Overview

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

> **Note:** To upgrade previous releases of Oracle Audit Vault to version 10.3, see the upgrade section of the *Oracle Audit Vault Release Notes*.

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

1.1 Deploying Oracle Audit Vault Server

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

1.2 Oracle Audit Vault Installation Components

Oracle Audit Vault software installation consists of two parts:

- 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 collection agent installation (see *Oracle Audit Vault Collection Agent Installation Guide*)

1.3 Oracle Audit Vault Installation Methods

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

- Interactive Installation Methods
- Automated Installation Methods Using Response Files

1.3.1 Interactive Installation Methods

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

1.3.2 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.

You can prepare the response file by entering values for all parameters that are missing in the response file, then save the file. For parameters that should not be changed, a comment is included in the file to indicate that you should not change the parameter value. Refer to Section A.3.2 for more information about saving a response file.

See Section 4.7 for specific information about performing an Audit Vault Server silent installation.

For information about installing Oracle products using response files, see Appendix A.

1.4 Oracle Audit Vault Server Installation

The Audit Vault server installation consists of two options:

- Create and configure Oracle Audit Vault - Performs a full installation and configuration of Audit Vault Server.
- Install Oracle Audit Vault software only - Only lays down the software bits and does no configuration of the Oracle Audit Vault Server software.

The Audit Vault server installation consists of two methods of installation:

- Basic installation – Simplifies the installation process and prompts for a minimal set of inputs from the user to perform a full installation. An Oracle RAC installation is not supported through this option; only a single instance installation is supported.
- Advanced installation – Offers the user more control and options for the installation process, including storage options and backup options. This option supports the installation of Audit Vault Server on a cluster and as a single instance.

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

After you check the requirements described in Section 1.6, the general steps to install Oracle Audit Vault Server include these tasks:

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

1.5 Oracle Audit Vault Server Software Only Installation

You can install Oracle Audit Vault Server as a software only installation for the purpose of installing software patches in which the installation installs only the software binaries and performs no configuration tasks. Then you can run the configuration assistants using a response file to automate the patch installation and configuration of the Audit Vault Server installation. The first configuration assistant will apply the patches, and the other configuration assistants will have fixes available to them before they run. This includes assistants that run Network Configuration Assistant (NETCA), Database Configuration Assistant (DBCA) or Database Upgrade Assistant (DBUA), Database Vault Configuration Assistant (DVCA), and Audit Vault Configuration Assistant (AVCA).

The advantages of performing a software only installation includes the following patch installation scenarios:

- Applying one or more required RDBMS patches that became available
- Applying a required CPU patch that became available for the database
- Applying a required Audit Vault 10.3.0.0 Bundle Patch that became available
- Applying one or more required one-off patches that became available

In all cases, instead of applying these patches after the installation completes, you can follow the steps in Section 4.6 and apply these patches as part of the installation process. This is a more efficient and automated way to apply any required software patches during an initial Oracle Audit Vault Server installation.

See Section 4.6 for more information about the steps to follow to complete a software only installation.

1.6 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
- Oracle Grid Infrastructure for a Standalone Server
- Oracle Cluster Synchronization Services

1.6.1 Hardware and Software Considerations

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

`https://support.oracle.com`

1.6.2 Multiple Oracle Homes

This product supports multiple Oracle homes. This means you can install this release of the software more than once on the same system, in different Oracle home directories. See Section 2.8.2 for more information.

1.6.3 Oracle Grid Infrastructure for a Standalone Server

The Oracle Grid Infrastructure for a standalone server provides the infrastructure to include your single-instance Oracle Audit Vault Server in an enterprise grid architecture. Because Oracle Audit Vault Server Release 10.3 installs a customized, specially configured release of Oracle Database 11*g* Release 2 (11.2.0.3.0), it combines these infrastructure products into one software installation called the Oracle Grid Infrastructure home. On a single-instance database, the Oracle Grid Infrastructure home includes Oracle Restart and Oracle Automatic Storage Management (Oracle ASM) software.

If you want to use Oracle ASM or Oracle Restart, then first install Oracle Grid Infrastructure for a standalone server, and then install Oracle Oracle Audit Vault Server Release 10.3.

Note: Oracle Audit Vault supports Oracle Restart, but only for the Audit Vault repository database. The Audit Vault Administrator must manually restart all Audit Vault services, those services being the Audit Vault Server (Audit Vault Console), the Audit Vault Collection Agent, and the Audit Vault Collectors, in that order, to complete the restart operation. See *Oracle Audit Vault Administrator's Guide* for more information.

See Also: Chapter 3 for more information about installing Oracle Grid Infrastructure for a standalone server

1.6.4 Oracle Cluster Synchronization Services

When you install Oracle Grid Infrastructure for a standalone server, Oracle Universal Installer (OUI) will configure the single-node version of Oracle Cluster Synchronization Services (CSS). The CSS service is required to enable synchronization between an Oracle ASM instance and the database instances that rely on it for database file storage. Because the service must be running before an Oracle ASM instance or database instance starts, it is configured to start automatically by Oracle Restart before the Oracle ASM instance is started.

For single-instance installations, the CSS daemon is installed in and runs from the Oracle Grid Infrastructure home which is the same home that runs Oracle ASM.

See Also:

- Section 1.7.2 about Oracle Automatic Storage Management
- Section 5.2 about reconfiguring Oracle Cluster Synchronization Services
- Section 5.3 about removing Oracle Audit Vault Server software using the Deinstallation Tool

1.7 Database Storage Options

When you install Oracle Audit Vault Server, it creates a database during the installation, which is why you can specify one of the following storage options for database files:

- File System
- Oracle Automatic Storage Management

Note: Installing files on raw devices is no longer an option during installation. You must use a file system or Oracle Automatic Storage Management (Oracle ASM).

1.7.1 File System

If you use the file system option, then Oracle Database Configuration Assistant creates the database files in a directory on a file system mounted on the computer. Oracle recommends that the file system be separate from the file systems used by the operating system or the Oracle software. The file system 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 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 mount point for the database storage.

- A network file system (NFS) mounted from a certified network-attached storage (NAS) device. You also have the option to use the Direct NFS feature, which simplifies the administration of NFS configurations and also improves performance.

  See Also: The "Direct NFS Client" section in the "Oracle Database Postinstallation Tasks" chapter in *Oracle Database Installation Guide for Linux*

  If the NAS device is certified by Oracle, then you can store the database files on them.

If you use the Advanced database creation option, then you can also use the Oracle Managed Files feature with the new database. If you use this feature, then you must specify only the database object name instead of file names when creating or deleting database files.

See Also: "Specifying Oracle Managed Files at Database Creation" in *Oracle Database Administrator's Guide*

1.7.2 Oracle Automatic Storage Management

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

Oracle ASM can be used with single database installations, multiple database installations, and in Oracle RAC environments. It can be used with databases created in Oracle Database 10*g* Release 1 (10.1.0.3 or later). However, Oracle Database 11*g* Release 2 (11.2) databases must use Oracle ASM from Oracle Database 11*g* Release 2 (11.2) or later. Oracle ASM is installed as part of the Oracle Grid Infrastructure installation. If you plan to use Oracle ASM, then you must install Oracle Grid Infrastructure before installing your database. If you want to upgrade an existing Oracle ASM installation, then you must upgrade Oracle ASM by running an Oracle Grid Infrastructure upgrade.

Oracle ASM Release 11.2.0.3 requires Oracle Clusterware Release 11.2.0.3. Oracle Audit Vault 10.3 requires Cluster Ready Services (CRS) 11.2.0.3, which installs with Oracle Clusterware Release 11.2.0.3.

See Also: Chapter 3 for more information about installing the Oracle Grid Infrastructure software

Oracle ASM manages the storage of all database files, such as redo logs, control files, and data pump export files.

Oracle ASM can manage the Oracle Audit Vault Server executable binary files and any other non-database file by creating a file system with Oracle Automatic Storage Management Cluster File System. Although Oracle Automatic Storage Management Cluster File System is cluster-aware, it also works as a file system on a single-instance database.

> **See Also:** "Introduction to Oracle ACFS" in *Oracle Automatic Storage Management Administrator's Guide* for information about Oracle Automatic Storage Management Cluster File System

At a high level, implementing Oracle ASM involves allocating partitioned disks for Oracle Audit Vault Server with preferences for striping and mirroring. Oracle ASM manages the disk space for you. This helps avoid the need for traditional disk management tools, such as Logical Volume Managers (LVM), file systems, and the numerous commands necessary to manage both. The synchronization between Oracle ASM and the database instance is handled by CSS.

The following are components of an Oracle ASM installation:

- Oracle Automatic Storage Management Disk Groups
- Oracle Automatic Storage Management Instance

Oracle Automatic Storage Management Disk Groups

A disk group is a set of disk devices that Oracle ASM manages as a single unit. Each disk device can be an individual physical disk, a multiple disk device, such as a RAID storage array or logical volume, or a partition on a physical disk. In most cases, disk groups consist of one or more individual physical disks. To enable Oracle ASM to balance input/output operations and storage efficiently within the disk group, you must ensure that all devices in the disk group have similar, if not identical, storage capacity and performance.

You can set the redundancy and striping attributes of individual file types within a disk group by using Oracle ASM disk group templates. When you create a disk group, Oracle ASM creates a set of default templates for that disk group. Default template settings depend on the disk group type. For example, the default template for control files for both normal and high redundancy disk groups is set to three-way mirroring. All other file templates are two-way mirrored. For a high redundancy disk group, the default mirroring cannot be changed, which implies that all files are always three-way mirrored in a high redundancy disk group. You can modify the default templates to suit your site's needs. See *Oracle Automatic Storage Management Administrator's Guide* for more information.

Oracle ASM spreads data evenly across all the devices in the disk group to optimize performance and utilization. You can add or remove disk devices from a disk group without shutting down the database. When you add or remove disks, Oracle ASM rebalances the files across the disk group. You can create multiple disk groups to do specific tasks, such as backup and recovery operations, in addition to regular file storage activities.

When you add a device to a disk group, you can specify a failure group for that device. Failure groups identify disk devices that have common failure characteristics, for example, devices that are attached to the same controller. If the controller fails, then all devices attached to it become unavailable. By default, each device also belongs to its own failure group. By using the failure groups you specify, Oracle ASM can distribute data among the devices in the disk group to minimize the risk of data loss caused by component failures.

Oracle Automatic Storage Management Instance

The Oracle ASM instance is a special Oracle instance that manages Oracle ASM disk groups. The Oracle ASM instance and the `ASMSNMP` account are created and started, if necessary, when you install Oracle Grid Infrastructure. Oracle Enterprise Manager uses this account to monitor Oracle ASM instances to retrieve data from Oracle

ASM-related data dictionary views. The ASMSNMP account status is set to OPEN upon creation, and it is granted the SYSDBA privilege.

Oracle recommends that you have the Oracle ASM instance in its own Oracle home. Oracle also recommends that you run this instance before you start a database instance that uses Oracle ASM.

For an Oracle Audit Vault Server installation, you only need one Oracle ASM instance, regardless of the number of database instances on the computer.

> **See Also:** "Managing Oracle ASM Users with Oracle Enterprise Manager" in *Oracle Automatic Storage Management Administrator's Guide* for information about the ASMSNMP user

1.8 Database Management Options

To simplify database administration, Oracle provides a Web-based management tool called Oracle Enterprise Manager. There are different ways to deploy Oracle Enterprise Manager:

- Deploy Oracle Enterprise Manager centrally in the environment

  To deploy Oracle Enterprise Manager centrally, you must install at least one Oracle Management Repository and one Oracle Management Service within the environment, then install an Oracle Enterprise Management Agent on every computer that you want to manage. You can then use a single HTML interface to manage and monitor software and hardware targets on all of those systems. Targets can include Oracle databases, application servers, net listeners, and third-party software. This single interface is called Oracle Enterprise Manager Grid Control (Grid Control).

  Note:

  - Oracle Enterprise Manager is available separately on the Oracle Enterprise Manager Grid Control installation media, and on the Oracle Technology Network Web site at:

    http://www.oracle.com/technology/documentation/oem.html

  - For the latest certification information, see My Oracle Support note 412431.1, "Oracle Enterprise Manager Grid Control Certification Checker" at:

    https://support.oracle.com/

- Deploy Oracle Enterprise Manager Database Control locally on the database system

  Oracle Enterprise Manager Database Control software is installed by default with every Oracle Audit Vault Server installation. This local installation provides a Web-based interface called Oracle Enterprise Manager Database Control. The Database Control is similar to the Grid Control, but it can manage only a single database. If you want to administer more than one database on a system, then you must either configure a separate Database Control for each database, or you must install Oracle Enterprise Manager Grid Control.

See Also: *Oracle Enterprise Manager Concepts* manual and the *Oracle Enterprise Manager Grid Control Basic Installation Guide* on the Oracle Enterprise Manager Grid Control installation media for more information about Oracle Enterprise Manager

This section contains the following topics:

- Management Options for Audit Vault Server
- Features Provided by Oracle Enterprise Manager Database Control

1.8.1 Management Options for Audit Vault Server

When you install Audit Vault Server, you must select the Oracle Enterprise Manager interface that you want to use to manage the Audit Vault repository database. The following options are available:

- Use Grid Control for central database management

  This option is available only if an Oracle Enterprise Manager Database Control Agent is installed on the system. When Oracle Universal Installer detects an Oracle Management Agent on the system, you can choose this option and specify the Oracle Management Service that you want to use to manage the database.

  If an Oracle Management Agent is not installed, then you must use Database Control to manage the database. However, if Oracle Management Agent is installed after Oracle Audit Vault Server, then you can use Grid Control to manage this database.

- Use Database Control for local database management

  This option is selected by default if an Oracle Management Agent is not installed on the system. However, even if a Management Agent is installed, you can still configure Database Control to manage the database.

1.8.2 Features Provided by Oracle Enterprise Manager Database Control

Oracle Enterprise Manager Database Control provides a Web-based user interface that enables you to monitor, administer, and maintain an Oracle database. You can use it to perform all database administration tasks. You can also use it to determine information about the database, such as:

- Instance name, database version, Oracle home location, media recovery options, and other instance data
- Current instance availability
- Database alert information
- Session and SQL-related performance information
- Space usage matrix

In addition, it provides you with automatic notification of security alerts and the ability to download and apply patches for the software.

1.9 Database Backup and Recovery Options

If you use Oracle Enterprise Manager Database Control during the installation, then you can optionally enable automated database backups that use the Oracle-suggested default backup strategy. You do not have to enable automated backups during the

installation. If you prefer, you can use Oracle Enterprise Manager Database Control or Grid Control to configure automated backups after you install the software and create a database.

This section contains the following topics:

- Enabling Automated Backups
- Backup Job Default Settings

See Also:

- *Oracle Database 2 Day DBA* for information about using Oracle Enterprise Manager Database Control to configure or customize automated backups or to recover a backed up database
- *Oracle Database Backup and Recovery User's Guide* for more detailed information about defining a backup strategy and backing up and recovering Oracle databases

1.9.1 Enabling Automated Backups

If you 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 a disk storage area called the fast recovery area. The first time the backup job runs, it creates a full backup of the database. Subsequent backup jobs perform incremental backups, which enable you to recover the database to its state at any point during the preceding 24 hours.

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

- The location of the fast recovery area

  You can use either a file system directory or an Oracle ASM disk group for the fast recovery area. To set the default values for fast recovery area and data file location, use Oracle base as the starting point. See Section 2.12.1 for more information on Oracle base.

  - Default fast recovery area: `$ORACLE_BASE/recovery_area`
  - Default data file location: `$ORACLE_BASE/oradata`

  The default disk quota configured for the fast recovery area is 2 GB. For Oracle ASM disk groups, the required disk space depends on the redundancy level of the disk group that you choose. Section 4.10.4 describes how to choose the location of the fast recovery area and identifies 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 UNIX group that identifies database administrators (the `ORA_DBA` group). This user also must have Logon As A Batch Job privilege.

1.9.2 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 every morning at 2.00 a.m.

- The disk quota for the fast recovery area is 2 GB.

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

1.10 E-mail Notification Options

If you use the Oracle Enterprise Manager Database Control during the installation, then you can configure Oracle Enterprise Manager to send an email when specific events occur. These events can include occurrences such as the disk space reaching a critical limit (a threshold) or a database shutting down unexpectedly.

If you enable email notifications, then you must specify the following information:

- The host name of a Simple Mail Transfer Protocol (SMTP) server
- The email address that should receive the alerts

  The email address that you specify could belong to an individual, or a shared email account, or a distribution list.

You can use Oracle Enterprise Manager Database Control to set up, change, or customize email notifications after you create the database.

2

Oracle Audit Vault Preinstallation Requirements

This chapter describes the tasks that you must complete before you start Oracle Universal Installer to install Oracle Audit Vault Server (Audit Vault Server) Release 10.3. It includes information about the following tasks:

> **Note:**
>
> If you want to use Oracle Automatic Storage Management (Oracle ASM) or Oracle Restart, then you must first install Oracle Grid Infrastructure for a standalone server and then install Oracle Audit Vault Server.

- Setting the Correct Locale

See Also:

- "Requirements for Oracle Grid Infrastructure Installation" section in *Oracle Database Installation Guide for Linux*
- "Preinstallation Requirements" section in *Oracle Configuration Manager Installation and Administration Guide* and *Oracle Configuration Manager Prerequisites*
- Appendix A, "Country Codes", in *Oracle Configuration Manager Installation and Administration Guide* for a list of valid country codes that can be used while installing Oracle Configuration Manager

2.1 Logging In to the System as root

Before you install the Oracle software, you must complete several tasks as the `root` user. To log in as the `root` user, complete the following procedure:

```
$ sudo sh
password:
#
```

2.2 Checking the Hardware Requirements

The system must meet the following minimum hardware requirements:

- Memory Requirements
- System Architecture
- Disk Space Requirements
- Display Requirements

2.2.1 Memory Requirements

The following are the memory requirements for installing Oracle Audit Vault Server Release 10.3, which installs a customized, specially configured release of Oracle Database 11*g* Release 2 (11.2.0.3).

On Linux x86-64:

Minimum: 1 GB of RAM

Recommended: 2 GB of RAM or more

- To determine the RAM size, enter the following command:

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

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

- The following table describes the relationship between the installed RAM and the configured swap space recommendation:

Note: On Linux, the HugePages feature allocates non-swappable memory for large page tables using memory-mapped files. If you enable HugePages, then you deduct the memory allocated to HugePages from the available RAM before calculating the swap space.

RAM	Swap Space
Between 1 GB and 2 GB	1.5 times the size of the RAM
Between 2 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

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

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

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

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

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

```
# free
```

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

Automatic Memory Management

In the current release, the Automatic Memory Management feature requires more shared memory (`/dev/shm`) and file descriptors. The size of the shared memory must be at least the greater of the `MEMORY_MAX_TARGET` and `MEMORY_TARGET` parameters for each Oracle instance on the computer. If the `MEMORY_MAX_TARGET` parameter or the `MEMORY_TARGET` parameter is set to a non-zero value, and an incorrect size is assigned to the shared memory, it results in an `ORA-00845` error at startup. On Linux systems, if the operating system `/dev/shm` mount size is too small for the Oracle system global area (SGA) and program global area (PGA), it will result in an `ORA-00845` error.

The number of file descriptors for each Oracle instance must be at least `512*`*`PROCESSES`*. The limit of descriptors for each process must be at least 512. If file descriptors are not sized correctly, you will see an `ORA-27123` error from various Oracle processes and potentially `Linux Error EMFILE (Too many open files)` in non-Oracle processes.

To determine the amount of shared memory available, enter the following command:

```
# df -h /dev/shm/
```

Note: The MEMORY_MAX_TARGET and MEMORY_TARGET parameters cannot be used when the LOCK_SGA parameter is enabled, or with HugePages on Linux.

On the Initialization Parameters page, note the **Memory Size** (SGA and PGA), which sets the initialization parameter MEMORY_TARGET or MEMORY_MAX_TARGET. Note that the initialization parameters cannot be greater than the shared memory file system on the operating system. For example, if the shared memory file system allocation on your system is 1 GB, but you set M**emory Size** (MEMORY_TARGET) to 2 GB, then the following error messages are displayed during database startup:

```
ORA-00845: MEMORY_TARGET not supported on this system
ORA-01078: Failure in processing system parameters
```

In addition, if you click **All Initialization Parameters** and the global database name is longer than eight characters, then the database name value (in the DB_NAME parameter) is truncated to the first eight characters, and the DB_UNIQUE_NAME parameter value is set to the global name.

The workaround, if you encounter the ORA-00845 error, is to increase the /dev/shm mountpoint size.

For example:

```
# mount -t tmpfs shmfs -o size=7g /dev/shm
```

To make this change persistent across system restarts, add an entry in /etc/fstab similar to the following:

```
shmfs /dev/shm tmpfs size=7g 0
```

2.2.2 System Architecture

To determine if the system architecture can run the software, enter the following command:

```
# uname -m
```

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

2.2.3 Disk Space Requirements

The following are the disk space requirements for installing Oracle Audit Vault Server Release 10.3:

- 1 GB of space in the /tmp directory

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

  ```
  # df -h /tmp
  ```

  If the free space available in the /tmp directory is less than what is required, 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.

  See Also: Section 2.18 for more information about setting `TMP` and `TMPDIR`

- Extend the file system that contains the `/tmp` directory. If necessary, contact the system administrator for information about extending file systems.

- The following tables describe the disk space requirements for software files and data files for each installation type on Linux x86-64:

Installation Type	Requirement for Software Files (GB)
Oracle Audit Vault Server	4.45

Installation Type	Disk Space for Data Files (GB)
Oracle Audit Vault Server	2.30

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

```
# df -h
```

Additional disk space, either on a file system or on an Oracle ASM disk group is required for the fast recovery area if you configure automated backups.

2.2.4 Display Requirements

The minimum resolution for Oracle Audit Vault Server is 1024 x 768 or higher.

2.3 Checking the Software Requirements

Depending on the products that you intend to install, verify that the following software is installed on your system:

- Operating System Requirements
- Kernel Requirements
- Package Requirements
- Additional Software Requirements

Note:

- This guide contains information required to install Oracle Audit Vault Server on various platforms. Ensure that you review information related to the platform on which you intend to install Oracle Audit Vault Server.
- Oracle Universal Installer performs checks on the system to verify that it meets the listed requirements. To ensure that these checks pass, verify the requirements before you start Oracle Universal Installer.

2.3.1 Operating System Requirements

The following operating system versions (or later) are required for Oracle Audit Vault Server Release 10.3:

- **On Linux x86-64**
  - Asianux Server 3 SP2
  - Oracle Linux 4 Update 7
  - Oracle Linux 5 Update 2
  - Oracle Linux 5 Update 5 (only if using Oracle Unbreakable Enterprise Kernel)
  - Red Hat Enterprise Linux 4 Update 7
  - Red Hat Enterprise Linux 5 Update 2
  - Red Hat Enterprise Linux 5 Update 5 (only if using Oracle Unbreakable Enterprise Kernel)
  - SUSE Linux Enterprise Server 10 SP2
  - SUSE Linux Enterprise Server 11

Starting with Oracle Audit Vault Server Release 10.3, the Security Enhanced Linux (SE Linux) feature is supported for Oracle Linux 4, Red Hat Enterprise Linux 4, Oracle Linux 5, and Red Hat Enterprise Linux 5.

Note: For Asianux Server, Oracle Linux, and Red Hat Enterprise Linux, the system requirements are identical by kernel version, specifically:

- Oracle Linux 4 and Red Hat Enterprise Linux 4 requirements are the same.
- Asianux Server 3, Oracle Linux 5, and Red Hat Enterprise Linux 5 Update 2 requirements are the same.
- Oracle Unbreakable Enterprise Kernel for Linux 5 Update 5 (2.6.32), available for x86-64 systems, contains several additional features and performance enhancements not available either with Oracle Linux or with other supported Linux distributions. This kernel can be installed on either Oracle Linux or Red Hat Enterprise Linux distributions. Before installing the Unbreakable Enterprise Kernel, you must have Oracle Linux 5 Update 5 or RHEL5 Update 5 installed on an x86-64 server.

To determine the distribution and version of Linux installed, enter the following command:

```
# cat /proc/version
```

You can also enter the following command on some distributions of Linux:

```
# lsb_release -id
```

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

See Also: Section 1.6.1 for information about how to access the latest system requirements

2.3.2 Kernel Requirements

The following are the kernel requirements for Oracle Audit Vault Server Release 10.3:

For Linux x86-64

- On Oracle Linux 4 and Red Hat Enterprise Linux 4

  2.6.9 or later

- On Oracle Linux 5 Update 5 with the Unbreakable Enterprise Kernel for Linux

  2.6.32-100.0.19 or later

  See *Oracle Database Installation Guide for Linux* for more information about Oracle Unbreakable Enterprise Kernel for Linux.

- On Red Hat Enterprise Linux 5 Update 5 with the Unbreakable Enterprise Kernel for Linux

  2.6.32 or later

  See *Oracle Database Installation Guide for Linux* for more information about Oracle Unbreakable Enterprise Kernel for Linux.

- On Oracle Linux 5 Update 2

  2.6.18 or later (compatible with Red Hat Enterprise kernel)

- On Asianux Server 3, Oracle Linux 5 Update 2, and Red Hat Enterprise Linux 5 Update 2

  2.6.18 or later

- On SUSE Linux Enterprise Server 10

  2.6.16.21 or later

- On SUSE Linux Enterprise Server 11

  2.6.27.19 or later

To determine if the required kernel is installed, enter the following command:

```
# uname -r
```

The following is a sample output displayed by running this command on an Oracle Linux 5 system:

```
2.6.18-128.el5PAE
```

In this example, the output shows the kernel version (`2.6.18`) and errata level (`-128.el5PAE`) on the system.

If the kernel version does not meet the requirement, then contact the operating system vendor for information about obtaining and installing kernel updates.

2.3.3 Package Requirements

The following are the list of packages required for Oracle Audit Vault Server Release 10.3:

- Linux x86-64

Note:

- Oracle recommends that you install your Linux operating system with the default software packages (RPMs), unless you specifically intend to perform a minimal installation and follow the directions for performing such an installation to ensure that you have all required packages for Oracle software.
- Oracle recommends that you do not customize RPMs during a default operating system installation. A default installation includes most required packages and will help you to limit manual verification of package dependencies.
- If you did not perform a default Linux installation, you intend to use LDAP, and you want to use the scripts `odisrvreg`, `oidca`, or `schemasync`, then install the Korn shell RPM for the Linux distribution.
- You must install the packages (or later versions) listed in the following table, and ensure that the list of RPMs and all of the prerequisites for these RPMs are installed.

Linux x86-64

IMPORTANT:

- Starting with Oracle Audit Vault Server Release 10.3 which installs a customized, specially configured release of Oracle Database 11*g* Release 2 (11.2.0.3), all the 32-bit packages, except for `gcc-32bit-4.3`, listed in the following table are no longer required for installing a database on Linux x86-64. Only the 64-bit packages are required.
- If you are using Oracle Unbreakable Enterprise Kernel, then all required kernel packages are installed as part of the Oracle Unbreakable Enterprise Kernel installation.

Operating System	Requirement
Oracle Linux 4 and Red Hat Enterprise Linux 4	The following packages (or later versions) must be installed: binutils-2.15.92.0.2 compat-libstdc++-33-3.2.3 compat-libstdc++-33-3.2.3 (32 bit) elfutils-libelf-0.97 elfutils-libelf-devel-0.97 expat-1.95.7 gcc-3.4.6 gcc-c++-3.4.6 glibc-2.3.4-2.41 glibc-2.3.4-2.41 (32 bit) glibc-common-2.3.4 glibc-devel-2.3.4 glibc-headers-2.3.4 libaio-0.3.105 libaio-0.3.105 (32 bit) libaio-devel-0.3.105 libaio-devel-0.3.105 (32 bit) libgcc-3.4.6 libgcc-3.4.6 (32-bit) libstdc++-3.4.6 libstdc++-3.4.6 (32 bit) libstdc++-devel 3.4.6 make-3.80 numactl-0.6.4.x86_64 pdksh-5.2.14 sysstat-5.0.5

Operating System	Requirement
Asianux Server 3, Oracle Linux 5, and Red Hat Enterprise Linux 5	The following packages (or later versions) must be installed: binutils-2.17.50.0.6 compat-libstdc++-33-3.2.3 compat-libstdc++-33-3.2.3 (32 bit) elfutils-libelf-0.125 elfutils-libelf-devel-0.125 gcc-4.1.2 gcc-c++-4.1.2 glibc-2.5-24 glibc-2.5-24 (32 bit) glibc-common-2.5 glibc-devel-2.5 glibc-devel-2.5 (32 bit) glibc-headers-2.5 ksh-20060214 libaio-0.3.106 libaio-0.3.106 (32 bit) libaio-devel-0.3.106 libaio-devel-0.3.106 (32 bit) libgcc-4.1.2 libgcc-4.1.2 (32 bit) libstdc++-4.1.2 libstdc++-4.1.2 (32 bit) libstdc++-devel 4.1.2 make-3.81 numactl-devel-0.9.8.x86_64 sysstat-7.0.2
SUSE Linux Enterprise Server 10	The following packages (or later versions) must be installed: binutils-2.16.91.0.5 compat-libstdc++-5.0.7 gcc-4.1.0 gcc-c++-4.1.2 glibc-2.4-31.63 glibc-devel-2.4-31.63 glibc-devel-32bit-2.4-31.63 ksh-93r-12.9 libaio-0.3.104 libaio-32bit-0.3.104 libaio-devel-0.3.104 libaio-devel-32bit-0.3.104 libelf-0.8.5 libgcc-4.1.2 libstdc++-4.1.2 libstdc++-devel-4.1.2 make-3.80 numactl-0.9.6.x86_64 sysstat-8.0.4

Operating System	Requirement
SUSE Linux Enterprise Server 11	The following packages (or later versions) must be installed: binutils-2.19 gcc-4.3 gcc-32bit-4.3 gcc-c++-4.3 glibc-2.9 glibc-32bit-2.9 glibc-devel-2.9 glibc-devel-32bit-2.9 ksh-93t libaio-0.3.104 libaio-32bit-0.3.104 libaio-devel-0.3.104 libaio-devel-32bit-0.3.104 libstdc++33-3.3.3 libstdc++33-32bit-3.3.3 libstdc++43-4.3.3_20081022 libstdc++43-32bit-4.3.3_20081022 libstdc++43-devel-4.3.3_20081022 libstdc++43-devel-32bit-4.3.3_20081022 libgcc43-4.3.3_20081022 libstdc++-devel-4.3 make-3.81 sysstat-8.1.5

Note: The `numa` package link for Linux x86-64 is `/usr/lib64/`.

To determine if the required packages are installed, enter commands similar to the following:

```
# rpm -q package_name
```

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

2.3.4 Additional Software Requirements

Depending on the components you want to use, you must ensure that the following software is installed:

- Oracle JDBC/OCI Drivers
- Linux-PAM Library
- Browser Requirements

See Also: Chapter 2, "Oracle Application Express Installation Requirements" and "Recommended Pre-installation Tasks" in *Oracle Application Express Installation Guide*

2.3.4.1 Oracle JDBC/OCI Drivers

Use JDK 6 (Java SE Development Kit `1.6.0_21`) or JDK 5 (`1.5.0_24`) with the JNDI extension with the Oracle Java Database Connectivity and Oracle Call Interface

drivers. However, these are not mandatory for the database installation. Note that JDK 1.5 is installed with this release.

2.3.4.2 Linux-PAM Library

Install the latest Linux-PAM (Pluggable Authentication Modules for Linux) library to enable the system administrator to choose how applications authenticate users.

2.3.4.3 Browser Requirements

Web browsers must support JavaScript, and the HTML 4.0 and CSS 1.0 standards. The following browsers meet these requirements for Oracle Enterprise Manager Database Control:

- Netscape Navigator 8.1
- Netscape Navigator 9.0
- Microsoft Internet Explorer 6.0 SP2
- Microsoft Internet Explorer 7.0 SP1
- Microsoft Internet Explorer 8.0
- Firefox 2.0
- Firefox 3.0.7
- Firefox 3.5
- Firefox 3.6
- Safari 3.1
- Safari 3.2
- Safari 4.0.x
- Google Chrome 3.0
- Google Chrome 4.0

2.4 Installation Fixup Scripts

During installation, for certain prerequisite verification failures, click **Fix & Check Again** to generate a fixup script (`runfixup.sh`). You can run this script as the `root` user to complete the required preinstallation steps.

The fixup script:

- Checks for and sets kernel parameters to values required for successful installation, including:
  - Shared memory parameters
  - Open file descriptor and UDP send/receive parameters

Oracle recommends that you do not modify the contents of the generated fixup script.

Note: Using fixup scripts does not ensure that all the prerequisites for installing Oracle Audit Vault Server are met. You must still verify that all the preinstallation requirements are met to ensure a successful installation.

2.5 Enabling Core File Creation

During installation, the installer checks the system configuration file that sets core dump preferences to see if core dumps are enabled. The value must be a file, and the file is checked to see if it contains the value of one (1). The following files are checked, in order of precedence:

```
/proc/sys/kernel/suid_dumpable
/proc/sys/fs/suid_dumpable
/proc/sys/kernel/core_setuid_ok
```

The first file that is present is read. If a value other than 1 is present in the file, then core files are disabled. Enabling core file creation can vary between Linux distributions; see your Linux vendor documentation for information about how to enable core file creation. The following example shows how to enable core file creation on Oracle Linux 5 and Red Hat Enterprise Linux 5:

1. Use a text editor to open the `/etc/profile` file of the Oracle Grid Infrastructure installation owner and find the following line:

   ```
   ulimit –S –c 0 > /dev/null 2>&1
   ```

   Change it to the following:

   ```
   ulimit -S -c unlimited > /dev/null 2>&1
   ```

2. Use a text editor to open `/etc/sysctl.conf` and find the following line:

   ```
   kernel.core_uses_pid
   ```

   Confirm that the file is set to 1. This setting appends the PID to the generated core file, which allows multiple core file dumps.

   If `kernel.core_uses_pid` is missing, then add the following line:

   ```
   kernel.core_uses_pid = 1
   ```

3. Find the following line:

   ```
   fs.suid_dumpable
   ```

   By default, this value is set to 0 . Change it to 1.

   If `fs.suid_dumpable` is not in the `sysctl.conf` file, then add the following line:

   ```
   fs.suid_dumpable = 1
   ```

4. Save `/etc/sysctl.conf` and use the following command to reload settings:

   ```
   # sysctl -p
   ```

2.6 Verifying UDP and TCP Kernel Parameters

Set TCP/IP ephemeral port range parameters to provide enough ephemeral ports for the anticipated server workload. Ensure that the lower range is set to at least 9000 or higher, to avoid Well Known ports, and to avoid ports in the Registered Ports range commonly used by Oracle and other server ports. Set the port range high enough to avoid reserved ports for any applications you may intend to use. If the lower value of the range you have is greater than 9000, and the range is large enough for your anticipated workload, then you can ignore OUI warnings regarding the ephemeral port range.

For example, with IPv4, use the following command to check your current range for ephemeral ports:

```
$ cat /proc/sys/net/ipv4/ip_local_port_range
32768 61000
```

In the preceding example, the lowest port (32768) and the highest port (61000) are set to the default range.

If necessary, update the UDP and TCP ephemeral port range to a range high enough for anticipated system workloads, and to ensure that the ephemeral port range starts at 9000 and above. For example:

```
# echo 9000 65500 > /proc/sys/net/ipv4/ip_local_port_range
```

Oracle recommends that you make these settings permanent. For example, as `root`, use a text editor to open `/etc/sysctl`, and add or change to the following: `net.ipv4.ip_local_port_range = 9000 65500`, and then restart the network (`# /etc/rc.d/init.d/network restart`). Refer to your Linux distribution system administration documentation for detailed information about how to automate this ephemeral port range alteration on system restarts.

2.7 Installing the cvuqdisk Package for Linux

Install the operating system package `cvuqdisk`. Without `cvuqdisk`, the Cluster Verification Utility cannot find shared disks, and you receive a "Package cvuqdisk not installed" error when you run the Cluster Verification Utility. Use the `cvuqdisk` RPM for your hardware (for example, `x86_64`, or `i386`).

To install the `cvuqdisk` RPM, complete the following procedure:

> **Note:** If you prefer, you can disable Cluster Verification Utility shared disk checks by adding the following line to the file *`oracle_home1`*`/cv/admin/cvu_config`:
>
> `CV_RAW_CHECK_ENABLED=FALSE`
>
> In this example, *`oracle_home1`* is the Oracle home directory where the database is installed.

1. Locate the `cvuqdisk` RPM package, which is in the directory `rpm` on the installation media. If you already installed Oracle Grid Infrastructure, then it is in the directory *`oracle_home1`*`/cv/rpm`.
2. Log in as `root`.
3. Use the following command to find if you have an existing version of the `cvuqdisk` package:

   ```
   # rpm -qi cvuqdisk
   ```

   If you have an existing version, then enter the following command to deinstall the existing version:

   ```
   # rpm -e cvuqdisk
   ```

4. Set the environment variable `CVUQDISK_GRP` to point to the group that will own `cvuqdisk`, typically `oinstall`, for example:

   ```
   # CVUQDISK_GRP=oinstall; export CVUQDISK_GRP
   ```

5. In the directory where you have saved the `cvuqdisk` RPM, use the following command to install the `cvuqdisk` package:

   ```
   rpm -iv package
   ```

   For example:

   ```
   # rpm -iv cvuqdisk-1.0.9-1.rpm
   ```

2.8 Checking the Network Setup

Typically, the computer on which you want to install Oracle Audit Vault Server is connected to the network. The computer has local storage to store the Oracle Audit Vault Server installation. It also contains a display monitor and DVD drive. This section describes how to install Oracle Audit Vault Server on computers that do not meet the typical scenario. It describes the following cases:

- Installing on DHCP Computers
- Installing on Multihomed Computers
- Installing on Computers with Multiple Aliases

2.8.1 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 a unique IP address to the newly added computer.

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

2.8.2 Installing on Multihomed Computers

You can install Oracle Audit Vault Server on a multihomed computer. A multihomed 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 `ORACLE_HOSTNAME` is not set and you are installing on a computer that has multiple network cards, then Oracle Universal Installer determines the host name from 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.example.com, then enter one of the following commands:

In Bourne, Bash, or Korn shell:

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

In C shell:

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

2.8.3 Installing on Computers with Multiple Aliases

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

2.9 Creating Required Operating System Groups and Users

Depending on if 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. Log in to your system as the root user before you attempt to create these operating system groups and users.

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

- The OSDBA group (dba)

  You must create this group the first time you install 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.

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

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

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

If you prefer to allocate operating system user privileges so that you can use one administrative user and one group for operating system authentication for all administrative privileges, then you can use the `oracle` user as the installation owner, and use one group as the primary group for any user requiring administrative privileges for Oracle ASM, and Oracle Audit Vault Server administration. This group must also be the Oracle Inventory group. To simplify using the defaults for Oracle tools the group name should be `oinstall`.

You can also create custom configuration groups and users based on job role separation. A custom configuration is a configuration with groups and users that divide access privileges granted by membership in separate operating system groups and users. You can create a single user (for example, `oracle`) to own both Oracle Audit Vault Server, and Oracle Grid Infrastructure installations. Alternatively, you can create a separate user (for example, `grid`) to own the Oracle Grid Infrastructure installation.

Note that all Oracle Audit Vault Server and Oracle Grid Infrastructure for a standalone server installations must be owned by the Oracle software owner user (`oracle`), and belong to the Oracle Inventory group (`oinstall`).

- Creating Custom Configuration Groups and Users for Job Roles
- Creating Database Operating System Groups and Users with Job Role Separation

> **Note:** In Oracle documentation, a user created to own only Oracle Grid Infrastructure software installations is called the `grid` user. A user created to own either all Oracle installations, or only Oracle database installations, is called the `oracle` user.

2.9.1 Creating Custom Configuration Groups and Users for Job Roles

This section provides an overview of how to create users and groups to divide access privileges by job roles. Log in as `root` to create these groups and users.

- Understanding Restrictions for Oracle Installations with Job Role Separation
- Database Groups for Job Role Installations
- Oracle Grid Infrastructure Groups for Job Role Installations

2.9.1.1 Understanding Restrictions for Oracle Installations with Job Role Separation

Oracle recommends that you create one software owner to own each Oracle software installation (typically, `oracle`, for the database software and `grid` for the Oracle Restart owner user). You must create at least one software owner the first time you install Oracle software on the system.

To create separate Oracle software owners, to create separate users, and separate operating system privileges groups for different Oracle software installations, note that each of these users must have the Oracle central inventory group (`oraInventory` group) as their primary group. Members of this group have write privileges to the Oracle central inventory (`oraInventory`) directory. In Oracle documentation, this group is represented as `oinstall` in code examples. See Section 2.9.2.1 about creating the Oracle Inventory Group.

The database software owner (typically, `oracle`) must also have the OSDBA group of the Oracle Grid Infrastructure home so that database instances can log on to Oracle ASM, and (if you create it) the OSOPER group as secondary groups. In Oracle documentation, the Oracle software owner users are referred to as `oracle` users.

For Oracle Grid Infrastructure only, the grid user (`grid`) must be in the OSDBA group of every database home.

> **See Also:** *Oracle Database Administrator's Guide* for more information about the OSDBA, OSASM and OSOPER groups, and the `SYSDBA`, `SYSASM` and `SYSOPER` privileges

2.9.1.2 Database Groups for Job Role Installations

Create the following operating system groups if you are installing Oracle Audit Vault Server:

- The OSDBA group (typically, `dba`)

You must create this group the first time you install Oracle software on the system. This group identifies operating system user accounts that have database administrative privileges (the SYSDBA privilege). The name used for this group in Oracle code examples is dba.

- The OSOPER group (typically, 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 database administrative privileges (the SYSOPER privilege). This group cannot directly connect as SYSOPER, unless explicitly granted. However, they will have the privileges granted by the SYSOPER privilege. By default, members of the OSDBA group have all privileges granted by the SYSOPER privilege.

  Oracle Universal Installer prompts you to specify the name of this group. The usual name chosen for this group is oper.

2.9.1.3 Oracle Grid Infrastructure Groups for Job Role Installations

Create the following operating system groups if you are installing Oracle Grid Infrastructure:

> **Note:** You can designate a unique group, separate from database administrator groups, or you can use the same group as the OSASM and OSDBA groups, to grant system privileges to administer both the Oracle ASM instances and Oracle Audit Vault Server instance.

- The OSDBA group for Oracle ASM (typically, asmdba)

  The OSDBA group for Oracle ASM can be the same group used as the OSDBA group for the database, or you can create a separate OSDBA group for Oracle ASM (typically, asmdba) to provide administrative access to Oracle ASM instances.

  The Oracle Grid Infrastructure software owner (typically, grid) must be a member of the OSDBA group. Membership in the OSDBA group enables access to the files managed by Oracle ASM. If you have a separate OSDBA group for Oracle ASM, then the Oracle Restart software owner must be a member of the OSDBA group for each database and the OSDBA group for Oracle ASM.

- The OSASM group for Oracle ASM (typically, asmadmin)

  SYSASM privileges for Oracle ASM files provide administrator privileges for storage file. In Oracle documentation, the operating system group whose members are granted SYSASM privileges is called the OSASM group, and in command lines, is referred to as asmadmin. Oracle ASM can support multiple databases.

  Members of the OSASM group can use SQL to connect to an Oracle ASM instance as SYSASM using operating system authentication. The SYSASM privileges permit mounting and dismounting of disk groups, and other storage administration tasks. SYSASM privileges provide no access privileges on an RDBMS instance.

  If you do not designate a separate group as the OSASM group, then the OSDBA group you define is also, by default, the OSASM group.

- The OSOPER group for Oracle ASM (typically, asmoper)

  This is an optional group. Create this group if you want a separate group of operating system users to have a limited set of Oracle instance administrative privileges (the SYSOPER for ASM privilege), including starting up and stopping the

Oracle ASM instance. By default, members of the OSASM group also have all privileges granted by the SYSOPER for ASM privilege.

If you want to have an OSOPER group for Oracle ASM, then the Oracle Grid Infrastructure owner must be a member of this group.

2.9.2 Creating Database Operating System Groups and Users with Job Role Separation

The following sections describe how to create the required operating system user and groups:

- Creating the Oracle Inventory Group
- Creating the OSDBA Group for Database Installations
- Creating an OSOPER Group for Database Installations
- Creating the OSASM Group for Oracle Automatic Storage Management
- Creating the OSDBA Group for Oracle Automatic Storage Management
- Creating the OSOPER Group for Oracle Automatic Storage Management
- Creating the Oracle Software Owner User

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

Oracle recommends that you do not use the UID and GID defaults on each node because group and user IDs likely will be different on each node. Instead, provide common assigned group and user IDs, and confirm that they are unused on any node before you create or modify groups and users.

2.9.2.1 Creating the Oracle Inventory Group

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 (typically, `oinstall`) and the path of the Oracle Inventory directory.

You can configure one group to be the access control group for Oracle Inventory, for database administrators (OSDBA), and for all other access control groups used by Oracle software for operating system authentication. However, this group then must be the primary group for all users granted administrative privileges.

Log in as `root`, and use the following instructions to locate or create the Oracle Inventory group and a software owner:

- Determining if the Oracle Inventory Group Exists
- Creating the Oracle Inventory Group

Determining if the Oracle Inventory Group Exists

An `oraInst.loc` file in the `/etc` or `/var/opt/oracle` directory has contents similar to the following:

```
inventory_loc=central_inventory_location
inst_group=group
```

In the preceding example, *central_inventory_location* is the location of the Oracle Central Inventory, and *group* is the name of the group that has permissions to write to the central inventory.

If you have an existing Oracle Inventory, then ensure that you use the same Oracle Inventory for all Oracle software installations, and ensure that all Oracle software users you intend to use for installation have permissions to write to this directory.

To determine if the Oracle Inventory group exist, enter the following command:

```
# grep oinstall /etc/group
```

To determine if the `oraInst.loc` file exists, enter the following command:

```
# 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/oraInventory
inst_group=oinstall
```

In the previous output example:

- The `inventory_loc` group shows the location of the Oracle Inventory
- The `inst_group` parameter shows the name of the Oracle Inventory group (in this example, `oinstall`).

Creating the Oracle Inventory Group

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

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

2.9.2.2 Creating the OSDBA Group for Database Installations

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 for a new Oracle installation

If the OSDBA group does not exist or if you require 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:

```
# /usr/sbin/groupadd -g 502 dba
```

2.9.2.3 Creating an OSOPER Group for Database Installations

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 require a new OSOPER group (typically, oper), then create it as follows. In the following, use the group name oper unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 503 oper
```

2.9.2.4 Creating the OSASM Group for Oracle Automatic Storage Management

If the OSASM group does not exist or if you require a new OSASM group, then create it as follows. In the following procedure, use the group name asmadmin unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 504 asmadmin
```

2.9.2.5 Creating the OSDBA Group for Oracle Automatic Storage Management

If you require a new OSDBA group for Oracle ASM, then create it as follows. In the following procedure, use the group name asmdba unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 506 asmdba
```

2.9.2.6 Creating the OSOPER Group for Oracle Automatic Storage Management

If you require an OSOPER group, then create it as follows. In the following procedure, use the group name asmoper unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 505 asmoper
```

2.9.2.7 Creating the Oracle Software Owner User

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

- If an Oracle software owner user does not exist; for example, if this is the first installation of Oracle software on the system.
- If an Oracle software owner user exists, but you want to use a different operating system user, with different group membership, to give database administrative privileges to those groups in a new Oracle Audit Vault Server installation.
- If you have created an Oracle software owner for Oracle Grid Infrastructure, such as grid, and you want to create a separate Oracle software owner for Oracle Audit Vault Server software, such as oracle.

2.9.2.7.1 Determining if an Oracle Software Owner User Exists To determine if an Oracle software owner user named oracle, or grid exists, enter a command similar to the following:

```
# id oracle
# id grid
```

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

```
uid=501(oracle) gid=501(oinstall) groups=502(dba),503(oper)
```

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

```
uid=8001(oracle) gid=8001(oinstall)
groups=8001(oinstall),8002(asmadmin),8003(asmdba),8006(dba)
```

Determine if you want to use the existing user or create another user. If you want to use the existing user, then ensure that the user's primary group is the Oracle Inventory group (`oinstall`) and that it is a member of the appropriate OSDBA and OSOPER groups. See the following sections for more information:

- Creating an Oracle Software Owner User
- Modifying an Existing Oracle Software Owner User

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

2.9.2.7.2 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, such as `oracle` or `grid`, then create it as described in this section (in this case to create the `oracle` user).

In the following procedure, use the user name `oracle` unless a user with that name already exists:

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

   ```
   # /usr/sbin/useradd -u 502 -g oinstall -G dba,asmdba,[oper] oracle
   ```

   In the preceding command:

   - The -u option specifies the user ID. Using this command flag is optional because the system can provide you with an automatically generated user ID number. You must note the `oracle` user ID number because you will need it during preinstallation.
   - The `-g` option specifies the primary group, which must be the Oracle Inventory group, for example `oinstall`.
   - The `-G` option specifies the secondary groups, which must include the OSDBA group, and, if required, the OSOPER and ASMDBA groups, for example, `dba`, `asmdba`, or `oper`.

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

   ```
   # passwd oracle
   ```

2.9.2.7.3 Modifying an Existing 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 modify it as follows:

Specify the primary group using the `-g` option and any required secondary group using the `-G` option:

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

2.10 Checking Resource Limits for the Oracle Software Installation Users

For each installation software owner, check the resource limits for installation, using the following recommended ranges:

Table 2–1 Installation Owner Resource Limit Recommended Ranges

Resource Shell Limit	Resource	Soft Limit	Hard Limit
Open file descriptors	nofile	At least 1024	At least 65536
Number of processes available to a single user	nproc	At least 2047	At least 16384
Size of the stack segment of the process	stack	At least 10240 KB	At least 10240 KB, and at most 32768 KB

To check resource limits:

1. Log in as an installation owner.
2. Check the soft and hard limits for the file descriptor setting. Ensure that the result is in the recommended range, for example:

```
$ ulimit -Sn
4096
$ ulimit -Hn
65536
```

3. Check the soft and hard limits for the number of processes available to a user. Ensure that the result is in the recommended range, for example:

```
$ ulimit -Su
2047
$ ulimit -Hu
16384
```

4. Check the soft limit for the stack setting. Ensure that the result is in the recommended range, for example:

```
$ ulimit -Ss
10240
$ ulimit -Hs
32768
```

5. Repeat this procedure for each Oracle software installation owner.

If necessary, update the resource limits in the `/etc/security/limits.conf` configuration file for the installation owner. For example, add the following lines to the `/etc/security/limits.conf` file:

```
oracle              soft    nproc   2047
oracle              hard    nproc   16384
oracle              soft    nofile  1024
oracle              hard    nofile  65536
oracle              soft    stack   10240
```

Note:

- The values mentioned in the previous example are illustrative and not actual values that must be added.
- When the `limits.conf` file is changed, these changes take effect immediately. However, if the `grid` or `oracle` users are logged in, then these changes will not take effect until you log these users out and log them back in. You must do this before you use these accounts for installation.

See Also: Section 2.18 about configuring the oracle user's environment

2.11 Configuring Kernel Parameters for Linux

During installation, you can generate and run the Fixup script to check and set the kernel parameter values required for successful installation of the database. This script updates required kernel packages if necessary to minimum values.

If you cannot use the Fixup scripts, then verify that the kernel parameters shown in the following table are set to values greater than or equal to the minimum value shown. The procedure following the table describes how to verify and set the values manually.

IMPORTANT: The kernel parameter and shell limit values shown in the following section are minimum values only. For production Oracle Audit Vault Server systems, Oracle recommends that you tune these values to optimize the performance of the system. See the operating system documentation for more information about tuning kernel parameters.

Parameter	Minimum Value	File
`semmsl`	250	`/proc/sys/kernel/sem`
`semmns`	32000	
`semopm`	100	
`semmni`	128	
`shmall`	2097152	`/proc/sys/kernel/shmall`
`shmmax`	**64-bit Linux Systems**: A maximum value of half the size of physical memory (in bytes). **Default**: 536870912 See *My Oracle Support* Note 567506.1 for additional information about configuring `shmmax`.	`/proc/sys/kernel/shmmax`
`shmmni`	4096	`/proc/sys/kernel/shmmni`

Parameter	Minimum Value	File
file-max	6815744	/proc/sys/fs/file-max
aio-max-nr	Maximum: 1048576 **Note**: This value limits concurrent outstanding requests and should be set to avoid I/O subsystem failures.	/proc/sys/fs/aio-max-nr
ip_local_port_range	Minimum: 9000 Maximum: 65500 See Section 2.6.	/proc/sys/net/ipv4/ip_local_port_range
rmem_default	262144	/proc/sys/net/core/rmem_default
rmem_max	4194304	/proc/sys/net/core/rmem_max
wmem_default	262144	/proc/sys/net/core/wmem_default
wmem_max	1048576	/proc/sys/net/core/wmem_max

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

See Also: Section 2.4 about installation fixup scripts

2.11.1 Displaying and Changing Kernel Parameter Values

Enter the commands shown in the following table to display the current values of the kernel parameters, make a note of these values and identify any values that you must change:

Parameter	Command
semmsl, semmns, semopm, and semmni	# /sbin/sysctl -a | grep sem This command displays the value of the semaphore parameters in the order listed.
shmall, shmmax, and shmmni	# /sbin/sysctl -a | grep shm This command displays the details of the shared memory segment sizes.
file-max	# /sbin/sysctl -a | grep file-max This command displays the maximum number of file handles.
ip_local_port_range	# /sbin/sysctl -a | grep ip_local_port_range This command displays a range of port numbers.
rmem_default	# /sbin/sysctl -a | grep rmem_default
rmem_max	# /sbin/sysctl -a | grep rmem_max
wmem_default	# /sbin/sysctl -a | grep wmem_default
wmem_max	# /sbin/sysctl -a | grep wmem_max
aio-max-nr	# /sbin/sysctl -a | grep aio-max-nr

If the value of any kernel parameter is different from the minimum value, then perform the following:

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

   Note: Include lines only for the kernel parameter values that you want to change. For the semaphore parameters (`kernel.sem`), you must specify all four values. If any of the current values are larger than the minimum value, then specify the larger value.

   ```
   fs.aio-max-nr = 1048576
   fs.file-max = 6815744
   kernel.shmall = 2097152
   kernel.shmmax = 536870912
   kernel.shmmni = 4096
   kernel.sem = 250 32000 100 128
   net.ipv4.ip_local_port_range = 9000 65500
   net.core.rmem_default = 262144
   net.core.rmem_max = 4194304
   net.core.wmem_default = 262144
   net.core.wmem_max = 1048586
   ```

   Note: The minimum value required for `shmmax` is 0.5 GB. However, Oracle recommends that you set the value of `shmmax` to 2.0 GB for optimum performance of the system.

   By specifying the values in the `/etc/sysctl.conf` file, they persist when you restart the system. However, on SUSE Linux Enterprise Server systems, enter the following command to ensure that the system reads the `/etc/sysctl.conf` file when it restarts:

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

2. Enter the following command to change the current values of the kernel parameters:

   ```
   # /sbin/sysctl -p
   ```

   Review the output from this command to verify that the values are correct. If the values are incorrect, edit the `/etc/sysctl.conf` file, then enter this command again.

3. Enter the command `/sbin/sysctl -a` to confirm that the values are set correctly.

4. On SUSE systems only, enter the following command for the system to read the `/etc/sysctl.conf` file when it restarts:

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

5. On SUSE systems only, you must enter the GID of the `oinstall` group as the value for the parameter `/proc/sys/vm/hugetlb_shm_group`. Doing this grants members of oinstall a group permission to create shared memory segments.

   For example, where the oinstall group GID is 501:

   ```
   # echo 501 > /proc/sys/vm/hugetlb_shm_group
   ```

After running this command, use `vi` to add the following text to `/etc/sysctl.conf`, and enable the `boot.sysctl` script to run on system restart:

```
vm.hugetlb_shm_group=501
```

Note: Only one group can be defined as the `vm.hugetlb_shm_group`.

6. After updating the values of kernel parameters in the `/etc/sysctl.conf` file, either restart the computer, or run the command `sysctl -p` to make the changes in the `/etc/sysctl.conf` file available in the active kernel memory.

2.12 Identifying Required Software Directories

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

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

Note:

- Ensure that the paths you select for Oracle software, such as the Oracle home path and the Oracle base path, use only ASCII characters. Because installation owner names are used by default for some path, this ASCII character restriction applies to user names, file names, and directory names.
- Ensure that all paths used by the database software, such as the Oracle home path and the Oracle base path, use characters only from the following set: "#%&'()*+,-./:;<=>?@_A-Za-z0-9. This includes user names, file names, and directory names. At the time of this release, the use of other characters for an Oracle Grid Infrastructure home or Oracle Audit Vault Server home is not supported. The set of characters provided above is further restricted by user and file naming rules of the operating system.

2.12.1 Oracle Base Directory

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

/mount_point/app/*software_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 can choose another mount point directory, such as `/oracle` or `/opt/oracle`.

- *software_owner* is the operating system user name of the software owner installing the Oracle software, for example `oracle`, or `grid`.

Note: If you start a database instance using `spfile` with `ORACLE_BASE` environment variable set, then its value is automatically stored in `spfile`. If you unset `ORACLE_BASE` environment variable subsequently and start the instance afresh, then database uses the value of Oracle base stored in `spfile`.

You must specify the Oracle base folder that contains all Oracle products.

Note: If you have an existing Oracle base, then you can select it from the Use existing list. By default, the list contains the existing value for Oracle base preselected. Refer to Section 4.3 and Section 4.5 for further information.

If you do not have an Oracle base, then you can create one by editing the text in the list box.

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 are examples of Oracle base directories that can exist on the same system:

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

Refer to Section 2.13.2 for information about creating an Oracle base directory.

2.12.2 Oracle Inventory Directory

The Oracle Inventory directory (`oraInventory`) stores an inventory of all software installed on the system. It is required and shared by all Oracle software installations on a single system. If you have an existing Oracle Inventory path, then Oracle Universal Installer continues to use that Oracle Inventory.

The first time you install Oracle software on a system, Oracle Universal Installer provides an OFA-compliant path in the format `u[01-09]/app`, such as `/u01/app`. The user running the installation has permissions to write to that path. If this is true, then Oracle Universal Installer creates the Oracle Inventory directory in the path `/u[01-09]/app/oraInventory`. For example:

```
/u01/app/oraInventory
```

If you have set `ORACLE_BASE` for the `oracle` user during installation, then Oracle Universal Installer creates the Oracle Inventory directory in the path `ORACLE_BASE/../oraInventory`. For example, if `ORACLE_BASE` is set to `/opt/oracle/11`, then the Oracle Inventory directory is created in the path `/opt/oracle/oraInventory`.

If you have neither created an OFA-compliant path nor set `ORACLE_BASE`, then the Oracle Inventory directory is placed in the home directory of the user that is performing the installation. For example:

```
/home/oracle/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.
- By default, the Oracle Inventory directory is not installed under the Oracle Base directory. This is because all Oracle software installations share a common Oracle Inventory, so there is only one Oracle Inventory for all users. Whereas, there is a separate Oracle Base for each user.

2.12.3 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 as well as 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/10.3.0/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.

Note: During installation, you must not specify an existing directory that has predefined permissions applied to it as the Oracle home directory. If you do, then you may experience installation failure due to file and group ownership permission errors.

2.13 Identifying or Creating an Oracle Base Directory

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

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

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

2.13.1 Identifying an Existing Oracle Base Directory

Existing Oracle base directories may not have paths that comply with OFA (Optimal Flexible Architecture) 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:

- Identifying an existing Oracle Inventory directory. Refer to Section 2.9.2.1 for more information.

  Note: Oracle recommends that you do not put the `oraInventory` directory under Oracle base for a new installation. However, if you have an existing installation, then you should follow the steps suggested in this section.

- Identifying an existing Oracle home directory

  Enter the following command to display 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/11.2.0/dbhome_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 can choose one of the following directories listed in the previous example:

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

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

- Identifying an existing Oracle base directory

  After you have located the Oracle home directory, run a similar command to confirm the location of Oracle base:

  ```
  cat /u01/app/oraInventory/ContentsXML/inventory.xml
  ```

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 follows:

Requirement	Free Disk Space
The Oracle base directory will contain only software files.	Up to 4 GB
The Oracle base directory will contain both software and database files (not recommended for production databases).	Up to 6 GB

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

```
# df -h oracle_base_path
```

To continue:

- If an Oracle base directory exists and you want to use it, then refer to Section 2.14.

  When you configure the `oracle` user's environment later in this chapter, set the `ORACLE_BASE` environment variable to specify the directory you chose.
- If an Oracle base directory does not exist on the system or if you want to create an Oracle base directory, then refer to the following section.

2.13.2 Creating an Oracle Base Directory

Before you create an Oracle base directory, you must identify an appropriate file system with sufficient free disk space.

To identify an appropriate file system:

1. To determine the free disk space on each mounted file system use the following command:

   ```
   # df -h
   ```

2. From the display, identify a file system that has appropriate free space.

   The file system that you identify can be a local file system, a cluster file system, or an NFS file system on a certified NAS device.

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:

   ```
   # mkdir -p /u01/app/oracle
   # chown -R oracle:oinstall /u01/app/oracle
   # chmod -R 775 /u01/app/oracle
   ```

2. When you configure the `oracle` user's environment (see Section 2.18), set the `ORACLE_BASE` environment variable to specify the Oracle base directory that you have created.

2.14 Choosing a Storage Option for Oracle Audit Vault Server and Recovery Files

Oracle Audit Vault Server files include data files, control files, redo log files, the server parameter file, and the password file. For all installations, you must choose the storage option that you want to use for Oracle Audit Vault Server files. If you want to enable automated backups during the installation, then you must also choose the storage option that you want to use for recovery files (the fast recovery area). You do not have to use the same storage option for each file type.

Note: Oracle Audit Vault Server files and recovery files are supported on file systems and Oracle ASM.

Use the following guidelines when choosing the storage options that you want to use for each file type:

- You can choose any combination of the supported storage options for each file type.
- Determine if you want to use Oracle ASM for Oracle Audit Vault Server files, recovery files, or both. Refer to the section Section 3.6.2.
- For more information about these storage options, refer to the Section 1.7.

For information about how to configure disk storage before you start the installation, refer to one of the following sections depending on your choice:

- To use a file system for database or recovery file storage, refer to Section 2.15.
- To use Oracle ASM for database or recovery file storage, refer to Section 3.6.
- To identify disk groups and determine the free disk space that they contain, refer to Section 4.1.1.

2.15 Creating Directories for Oracle Audit Vault Server or Recovery Files

This section contains the following topics:

- Guidelines for Placing Oracle Audit Vault Server Files on a File System
- Creating Required Directories

2.15.1 Guidelines for Placing Oracle Audit Vault Server Files on a File System

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

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

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

    This method enables you to distribute physical input-output operations and create separate control files on different devices for increased reliability. It also enables you to fully implement the OFA guidelines. You can choose the Advanced database creation option to implement this method.
- If you intend to create a preconfigured database during the installation, then the file system (or file systems) that you choose must have at least 2 GB of free disk space.

For production databases, you must estimate the disk space requirement depending on the use that you want to make of the database.

- 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.

2.15.2 Creating Required Directories

Note: You must perform this procedure only if you want to place the Oracle Audit Vault Server or recovery files on a separate file system to the Oracle base directory.

To create directories for the Oracle Audit Vault Server, or recovery files on separate file systems to the Oracle base directory:

1. Use the following to determine the free disk space on each mounted file system:

```
# df -h
```

2. From the display, identify the file systems that you want to use:

File Type	File System Requirements
Oracle Audit Vault Server files	Choose either: ■ A single file system with at least 2 GB of free disk space ■ Two or more file systems with at least 2 GB of free disk space in total
Recovery files	Choose a file system with at least 2.4 GB of free disk space

If you are using the same file system for more than one type of file, then add the disk space requirements for each type to determine the total disk space requirement.

3. Note the names of the mount point directories for the file systems that you identified.
4. Enter commands similar to the following to create the recommended subdirectories in each of the mount point directories and set the appropriate owner, group, and permissions on them:
   - Database file directory:

```
# mkdir /mount_point/oradata
# chown oracle:oinstall /mount_point/oradata
# chmod 775 /mount_point/oradata
```

     The default location for Database file directory is `$ORACLE_BASE/oradata`.

   - Recovery file directory (fast recovery area):

```
# mkdir /mount_point/recovery_area
# chown oracle:oinstall /mount_point/recovery_area
# chmod 775 /mount_point/recovery_area
```

The default fast recovery area is `$ORACLE_BASE/recovery_area`. However, Oracle recommends that you keep the fast recovery area on a separate physical disk than that of the database file directory. This will enable you to use the fast recovery area to retrieve data if the disk containing `oradata` is unusable due to any reasons.

5. If you also want to use Oracle ASM for storage, then refer to Section 3.6.

2.16 Configuring Storage for Oracle Audit Vault Server Files Using Block Devices

This section describes how to configure Oracle Audit Vault Server files on block devices. Use the following procedure to create block device partitions:

1. Use `fdisk` to create disk partitions on block devices for database files.

   If you intend to configure block devices and use Oracle ASM to manage data files, then create one partition for each disk comprising the whole disk, and go through the section Configuring Disks for Oracle ASM with ASMLIB in *Oracle Grid Infrastructure Installation Guide*.

2. Create or modify a rules file in `/etc/udev/rules.d`, to change the permissions of the datafiles from default `root` ownership.

   Ensure that the file you create is appropriate for your distribution. For example, name this file `99-oracle.rules` on Asianux, Red Hat Enterprise Linux, Oracle Linux, `and` SUSE Enterprise Server systems.

Example 2–1 Example of a Rules File With User oracle

```
/etc/udev/rules.d/99-oracle.rules
#
# ASM disks
KERNEL=="sdb[6-9]", OWNER="oracle", GROUP="dba", MODE="0660"
KERNEL=="sdb10", OWNER="oracle", GROUP="dba", MODE="0660"
```

Example 2–2 Example of a Rules File With User grid

```
/etc/udev/rules.d/99-oracle.rules
#
# ASM disks
KERNEL=="sdb[6-9]", OWNER="grid", GROUP="asmadmin", MODE="0660"
KERNEL=="sdb10", OWNER="grid", GROUP="asmadmin", MODE="0660"
```

See Also: Chapter 2, "Preparing Storage for ASM" in the *Oracle Automatic Storage Management Administrator's Guide* for information about preparing the storage subsystem before you configure Oracle ASM.

2.17 Configuring Disk Devices for Oracle Audit Vault Server

The `O_DIRECT` parameter enables direct read and writes to block devices, avoiding kernel overhead. With Oracle Audit Vault Server Release 10.2.3 and later, Oracle Audit Vault Server files are configured by default to use direct input/output.

With the 2. 6 kernel or later for Red Hat Enterprise Linux, Oracle Linux, and SUSE Enterprise Server, you must create a permissions file to maintain permissions on

Oracle Audit Vault Server files. If you do not create this permissions file, then permissions on disk devices revert to their default values, `root:disk`, and Oracle Audit Vault Server fails to start. Use the following steps to set the permissions file number:

- On Red Hat Enterprise Linux 4 and Oracle Linux 4, you must create a permissions file number that is lower than 50.
- On Asianux Server 3, Red Hat Enterprise Linux 5, Oracle Linux 5, SUSE Enterprise Linux 10, or SUSE Enterprise Linux 11, you must create a permissions file number that is higher than 50.

To configure a permissions file for disk devices, complete the following tasks:

- Example of Creating a Udev Permissions File for Oracle Audit Vault Server
- Example of Configuring Block Device Storage for Oracle Audit Vault Server

> **See Also:** *Oracle Grid Infrastructure Installation Guide* for information about configuring storage for Oracle Audit Vault Server files on shared storage devices.

2.17.1 Example of Creating a Udev Permissions File for Oracle Audit Vault Server

Refer to the examples in Section 2.16 for more information about creating a permissions file.

2.17.2 Example of Configuring Block Device Storage for Oracle Audit Vault Server

The following is the procedure to create partitions for Oracle Audit Vault Server files on block devices:

1. Log in as `root`
2. Enter the `fdisk` command to format a specific storage disk. For example, `/sbin/fdisk /dev/sdb`
3. Create a partition. For instance, make a partition of 280 MB for data files.
4. Use the command similar to the following to update the kernel partition table for the shared storage device:

   ```
   /sbin/partprobe diskpath
   ```

The following is an example of how to use `fdisk` to create one partition on a shared storage block disk device for a data file:

```
$ sudo sh
Password:
# /sbin/fdisk /dev/sdb
The number of cylinders for this disk is set to 1024.
Command (m for help): n
Command action
  e   extended
  P   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1024, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-4462, default 1)
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1024, default 4462): using default
value 4462
```

```
Command (m for help):w

The partition table has been altered!
Calling ioctl () to re-read partition table.
Synching disks.
# exit
Last login Wed Feb 21 20:23:01 from localnode
$ sudo sh
Password:
# /sbin/partprobe /dev/sdb1
```

2.18 Configuring the oracle User's Environment

You run Oracle Universal Installer from the `oracle` account. However, before you start Oracle Universal Installer you must configure the environment of the `oracle` user. To configure the environment, you must:

- Set the default file mode creation mask (umask) to 022 in the shell startup file.
- Set the `DISPLAY` environment variable. (see Section 2.19)

> **Caution:** Use shell programs supported by your operating system vendor. If you use a shell program that is not supported by your operating system, then you can encounter errors during installation.

To set the `oracle` user's environment:

1. Start a new terminal session, for example, an X terminal (`xterm`).
2. Enter the following command to ensure that X Window applications can display on this system:

   ```
   $ xhost fully_qualified_remote_host_name
   ```

   For example:

   ```
   $ xhost somehost.us.example.com
   ```

3. If you are not already logged in to the system where you want to install the software, then log in to that system as the `oracle` user.
4. If you are not logged in as the `oracle` user, then switch user to `oracle`:

   ```
   $ su - oracle
   ```

5. To determine the default shell for the `oracle` user, enter the following command:

   ```
   $ echo $SHELL
   ```

6. To run the shell startup script, enter one of the following commands:
   - Bash shell:

     ```
     $ . ./.bash_profile
     ```

   - Bourne or Korn shell:

     ```
     $ . ./.profile
     ```

   - C shell:

```
% source ./.login
```

7. If you are not installing the software on the local computer, then run the following command on the remote machine to set the DISPLAY variable:

   - Bourne, Bash or Korn shell:

     ```
     $ export DISPLAY=local_host:0.0
     ```

   - C shell:

     ```
     % setenv DISPLAY local_host:0.0
     ```

   In this example, local_host is the host name or IP address of the local computer that you want to use to display Oracle Universal Installer.

   Run the following command on the remote machine to check if the shell and the DISPLAY environmental variable are set correctly:

   ```
   echo $SHELL
   echo $DISPLAY
   ```

   Now to enable X applications, run the following commands on the local computer:

   ```
   $ xhost + fully_qualified_remote_host_name
   ```

   To verify that X applications display is set properly, run a X11 based program that comes with the operating system such as xclock:

   ```
   $ xclock
   ```

   In this example, you can find xclock at /usr/X11R6/bin/xclocks. If the DISPLAY variable is set properly, then you can see xclock on your computer screen. If you receive any display errors, refer to the section "X Window Display Errors" the Troubleshooting chapter in *Oracle Database Installation Guide for Linux* for more information.

   See Also: PC-X Server or operating system vendor documents for further assistance

8. If you determined that the /tmp directory has less than 1 GB of free disk space, then identify a file system with at least 1 GB of free space and set the TMP and TMPDIR environment variables to specify a temporary directory on this file system:

   a. To determine the free disk space on each mounted file system use the following command:

   ```
   # df -h /tmp
   ```

   b. If necessary, enter commands similar to the following to create a temporary directory on the file system that you identified, and set the appropriate permissions on the directory:

   ```
   $ sudo mkdir /mount_point/tmp
   $ sudo chmod a+wr /mount_point/tmp
   # exit
   ```

   c. Enter commands similar to the following to set the TMP and TMPDIR environment variables:

   * Bourne, Bash, or Korn shell:

     ```
     $ TMP=/mount_point/tmp
     ```

```
$ TMPDIR=/mount_point/tmp
$ export TMP TMPDIR
```

* C shell:

```
% setenv TMP /mount_point/tmp
% setenv TMPDIR /mount_point/tmp
```

9. Enter commands similar to the following to set the `ORACLE_BASE` and `ORACLE_SID` environment variables:

   - Bourne, Bash, or Korn shell:

     ```
     $ ORACLE_BASE=/u01/app/oracle
     $ ORACLE_SID=sales
     $ export ORACLE_BASE ORACLE_SID
     ```

   - C shell:

     ```
     % setenv ORACLE_BASE /u01/app/oracle
     % setenv ORACLE_SID sales
     ```

   In this example, `/u01/app/oracle` is the Oracle base directory that you created or identified earlier and `sales` is the name that you want to call the database (typically no more than five characters).

10. Enter the following commands to ensure that the `ORACLE_HOME` and `TNS_ADMIN` environment variables are not set:

    - Bourne, Bash, or Korn shell:

      ```
      $ unset ORACLE_HOME
      $ unset TNS_ADMIN
      ```

    - C shell:

      ```
      % unsetenv ORACLE_HOME
      % unsetenv TNS_ADMIN
      ```

Note: If the `ORACLE_HOME` environment variable is set, then Oracle Universal Installer uses the value that it specifies as the default path for the Oracle home directory. However, if you set the `ORACLE_BASE` environment variable, then Oracle recommends that you unset the `ORACLE_HOME` environment variable and choose the default path suggested by Oracle Universal Installer.

See Also: Section 3.1.3 about configuring the user's environment

2.19 Setting the DISPLAY Environment Variable

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

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

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

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

2.20 Setting the Correct Locale

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

For example, for C shell:

```
unsetenv NLS_LANG
```

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

```
unset NLS_LANG
```

3

Oracle Grid Infrastructure

The Oracle Grid Infrastructure for a standalone server is the Oracle software that provides system support for an Oracle database including volume management, file system, and automatic restart capabilities. If you plan to use Oracle Restart or Oracle Automatic Storage Management (Oracle ASM), you must install Oracle Grid Infrastructure before installing Oracle Audit Vault Server. Oracle Grid Infrastructure for a standalone server is the software that includes Oracle Restart and Oracle ASM. Oracle combined the two infrastructure products into a single set of binaries that is installed as the Oracle Grid Infrastructure home. Oracle Grid Infrastructure should be installed before installing Oracle Audit Vault Server because Oracle Audit Vault Server installs a customized, specially configured release of Oracle Database 11*g* Release 2 (11.2.0.3).

Oracle ASM is a volume manager and a file system for Oracle database files that supports single-instance Oracle Audit Vault Server and Oracle Real Application Clusters (Oracle RAC) configurations. Oracle ASM also supports a general purpose file system for your application needs including Oracle Audit Vault Server binaries. Oracle ASM is Oracle's recommended storage management solution that provides an alternative to conventional volume managers, file systems, and raw devices.

Oracle Restart improves the availability of your Oracle database by providing the following:

- When there is a hardware or a software failure, Oracle Restart automatically starts all Oracle components, including Oracle database instance, Oracle Net Listener, database services, and Oracle ASM.
- Oracle Restart starts components in the proper order when the database host is restarted.
- Oracle Restart runs periodic checks to monitor the health of Oracle components. If a check operation fails for a component, then the component is shut down and restarted.

Note:

- If you want to use Oracle ASM or Oracle Restart, then you must first install Oracle Grid Infrastructure for a standalone server and then install Oracle Audit Vault Server.
- Oracle Restart is used in single-instance (non-clustered) environments only. See Section 1.6.3 for more information about how Oracle Audit Vault supports Oracle Restart.

This chapter contains the following sections:

3.1 Requirements for Oracle Grid Infrastructure Installation

The system must meet the following requirements:

3.1.1 Memory Requirements

The following are the memory requirements for installing Oracle Grid Infrastructure for a Standalone Server.

On Linux x86-64:

Minimum: At least 1.5 GB of RAM for Oracle Grid Infrastructure for a Standalone Server; at least 1 GB of additional RAM if you plan to install Oracle Audit Vault after installing Oracle Grid Infrastructure for a Standalone Server.

Recommended: 4 GB of RAM or more if you plan to install both Oracle Grid Infrastructure for a Standalone Server and Oracle Audit Vault Server.

- To determine the RAM size, enter the following command:

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

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

- The following table describes the relationship between installed RAM and the configured swap space requirement:

Note: On Linux, the HugePages feature allocates non-swappable memory for large page tables using memory-mapped files. If you enable HugePages, then you should deduct the memory allocated to HugePages from the available RAM before calculating swap space.

RAM	Swap Space
Between 1.5 GB and 2 GB	1.5 times the size of RAM
Between 2 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

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

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

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

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

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

```
# free
```

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

3.1.2 Disk Space Requirements

The following are the disk space requirements for installing Oracle Grid Infrastructure:

- At least 5.5 GB of disk space.
- At least 1 GB of space in the `/tmp` directory.

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

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

If there is less than 1 GB of free 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 to specify a temporary directory when setting the `oracle` user's environment.

  See Also: Section 2.18 for more information about setting `TMP` and `TMPDIR`

- Extend the file system that contains the `/tmp` directory. If necessary, contact the system administrator for information about extending file systems.

3.1.3 Configuring the User's Environment

Complete the following tasks to set the Oracle Grid Infrastructure software owner user's environment:

- Review the information in Section 2.1.
- Ensure that you set the path to the Oracle base directory. Oracle Restart and Oracle Audit Vault Server reside under the same Oracle base. For example:

```
# ORACLE_BASE=/u01/app/oracle;
# export ORACLE_BASE
```

- Set the Oracle Grid Infrastructure software owner user default file mode creation mask (`umask`) to 022 in the shell startup file. Setting the mask to 022 ensures that the user performing the software installation creates files with 755 permissions.
- Set `ulimit` settings for file descriptors and processes for the Oracle Grid Infrastructure installation software owner.
- Set the `DISPLAY` environment variable in preparation for installation.

If you plan to install Oracle Audit Vault Server, then you must meet additional preinstallation requirements. See Chapter 2.

3.2 Oracle ACFS and Oracle ADVM Support

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) extends Oracle ASM technology to support all of your application data in both single instance and cluster configurations. Oracle Automatic Storage Management Dynamic Volume Manager (Oracle ADVM) provides volume management services and a standard disk device driver interface to clients. Oracle Automatic Storage Management Cluster File System is layered on Oracle ASM through the Oracle Automatic Storage Management Dynamic Volume Manager interface.

Oracle Automatic Storage Management Cluster File System and Oracle Automatic Storage Management Dynamic Volume Manager are supported on Oracle Linux 5 and Red Hat Enterprise Linux 5 for Linux x86 and Linux x86-64. In the current release, it is also supported on SUSE Linux Enterprise Server 10 SP3 and later SUSE Linux Enterprise Server 10 Service Pack's for Linux x86-64 only.

Note: Oracle recommends that Oracle data files are installed in Oracle ASM disk groups. Installing Oracle data files on an Oracle ACFS file system is not supported. Oracle ACFS can be used as an option only when Oracle ASM is configured.

Automatic Storage Management Cluster File System (ACFS) resources are not supported for Oracle Restart configurations on all platforms. ACFS drivers must be manually unloaded and loaded; ACFS file systems must be manually unmounted and mounted (after the ASM instance is running); ACFS database home file systems can be placed into the ACFS mount registry to be mounted along with other registered ACFS file systems.

See Also:

- *Oracle Database Release Notes for Linux* for latest information about supported platforms and releases
- *Oracle Automatic Storage Management Administrator's Guide* for more information about Oracle Automatic Storage Management Cluster File System and Oracle Automatic Storage Management Dynamic Volume Manager

3.3 Managing Disk Groups for Older Database Versions

Releases prior to Oracle Audit Vault Server Release 10.3 used Database Configuration Assistant to perform administrative tasks on Oracle ASM. In the current release, Oracle ASM is installed with Oracle Restart.

3.4 Migrating Existing Oracle Automatic Storage Management Instances

If you have an Oracle ASM installation from a prior release installed on your server, or in an existing Oracle Grid Infrastructure installation, you can use Oracle Automatic Storage Management Configuration Assistant (Oracle ASMCA) to upgrade the existing Oracle ASM instance to 11*g* Release 2 (11.2), and subsequently configure disk groups, Oracle ASM volumes and Oracle ASM file systems.

Note: You must first shut down all databases and applications using an existing Oracle ASM instance before upgrading it.

During installation, if you chose to use Oracle ASM and Oracle ASMCA detects that there is a prior Oracle ASM version installed in another Oracle ASM home, then after installing the Oracle ASM 11*g* Release 2 (11.2) binaries, you can start Oracle ASMCA to upgrade the existing Oracle ASM instance.

See Also:

- "Upgrading an Oracle ASM Instance with Oracle ASM Configuration Assistant" in *Oracle Automatic Storage Management Administrator's Guide*
- "Upgrading an Oracle ASM Instance With Oracle Universal Installer" in *Oracle Automatic Storage Management Administrator's Guide*

3.5 Oracle Automatic Storage Management Installation Considerations

In previous releases, Oracle Automatic Storage Management (Oracle ASM) was installed as part of the Oracle Audit Vault Server installation. In the current release, Oracle ASM is part of an Oracle Grid Infrastructure installation, either for a cluster, or for a standalone server.

If you want to upgrade an existing Oracle ASM installation, then you must upgrade Oracle ASM by running an Oracle Grid Infrastructure upgrade (upgrades of existing Oracle ASM installations). If you do not have Oracle ASM installed and you want to use Oracle ASM as your storage option, then you must complete an Oracle Grid Infrastructure installation before you start your Oracle Audit Vault Server installation.

You must run Oracle Automatic Storage Management Configuration Assistant (Oracle ASMCA) for installing and configuring Oracle ASM instances, disk groups, volumes, and Oracle Automatic Storage Management Cluster File System (Oracle ACFS). In addition, you can use the ASMCA command-line interface as a non-GUI utility.

See Also: Chapter 11, "Oracle ASM Configuration Assistant" in *Oracle Automatic Storage Management Administrator's Guide* for information about Oracle ASMCA

Apply the following guidelines when you install Oracle ASM:

- You must complete the steps listed under Section 3.6 to prepare a disk partition to use for the Oracle ASM disk groups.
- Ensure that at least one disk is configured appropriately for use in an Oracle ASM diskgroup before beginning the installation.
- When you install Oracle ASM, Oracle Automatic Storage Management Configuration Assistant (Oracle ASMCA) creates a separate server parameter file (`SPFILE`) and password file for the Oracle ASM instance. As soon as Oracle ASM is installed, the `ASMSNMP` schema and user are created. See *Oracle Automatic Storage Management Administrator's Guide* for more information.
- The Oracle ASM instance that manages the existing disk group will be running in the Oracle Grid Infrastructure home directory.

3.6 Preparing Disks for an Oracle Automatic Storage Management Installation

This section describes how to configure disks for use with Oracle ASM. The following sections describe how to identify the requirements and configure the disks on each platform:

- General Steps for Configuring Oracle Automatic Storage Management
- Step 1: Identifying Storage Requirements for Oracle Automatic Storage Management
- Step 2: Creating DAS or SAN Disk Partitions for Oracle Automatic Storage Management
- Step 3: Configuring Disks for Oracle Automatic Storage Management

---

Note: Oracle does not recommend using identifiers for database object names that must be quoted. While these quoted identifiers may be valid as names in the `SQL CREATE` statement, such as `CREATE DISKGROUP "1data" ...`, the names may not be valid when using other tools that manage the database object.

See Also: "Creating Disk Groups for a New Oracle Installation", in *Oracle Automatic Storage Management Administrator's Guide* for information about creating and managing disk groups

3.6.1 General Steps for Configuring Oracle Automatic Storage Management

The following are the general steps to configure Oracle ASM:

1. Identify the storage requirements of the site.
2. If you are creating a new Oracle ASM disk group, create partitions for DAS or SAN disks.
3. Configure the disks for use with Oracle ASM. You must provide the Oracle ASM disk configuration information during the Oracle Grid Infrastructure installation.

3.6.2 Step 1: Identifying Storage Requirements for Oracle Automatic Storage Management

To identify the storage requirements for using Oracle ASM, you must determine the number of devices and the amount of free disk space that you require. To complete this task:

1. Determine if you want to use Oracle ASM for Oracle Audit Vault Server files, recovery files, or both.

   Note: You do not have to use the same storage mechanism for Oracle Vault Server files and recovery files. You can use a file system for one file type and Oracle ASM for the other.

   If you choose to enable automated backups and you do not have a shared file system available, then you must choose Oracle ASM for recovery file storage.

   During the database installation, if you plan to enable automated backups, then you can choose Oracle ASM as the storage mechanism for recovery files by specifying an Oracle ASM disk group for the fast recovery area. Depending on how you choose to create a database during the database installation, you have the following options:

   - You can run Oracle ASMCA in interactive mode to create and configure the required disk groups.

     During the database installation, if you select an installation method that runs Database Configuration Assistant in interactive mode (Advanced Installation type), then you can select the diskgroups that you created using Oracle ASMCA.

     You have the option to use the disk groups you created using Oracle ASMCA both for database files and recovery files, or you can choose to use different disk groups for each file type. Ideally, you should create separate Oracle ASM disk groups for data files and for recovery files.

   - If you run Oracle ASMCA in noninteractive mode, then you must use the same Oracle ASM disk group for data files and recovery files. During the database installation (Typical Installation type), you will have to select the same disk group for both data files and recovery files.

     See Also:

     - "Oracle ASM Configuration Assistant Command-Line Interface" section in *Oracle Automatic Storage Management Administrator's Guide*
     - Section 4.10.4 about creating fast recovery area disk group

2. Choose the Oracle ASM redundancy level that you want to use for each Oracle ASM disk group that you create.

   The redundancy level that you choose for the Oracle ASM disk group determines how Oracle ASM mirrors files in the disk group and determines the number of disks and amount of disk space that you require, as follows:

   - External redundancy

This option does not allow Oracle ASM to mirror the contents of the disk group. Oracle recommends that you select this redundancy level either when the disk group contains devices, such as RAID devices, that provide their own data protection or when the database does not require an uninterrupted access to data.

- Normal redundancy

  To optimize performance and reliability in a normal redundancy disk group, Oracle ASM uses two-way mirroring for data files and three-way mirroring for control files, by default. In addition, you can choose the mirroring characteristics for individual files in a disk group. Alternatively, you can use two-way mirroring or no mirroring.

  A normal redundancy disk group requires a minimum of two failure groups (or two disk devices) if you are using two-way mirroring. The effective disk space in a normal redundancy disk group is half the sum of the disk space in all of its devices.

  For most installations, Oracle recommends that you use normal redundancy disk groups.

- High redundancy

  The contents of the disk group are three-way mirrored by default. To create a disk group with high redundancy, you must specify at least three failure groups (a minimum of 3 devices).

  Although high-redundancy disk groups provide a high level of data protection, you must consider the higher cost of additional storage devices before deciding to use this redundancy level.

3. Determine the total amount of disk space that you require for the database files and recovery files.

   If an Oracle ASM instance is already running on the system, then you can use an existing disk group to meet these storage requirements. If necessary, you can add disks to an existing disk group during the database installation.

   Use the following table to determine the minimum number of disks and the minimum disk space requirements for the installation:

Redundancy Level	Minimum Number of Disks	Data Files	Recovery Files	Both File Types
External	1	1.8 GB	3.6 GB	5.4 GB
Normal	2	3.6 GB	7.2 GB	10.8 GB
High	3	5.4 GB	10.8 GB	16.2 GB

4. Optionally, identify failure groups for the Oracle ASM disk group devices.

   If you intend to use a normal or high redundancy disk group, then you can further protect the database against hardware failure by associating a set of disk devices in a custom failure group. By default, each device comprises its failure group. However, if two disk devices in a normal redundancy disk group are attached to the same SCSI controller, then the disk group becomes unavailable if the controller fails. The controller in this example is a single point of failure.

   For instance, to avoid failures of this type, you can use two SCSI controllers, each with two disks, and define a failure group for the disks attached to each controller.

This configuration would enable the disk group to tolerate the failure of one SCSI controller.

Note: If you define custom failure groups, then you must specify a minimum of two failure groups for normal redundancy disk groups and three failure groups for high redundancy disk groups.

5. If you are sure that a suitable disk group does not exist on the system, then install or identify appropriate disk devices to add to a new disk group. Apply the following guidelines when identifying appropriate disk devices:
   - The disk devices must be owned by the user performing the grid installation.

     See Also: Example 2–2 for information about creating or modifying permissions

   - All the devices in an Oracle ASM disk group should be the same size and have the same performance characteristics.
   - Do not specify multiple partitions on a single physical disk as a disk group device. Oracle ASM expects each disk group device to be on a separate physical disk.
   - Oracle does not recommend the use of a logical volume as a device in Oracle ASM because the logical volume can hide the physical disk architecture which prevents Oracle ASM from optimizing I/O across physical devices.

     See Also:

     - "Step 3: Configuring Disks for Oracle Automatic Storage Management" on page 3-9 for information about completing this task
     - "Preparing Storage for ASM" in *Oracle Automatic Storage Management Administrator's Guide* for information about configuring Oracle ASM disk groups

3.6.3 Step 2: Creating DAS or SAN Disk Partitions for Oracle Automatic Storage Management

In order to use a DAS or SAN disk in Oracle ASM, the disk must have a partition table. Oracle recommends creating exactly one partition for each disk containing the entire disk.

Note: You can use any physical disk for Oracle ASM, as long as it is partitioned.

3.6.4 Step 3: Configuring Disks for Oracle Automatic Storage Management

Oracle provides an Oracle ASM library driver that you can use to simplify the configuration and management of the disk devices that you want to use with Oracle ASM. A disk that is configured for Oracle ASM is known as a candidate disk.

If you intend to use Oracle ASM for database storage, then Oracle recommends that you install the Automatic Storage Management library driver (ASMLIB) and

associated utilities and use them to configure the devices that you want to include in an Oracle ASM disk group.

> **Note:** If you choose to configure disks using the Oracle Automatic Storage Management library driver, then you must change the default disk discovery string to `ORCLDISK:*`. If the diskstring is set to `ORCLDISK:*`, or is left empty (""), then the installer discovers these disks.

This section describes how to configure storage for use with Oracle ASM.

- Configuring Disks for Oracle Automatic Storage Management Using the Automatic Storage Management Library Driver (ASMLIB)
- Configuring Disk Devices Manually for Oracle Automatic Storage Management

3.6.4.1 Configuring Disks for Oracle Automatic Storage Management Using the Automatic Storage Management Library Driver (ASMLIB)

To use the Automatic Storage Management library driver to configure Automatic Storage Management devices, complete the following tasks:

- Installing and Configuring the Automatic Storage Management Library Driver Software
- Configuring the Disk Devices to Use the Automatic Storage Management Library Driver
- Administering the Automatic Storage Management Library Driver and Disks

Installing and Configuring the Automatic Storage Management Library Driver Software

To install and configure the Automatic Storage Management library driver software:

1. Enter the following command to determine the kernel version and architecture of the system:

   ```
   # uname -rm
   ```

2. If necessary, download the required Automatic Storage Management library driver packages from the Oracle Technology Network Web site:

   `http://www.oracle.com/technology/tech/linux/asmlib/index.html`

   You must install the following packages, where *version* is the version of the Automatic Storage Management library driver, *arch* is the system architecture, and *kernel* is the version of the kernel that you are using:

   ```
   oracleasm-support-version.arch.rpm
   oracleasm-kernel-version.arch.rpm
   oracleasmlib-version.arch.rpm
   ```

3. Enter a command similar to the following to install the packages:

   ```
   # sudo rpm -Uvh oracleasm-support-version.arch.rpm \
               oracleasm-kernel-version.arch.rpm \
               oracleasmlib-version.arch.rpm
   ```

   For example, if you are using the Red Hat Enterprise Linux AS 3.0 enterprise kernel on an x86 system, then enter a command similar to the following:

```
# sudo rpm -Uvh oracleasm-support-1.0.0-1.i386.rpm \
           oracleasm-2.4.9-e-enterprise-1.0.0-1.i686.rpm \
           oracleasmlib-1.0.0-1.i386.rpm
```

4. Enter a command similar to the following to determine the UID of the Oracle software owner user that you are using for this installation and the GID of the OSASM group:

   ```
   # id oracle
   ```

5. Enter the following command to run the `oracleasm` initialization script with the `configure` option:

   ```
   # /etc/init.d/oracleasm configure
   ```

6. Enter the following information in response to the prompts that the script displays:

Prompt	Suggested Response
Default UID to own the driver interface:	Specify the UID of the Oracle Grid Infrastructure owner user (typically, `grid`).
Default GID to own the driver interface:	Specify the GID of the OSASM group (typically, `asmadmin`).
Start Oracle Automatic Storage Management Library driver on start (y/n):	Enter `y` to start the Oracle Automatic Storage Management library driver when the system starts.
Scan for Oracle ASM disks on boot (y/n):	Enter `y` to scan for presence of any Oracle Automatic Storage Management disks when the system starts.

Configuring the Disk Devices to Use the Automatic Storage Management Library Driver

To configure the disk devices that you want to use in an Automatic Storage Management disk group:

1. If you intend to use IDE, SCSI, or RAID devices in the Automatic Storage Management disk group, then:

   a. If necessary, install or configure the disk devices that you intend to use for the disk group and restart the system.

   b. To identify the device name for the disks that you want to use, enter the following command:

      ```
      # /sbin/fdisk -l
      ```

      Depending on the type of disk, the device name can vary:

Disk Type	Device Name Format	Description
IDE disk	`/dev/hd`*`x`*`n`	In this example, *x* is a letter that identifies the IDE disk and *n* is the partition number. For example, `/dev/hda` is the first disk on the first IDE bus.

Disk Type	Device Name Format	Description
SCSI disk	/dev/sd*xn*	In this example, *x* is a letter that identifies the SCSI disk and *n* is the partition number. For example, /dev/sda is the first disk on the first SCSI bus.
RAID disk	/dev/rd/c*x*d*y*p*z* /dev/ida/c*x*d*y*p*z*	Depending on the RAID controller, RAID devices can have different device names. In the examples shown, *x* is a number that identifies the controller, *y* is a number that identifies the disk, and *z* is a number that identifies the partition. For example, /dev/ida/c0d1 is the second logical drive on the first controller.

Note: Oracle recommends that you create a single whole-disk partition on each disk that you want to use.

c. Use either `fdisk` or `parted` to create a single whole-disk partition on the disk devices that you want to use.

2. Enter a command similar to the following to mark a disk as an Automatic Storage Management disk:

```
# /etc/init.d/oracleasm createdisk DISK1 /dev/sdb1
```

In this example, `DISK1` is a name that you want to assign to the disk.

Note:

- If you are using a multipathing disk driver with Automatic Storage Management, then ensure that you specify the correct logical device name for the disk.

  The disk names that you specify can contain uppercase letters, numbers, and the underscore character. They must start with an uppercase letter.

- To create a database during the installation using the Automatic Storage Management library driver, you must change the default disk discovery string to `ORCLDISK:*`.

Administering the Automatic Storage Management Library Driver and Disks

To administer the Automatic Storage Management library driver and disks, use the `oracleasm` initialization script with different options, as follows:

Option	Description
`configure`	Use the `configure` option to reconfigure the Automatic Storage Management library driver, if necessary: `# /etc/init.d/oracleasm configure`

Option	Description
`enable` `disable`	Use the `disable` and `enable` options to change the behavior of the Automatic Storage Management library driver when the system starts. The `enable` option causes the Automatic Storage Management library driver to load when the system starts: `# /etc/init.d/oracleasm enable`

`start`
`stop`
`restart`
	Use the `start`, `stop`, and `restart` options to load or unload the Automatic Storage Management library driver without restarting the system:
	`# /etc/init.d/oracleasm restart`

`createdisk`	Use the `createdisk` option to mark a disk device for use with the Automatic Storage Management library driver and give it a name: `# /etc/init.d/oracleasm createdisk` *`DISKNAME devicename`*
`deletedisk`	Use the `deletedisk` option to unmark a named disk device: `# /etc/init.d/oracleasm deletedisk` *`DISKNAME`* **Note:** Do not use this command to unmark disks that are being used by an Automatic Storage Management disk group. You must drop the disk from the Automatic Storage Management disk group before you unmark it.
`querydisk`	Use the `querydisk` option to determine if a disk device or disk name is being used by the Automatic Storage Management library driver: `# /etc/init.d/oracleasm querydisk {`*`DISKNAME`* `|` *`devicename`*`}`
`listdisks`	Use the `listdisks` option to list the disk names of marked Automatic Storage Management library driver disks: `# /etc/init.d/oracleasm listdisks`
`scandisks`	Use the `scandisks` option to enable cluster nodes to identify which shared disks have been marked as Automatic Storage Management library driver disks on another node: `# /etc/init.d/oracleasm scandisks`

3.6.4.2 Configuring Disk Devices Manually for Oracle Automatic Storage Management

By default, the 2.6 kernel device file naming scheme `udev` dynamically creates device file names when the server is started, and assigns ownership of them to `root`. If `udev` applies default settings, then it changes device file names and owners for the disks, corrupting them when Oracle Storage Management instance is restarted. If you use ASMLIB, then you do not need to ensure permissions and device path persistency in udev.

If you do not use ASMLIB, then you must create a custom rules file. When `udev` is started, it sequentially carries out rules (configuration directives) defined in rules files. These files are in the path `/etc/udev/rules.d/`. Rules files are read in lexical order. For example, rules in the file `10-wacom.rules` are parsed and carried out before rules in the rules file `90-ib.rules`.

Where rules files describe the same devices, on Asianux, Red Hat, and Oracle Linux, the last file read is the one that is applied. On SUSE 2.6 kernels, the first file read is the one that is applied.

To configure a permissions file for disk devices, complete the following tasks:

1. Configure SCSI devices as trusted devices (white listed), by editing the `/etc/scsi_id.config` file and adding "options=-g" to the file. For example:

   ```
   # cat > /etc/scsi_id.config
   vendor="ATA",options=-p 0x80
   options=-g
   ```

2. Using a text editor, create a UDEV rules file for the Oracle ASM devices, setting permissions to 0660 for the installation owner and the group whose members are administrators of the grid infrastructure software. For example, using the installation owner `grid` and using a role-based group configuration, with the OSASM group `asmadmin`:

   ```
   # vi /etc/udev/rules.d/99-oracle-asmdevices.rules

   KERNEL=="sd?1", BUS=="scsi", PROGRAM=="/sbin/scsi_id",
   RESULT=="14f70656e66696c00000000", OWNER="grid", GROUP="asmadmin", MODE="0660"
   KERNEL=="sd?2", BUS=="scsi", PROGRAM=="/sbin/scsi_id",
   RESULT=="14f70656e66696c00000000", OWNER="grid", GROUP="asmadmin", MODE="0660"
   KERNEL=="sd?3", BUS=="scsi", PROGRAM=="/sbin/scsi_id",
   RESULT=="14f70656e66696c00000000", OWNER="grid", GROUP="asmadmin", MODE="0660"
   ```

3. Load updated block device partition tables on the server, using `/sbin/partprobe` *`devicename`*. You must do this as `root`.

4. Enter the command to restart the UDEV service.

   On Asianux, OEL5, and RHEL5, the commands are:

   ```
   # /sbin/udevcontrol reload_rules
   # /sbin/start_udev
   ```

   On SUSE 10 and 11, the command is:

   ```
   # /etc/init.d boot.udev restart
   ```

   Check to ensure that your system is configured correctly.

3.7 Installing Oracle Grid Infrastructure Using a Software-Only Installation

A software-only installation only copies the Oracle Grid Infrastructure for a Standalone Server binaries to the specified location. Configuring Oracle Grid Infrastructure for a standalone server and Oracle ASM must be done manually after the installation has finished.

When you perform a software-only installation of Oracle Grid Infrastructure software, you must complete a few manual configuration steps to enable Oracle Restart after you install the software.

Note: Oracle recommends that only advanced users perform the software-only installation, because this installation method provides no validation of the installation and this installation option requires manual postinstallation steps to enable the Oracle Grid Infrastructure software.

Performing a software-only installation involves the following steps:

1. Installing the Software Binaries
2. Configuring the Software Binaries

3.7.1 Installing the Software Binaries

1. Start the `runInstaller` command from the relevant directory on the Oracle Database 11*g* release 2 (11.2) installation media or download directory.
2. Complete a software-only installation of Oracle Grid Infrastructure.

   See Section 3.7.2 for information about configuring Oracle Grid Infrastructure after performing a software-only installation.
3. Verify that the server meets the installation requirements using the command `runcluvfy.bat stage -pre hacfg`. Ensure that you have completed all storage and server preinstallation requirements.

3.7.2 Configuring the Software Binaries

To configure and activate a software-only Oracle Grid Infrastructure installation for Oracle Restart, complete the following tasks:

1. Run the `roothas.pl` script from *`Grid_home`*, using the following syntax:

   ```
   Grid_home/perl/bin/perl -I Grid_home/perl/lib -I Grid_home/crs/install
   Grid_home/crs/install/roothas.pl
   ```

   For example, if your Grid home is `/app/11.2.0/grid`, then run the following script:

   ```
   $ /app/11.2.0/grid/perl/bin/perl -I /app/11.2.0/grid/perl/lib -I /app
   /11.2.0/grid/crs/install /app/11.2.0/grid/crs/install/roothas.pl
   ```
2. Change the directory to *`Grid_home`*`/oui/bin`, where *`Grid_home`* is the path of the Oracle Grid Infrastructure home.
3. Enter the following command:

   ```
   ./runInstaller -updateNodeList ORACLE_HOME=Grid_home -defaultHomeName
   ```

   For example:

   ```
   $ ./runInstaller -updateNodeList ORACLE_HOME=/u01/app/11.2.0/grid
   -defaultHomeName
   CLUSTER_NODES= CRS=TRUE
   ```
4. Use the `SRVCTL` utility along with Network Configuration Assistant and Oracle ASMCA to add the listener, the Oracle ASM instance, and all Oracle ASM disk groups to the Oracle Restart configuration.

3.8 Installing and Configuring Oracle Grid Infrastructure for a Standalone Server

If you install Oracle Grid Infrastructure and then create your database, the database is automatically added to the Oracle Grid Infrastructure configuration, and is then automatically restarted when required. However, if you install Oracle Grid Infrastructure on a host computer on which a database already exists, you must manually add the database, the listener, the Oracle ASM instance, and other components to the Oracle Grid Infrastructure configuration.

Note: Oracle Grid Infrastructure can accommodate multiple single-instance databases on a single host computer.

This section includes the following topics:

- Installing Oracle Grid Infrastructure with a New Database Installation
- Installing Oracle Grid Infrastructure for an Existing Database

3.8.1 Installing Oracle Grid Infrastructure with a New Database Installation

Perform the following steps to install Oracle Grid Infrastructure and then create a database that is managed by Oracle Restart. First install Oracle Grid Infrastructure, which installs Oracle Restart and Oracle ASM, then configure Oracle ASM with at least one disk group, and then install Oracle Audit Vault Server that stores database files in Oracle ASM disk groups. Click the help button on the Oracle Universal Installer page for page level assistance.

You may need to shut down existing Oracle processes before you proceed with the Oracle Grid Infrastructure installation. Refer to *Oracle Database Installation Guide for Linux* for more information.

To install Oracle Grid Infrastructure for a standalone server with a new database installation:

1. Start Oracle Universal Installer as the Oracle Grid Infrastructure software owner user. Complete one of the following steps depending on the location of the installation files:

   - If the installation files are on installation media, enter commands similar to the following, where *directory_path* is the path of the Oracle Grid Infrastructure directory on the installation media:

     ```
     $ /directory_path/runInstaller
     ```

     Note: You must install Oracle Grid Infrastructure for a standalone server from the Oracle Grid Infrastructure media.

   - If the installation files are on the hard disk, change the directory to the path of the Oracle Grid Infrastructure (`clusterware`) directory and enter the following command:

     ```
     $ ./runInstaller
     ```

   - **Downloading Updates Before Installation**

Starting with Oracle Database 11*g* Release 2 (11.2.0.2), if you plan to run the installation in a secured data center, then you can download updates before starting the installation by starting Oracle Universal Installer on a system that has Internet access in update download mode. To start Oracle Universal Installer to download updates, enter the following command:

```
$ ./runInstaller -downloadUpdates
```

Provide the My Oracle Support user name and password, and provide proxy settings if needed. After you download updates, transfer the update file to a directory on the server where you plan to run the installation.

See Also:

- *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX* for more information about response file formats
- Section 3.1.3 for information about setting the Oracle Grid Infrastructure software owner user's environment

---

Note: Start Oracle Universal Installer from the terminal session where you logged in as the Oracle Grid Infrastructure software owner user and set the user's environment.

If Oracle Universal Installer is not displayed, refer to the sections "X Window Display Errors" and "Remote Terminal Installation Error" in the Troubleshooting appendix in *Oracle Database Installation Guide for Linux* for information about troubleshooting.

2. Starting with Oracle Database 11*g* Release 2 (11.2.0.2), you can use the Software Updates feature to dynamically download and apply latest updates. In the Download Software Updates screen, select one of the following options and click **Next:**

   - Use My Oracle Support credentials for download: Select this option to download and apply the latest software updates.

     Click **Proxy Settings** to configure a proxy for Oracle Universal Installer to use to connect to the Internet. Provide the proxy server information for your site, along with a user account that has access to the local area network through which the server is connecting.

     Click **Test Connection** to ensure that your proxy settings are correctly entered, and the installer can download the updates.

   - Use pre-downloaded software updates: Select this option to apply the software updates previously downloaded using the `-downloadUpdates` flag.
   - Skip Software Updates: Select this option if you do not want to apply any updates.

3. The Apply Software Updates screen is displayed if you select to download the software updates or provide the pre-downloaded software updates location. If you selected Use My Oracle Support credentials for download in the previous screen, then select **Download and apply all updates**, and click **Next.**

   If you selected Use pre-downloaded software updates in the previous screen, then select **Apply all updates**, and click **Next.**

4. In the Select Installation Option screen, select the **Install and Configure Grid Infrastructure for a Standalone Server** option to install and configure Oracle Restart and Oracle ASM. Click **Next.**
5. In the Select Product Languages screen, select one or more languages. Move the languages from the Available Languages list to the Selected Languages list. Click **Next.**
6. The Create ASM Disk Group screen lists all the Oracle ASM disks under `ORCLDISK:*`

   Click **Change Disk Discovery Path** to select any devices that will be used by Oracle ASM but are not listed. In the Change Disk Discovery Path window, enter a string to use to search for devices that Oracle ASM will use. If the diskstring is set to `ORCLDISK:*` or is left empty (""), then the installer discovers these disks. Click **OK.**

   After you finish selecting the disks to be used by Oracle ASM, click **Next**.

   Note: During installation, disk paths mounted on ASM and registered on ASMLIB with the string `ORCLDISK:*` are listed as default database storage candidate disks.

   Consider the following information about disk devices while performing this step:

   - The Disk Group Name default is `DATA`. You can enter a new name for the disk group, or use the default name.
   - The disk devices must be owned by the user performing the grid installation.

     See Also: Example 2–2 for information about creating or modifying permissions

   - Check with your system administrator to determine if the disks used by Oracle ASM are mirrored at the storage level. If so, select External for the redundancy. If the disks are not mirrored at the storage level, then choose Normal for the redundancy.

     Note: For normal redundancy, you require twice as much disk space to hold the same amount of data. For example, if your database is 100 GB, then you require approximately 200 GB of storage.

     ---

7. In the Specify ASM Password screen, enter `SYSASM` password required to connect to the Oracle ASM instance. The Oracle ASM instance is managed by a privileged role called `SYSASM`, which grants full access to Oracle ASM disk groups. Oracle recommends that you create a less privileged user, `ASMSNMP`, with `SYSDBA` privileges to monitor the Oracle ASM instance.

   Enter passwords for the `SYS` and `ASMSNMP` user accounts. The passwords should be at least eight characters in length and include at least one alphabetic and one numeric character.

   Optionally, you can use the same password for all accounts. However, Oracle recommends that you specify a different password for each account. You must remember the passwords that you specify.

8. In the Privileged Operating System Groups screen, select the name of the operating system group you created for the `OSDBA` group, the `OSASM` group, and the database operator group `OSOPER`. If you choose to create only the `dba` group, then you can use that group for all three privileged groups. If you created a separate `asmadmin` group, then use that value for the `OSASM` group. Click **Next**.
9. In the Specify Installation Location screen, enter the following details, and click **Next:**
   - **Oracle Base**: Enter the directory location for Oracle base. Do not include spaces in the path name.
   - **Software Location:** This field is populated by default in concurrence with Oracle base location.

     See Also: "Naming Directories" section in the Optimal Flexible Architecture appendix in *Oracle Database Installation Guide for Linux* for directory naming conventions
10. If you have not installed any Oracle software previously on this server, the Create Inventory screen appears.

    Change the path for the Inventory Directory, if required. Select `oinstall` for the oraInventory Group Name, if required. Click **Next.**
11. The Perform Prerequisite Checks screen checks if the minimum system requirements are met to perform the Oracle Grid Infrastructure installation. If all the system requirements are met, then you will be directed to the Summary screen. However, if an installation fails, you can review the error.

    If you click **Check Again**, then you can run the prerequisite check again to see if the minimum requirements are met to carry on with the database installation.

    Click **Fix & Check Again**, if you want the installer to fix the problem and check the system requirements once more.

    Note: The Fix & Check Again option generates a script that you must run as the `root` user. This generated script sets some of the system parameter values. Oracle recommends that you do not modify the contents of this script. Refer to Section 2.4 for more information about fixup scripts.

    To get a list of failed requirements, select **Show Failed** from the list. To get a list of all the prerequirement checks run by the OUI, select **Show All**. To get a list of the prerequirement checks that are successful, select **Show Succeeded.**

    Note: Oracle recommends that you use caution in checking the Ignore All option. If you check this option, then Oracle Universal Installer may not confirm that your system is able to install Oracle Audit Vault Server successfully.
12. Review the contents of the Summary screen, and click **Finish.**

    Starting with Oracle Database 11*g* Release 2 (11.2), you can click **Save Response File** to save all the installation steps into a response file. This file can be used for a silent installation.

13. The Setup screen displays the progress of the Oracle Grid Infrastructure installation. During the installation process, the Execute Configuration Scripts window appears. Do *not* click **OK** until you have run the scripts mentioned in this screen.

    Run the `root.sh` and, if required, the `orainstRoot.sh` configuration scripts as the `root` user.

14. The Finish screen displays the installation status. Click **Close** to end the installation, then **Yes** to confirm that you want to exit Oracle Universal Installer.

    If you encounter any problems, refer to the configuration log for information. The path to the configuration log is displayed on the Configuration Assistants window.

15. To create additional disk groups, run the Oracle ASMCA utility. For example, you can create another disk group named `RECOVERY` to store the fast recovery area.

    See Also:

    - "Manually Configuring Oracle Automatic Storage Management Disk Groups" on page 3-21
    - Section 4.10.4 about creating a fast recovery area disk group

    Note: To check if the Oracle High Availability Service is installed properly, run `./crsctl check has` command from *`Grid_home`*`/bin` directory.

    `Grid_home` is the path to the Oracle Grid Infrastructure home for a standalone server. `Ohasd` is a daemon installed with Oracle Grid Infrastructure that starts software services, such as Oracle ASM.

16. Install Oracle Audit Vault Server. Refer to Section 4.3 and Section 4.5 for information about installing Oracle Audit Vault Server.

    Note:

    - If a new database is installed after a grid infrastructure installation, then the listener runs from the Oracle Grid Infrastructure home. Because Oracle ASM is installed as part of Oracle Grid Infrastructure, the default listener is created and runs from the Oracle Grid Infrastructure home. If you perform a database installation, then the database must use the same listener created during the Oracle Grid Infrastructure installation.
    - If you are using Oracle Restart, then the default listener and any additional listeners must run from the Oracle Grid Infrastructure home.

3.8.2 Installing Oracle Grid Infrastructure for an Existing Database

Follow the high-level instructions in this section to install Oracle Grid Infrastructure and configure it for an existing Oracle database. Please note that Oracle Restart can only manage existing 11.2 resources and hence you can install Oracle Grid Infrastructure only for an existing 11.2 database. However, Oracle database releases prior to 11.2 can coexist on the same server without being managed by Oracle Restart.

To install Oracle Grid Infrastructure for an existing database:

- On the same host computer as the database, use Oracle Universal Installer to install Oracle Grid Infrastructure, and select **Install and Configure Grid Infrastructure for a Standalone Server** as the installation option.

  The Oracle Grid Infrastructure components are installed in a separate Oracle home.

  Refer to Section 3.8.1 for detailed instructions to install Oracle Grid Infrastructure.

- Go to the Grid home's `bin` directory. Use the `srvctl add database` command to manually add the database, the listener, the Oracle ASM instance, all Oracle ASM disk groups, and any database services to the Oracle Grid Infrastructure configuration.

  See Also: "srvctl add database" in *Oracle Database Administrator's Guide* for more information about the `srvctl add database` command

3.9 Modifying Oracle Grid Infrastructure Binaries After Installation

After installation, you must first stop the Oracle Restart stack to modify the software installed in your Grid home. For example, if you want to apply a one-off patch or modify any of the DLLs used by Oracle Restart or Oracle ASM, then you must follow these steps to stop and restart the Oracle Restart stack.

Caution: Before relinking executables, you must shut down all executables that run in the Oracle home directory that you are relinking. In addition, shut down applications linked with Oracle shared libraries.

Prepare the Oracle Grid Infrastructure home for modification using the following procedure:

1. Log in as the Oracle Grid Infrastructure software owner user and change the directory to the path *Grid_home*\bin, where *Grid_home* is the path to the Oracle Grid Infrastructure home:

   ```
   $ cd Grid_home/bin
   ```

2. Shut down the Oracle Restart stack using the following command:

   ```
   $ crsctl stop has -f
   ```

3. After the Oracle Restart stack is completely shut down, perform the updates to the software installed in the Grid home.

4. Use the following command to restart the Oracle Restart stack:

   ```
   $ crsctl start has
   ```

3.10 Manually Configuring Oracle Automatic Storage Management Disk Groups

The Oracle Automatic Storage Management Configuration Assistant utility creates a new Automatic Storage Management instance if there is no Oracle ASM instance currently configured on the computer.

After installing Oracle Grid Infrastructure, you can also use Oracle ASMCA to create and configure disk groups, Oracle Automatic Storage Management Dynamic Volume Manager (Oracle ADVM) and Oracle Automatic Storage Management Cluster File System (Oracle ACFS).

If you want to create additional disk groups or manually configure Oracle ASM disks, then you can run the Oracle ASMCA as follows:

```
$ cd Grid_home/bin
$ ./asmca
```

Where *Grid_home* is the path to the Oracle Grid Infrastructure home for a standalone server.

> **See Also:** *Oracle Automatic Storage Management Administrator's Guide* for more information on Oracle ASMCA

3.11 Testing the Oracle Automatic Storage Management Installation

To test the Oracle ASM installation, try logging in by using the `asmcmd` command-line utility, which lets you manage Oracle ASM disk group files and directories. To do this:

1. Open a shell window, and temporarily set the `ORACLE_SID` and `ORACLE_HOME` environment variables to specify the appropriate values for the Oracle ASM instance that you want to use.

   For example, if the Oracle ASM `SID` is named `+ASM` and the Oracle home is located in the `grid` subdirectory of the `ORACLE_BASE` directory, then enter the following commands to create the required settings:

   - Bourne, Bash, or Korn shell:

     ```
     $ ORACLE_SID=+ASM
     $ export ORACLE_SID
     $ ORACLE_HOME=/u01/app/oracle/product/11.2.0/grid
     $ export ORACLE_HOME
     ```

   - C shell:

     ```
     % setenv ORACLE_SID +ASM
     % setenv ORACLE_HOME /u01/app/oracle/product/11.2.0/grid
     ```

2. Use ASMCMD to list the disk groups for the Oracle ASM instance:

   ```
   $ORACLE_HOME/bin/asmcmd lsdg
   ```

   ASMCMD connects by default as the SYS user with SYSASM privileges.

   If the Oracle ASM instance is not running, you can start the instance with the following:

   ```
   $ORACLE_HOME/bin/asmcmd startup
   ```

   See Also:

   - *Oracle Database Utilities* for more information about ASMCMD
   - *Oracle Automatic Storage Management Administrator's Guide* for a more information about Oracle ASM

4

Installing the Oracle Audit Vault Server

This chapter includes an overview of the major steps required to install single instance Oracle Audit Vault Server (Audit Vault Server) and to install Audit Vault Server with Oracle Real Application Clusters (Oracle RAC). In each case, Oracle Audit Vault Server installs a customized, specially configured release of Oracle Database 11*g* Release 2 (11.2.0.3.0)

This chapter includes the following sections:

4.1 Reviewing Component-Specific Installation Guidelines

Review the following guidelines before starting Oracle Universal Installer:

- Oracle Universal Installer

  Using Oracle Universal Installer from an earlier Oracle release to install components from this release is no longer allowed.

- Oracle Automatic Storage Management

  In previous releases, Oracle Automatic Storage Management (Oracle ASM) was installed as part of the Oracle Audit Vault Server installation. With Oracle Audit Vault Release 10.3, Oracle ASM is part of an Oracle Grid Infrastructure installation, either for a cluster, or for a standalone server.

  If you want to upgrade an existing Oracle ASM installation, then you must upgrade Oracle ASM by running an Oracle Grid Infrastructure upgrade. If you do not have Oracle ASM installed and you want to use Oracle ASM as your storage option, then you must complete an Oracle Grid Infrastructure installation before you start your Oracle Audit Vault Server installation.

See Also: Chapter 3 for information about Oracle Grid Infrastructure for a standalone server

- Installations on a Cluster

  If Oracle Clusterware and Oracle RAC are already installed on the system, Oracle Universal Installer displays the Specify Hardware Cluster Installation page. You must select the Local Installation option, unless you want to install Oracle RAC.

  See Also: *Oracle Real Application Clusters Installation Guide* for information about installing Oracle RAC

4.1.1 Using an Oracle Automatic Storage Management Disk Group

This section is optional and describes how to identify disk groups and determine the free disk space that they contain. You can store either database or recovery files in an existing Oracle ASM disk group that you created during the Oracle Grid Infrastructure installation.

Note: The Oracle ASM instance that manages the existing disk group will be running in the Oracle Grid Infrastructure home directory.

To determine if an existing Oracle ASM disk group exists, or to determine if there is sufficient disk space in a disk group, use the following procedure:

1. View the contents of the `oratab` file to determine if an Oracle ASM instance is configured on the system:

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

   If an Oracle ASM instance is configured on the system, then the `oratab` file should contain a line similar to the following:

   ```
   +ASM:oracle_home_path:N
   ```

   In this example, `+ASM` is the system identifier (`SID`) of the Oracle ASM instance and *`oracle_home_path`* is the Oracle home directory where Oracle ASM is installed. By convention, the `SID` for an Oracle ASM instance should be `+ASM`.

2. Open a shell prompt and temporarily set the `ORACLE_SID` and `ORACLE_HOME` environment variables to specify the appropriate values for the Oracle ASM instance that you want to use.

   For example, if the Oracle ASM `SID` is named `+ASM` and is located in the `grid` subdirectory of the `ORACLE_BASE` directory, then enter the following commands to create the required settings:

   - Bourne, Bash, or Korn shell:

     ```
     $ ORACLE_SID=+ASM
     $ export ORACLE_SID
     $ ORACLE_HOME=/u01/app/oracle/product/11.2.0/grid/
     $ export ORACLE_HOME
     ```

   - C shell:

     ```
     % setenv ORACLE_SID +ASM
     % setenv ORACLE_HOME /u01/app/oracle/product/11.2.0/grid
     ```

3. By using SQL*Plus, connect to the Oracle ASM instance as the `SYS` user with `SYSASM` privilege and start the instance if necessary:

```
# $ORACLE_HOME/bin/sqlplus /nolog
SQL> CONNECT SYS as SYSASM
Enter password: SYS_password
SQL> STARTUP
```

4. Enter the following command to view the existing disk groups, their redundancy level, and the amount of free disk space in each one:

```
SQL> SELECT NAME,TYPE,TOTAL_MB,FREE_MB FROM V$ASM_DISKGROUP;
```

5. From the output, identify a disk group with the appropriate redundancy level and note the free space that it contains.
6. If necessary, install or identify the additional disk devices required to meet the storage requirements listed in the previous section.

Note: If you are adding devices to an existing disk group, then Oracle recommends that you use devices that have the same size and performance characteristics as the existing devices in that disk group.

See Also: Section 3.4, "Migrating Existing Oracle Automatic Storage Management Instances"

4.2 Accessing the Server Installation Software

The Oracle Audit Vault Server software is available:

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

4.3 Basic Installation – Performing the Single Instance Server Installation

For an overview of requested information specific to the Audit Vault Server installation, see Section 4.8.

See Section 2.20 for important information about setting the correct locale.

To perform Audit Vault Server single instance basic installation:

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

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

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

   Oracle Universal Installer starts up and launches itself.

   If you need assistance at any time during installation, click **Help**.

If you encounter problems during installation, 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`

2. The following table lists the various screens displayed and the options to select during an Oracle Audit Vault Server Basic Installation:

Screen	Action
Configure Security Updates	Enter your e-mail address, preferably your My Oracle Support (formerly Oracle*MetaLink*) e-mail address or user name in the **Email** field. Select the **I wish to receive security updates via My Oracle Support** check box if you want to receive security updates. Enter your My Oracle Support password in the **My Oracle Support Password** field. Click **Next**.
Select Installation Option	Select **Create and configure Oracle Audit Vault**, and click **Next** This option installs and configures Oracle Audit Vault Server.
Select Install Type	Select **Basic install**, and click **Next:** This installation method is selected by default. It lets you quickly install Oracle Audit Vault Server with standard configuration options requiring minimal input.

Screen	Action
Basic Install Configuration	Specify information for the following fields: ■ **Oracle Base** The Oracle base directory is a top-level directory for Oracle software installations owned by an Oracle installation owner account. The default Oracle base path is *mountpoint/app/user*, where *user* is the user account running the installation. You can change the path based on your requirements. ■ **Software Location** Either accept the default value or enter or browse to the Oracle home directory path in which you want to install Oracle Audit Vault Server. The directory path should not contain spaces. Ensure that the Oracle home path for the Oracle Audit Vault Server home and the Oracle base path use only ASCII characters. At the time of this release, the use of non-ASCII characters for a Oracle Audit Vault Server home or Oracle base is not supported. ■ **Audit Vault SID** Specify a unique Database Service ID (SID) for the Oracle Audit Vault Server installation. The Oracle Audit Vault SID is required. The SID will be used as the database SID, and will be the first portion (*db_name*) of the database service name. ■ **Audit Vault Admin** The account name of the Oracle Audit Vault Administrator. The Oracle Audit Vault Administrator account name is required. The Oracle Audit Vault Administrator user name will also be used for the following Oracle Database Vault users that are created to facilitate the separation of duties: *AV_ADMIN*dvo – The Database Vault Owner (granted DV_OWNER role) to manage Database Vault roles and configuration, where *AV_ADMIN* represents the Oracle Audit Vault Administrator user name. *AV_ADMIN*dva – The Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts, where *AV_ADMIN* represents the Oracle Audit Vault administrator user name. ■ **Password** The password for the Oracle Audit Vault administrator account. The password entered will also be used for the standard database accounts (sys, system, sysman, dbsnmp). The password will also be used for the Oracle Database Vault users (Database Vault Owner and the Database Vault Account Manager users) that are created to facilitate the separation of duties. ■ **Confirm Password** The confirming password for the Oracle Audit Vault Administrator account.

Screen	Action
Basic Install Configuration **(Continued)**	Specify information for the following fields, and click **Next.** ■ **Create a Separate Audit Vault Auditor** Accept the selected default check box to choose to create the Oracle Audit Vault Auditor account name to have a separation of duties between the Oracle Audit Vault Administrator and Auditor. Deselecting the check box disables the text fields for the Oracle Audit Vault Auditor user name and password. The Oracle Audit Vault Administrator in this case will be granted the role of Oracle Audit Vault Auditor and assume these duties. ■ **Audit Vault Auditor** The account name of the Oracle Audit Vault Auditor. ■ **Password** The password for the Oracle Audit Vault auditor account. ■ **Confirm Password** The confirming password for the Oracle Audit Vault Auditor account.
Create Inventory	You are prompted by the installer to specify the **Inventory Directory** path for the central inventory the first time you install any Oracle software on your computer. Select the **oraInventory Group Name** of the operating system group that should own the Oracle Inventory directory (the Oracle Inventory group). Click **Next.** **Note:** By default, the Oracle Inventory directory is not installed under the Oracle Base directory. This is because all Oracle software installations share a common Oracle Inventory, so there is only one Oracle Inventory for all users, whereas there is a separate Oracle Base for each user.
Perform Prerequisite Checks	This option checks the system to verify that it is configured correctly and the minimum requirements are met to perform the Oracle Audit Vault Server installation. If you have completed all of the preinstallation steps in this guide, all of the checks should pass. If you click **Check Again,** then you can run the prerequisite check again to see if the minimum requirements are met to carry on with the database installation. Click **Fix & Check Again,** if you want the installer to fix the problem and check the system requirements once more. **Note**: The Fix & Check Again option generates a script that you need to run as the `root` user. This generated script sets some of the system parameters to Oracle-recommended values. Oracle recommends that you do not modify the contents of this script. Refer to Section 2.4 for more information about fixup scripts. To get a list of failed requirements, select **ShowFailed** from the list. To get a list of all the prerequirement checks run by the OUI, select **Show All**. To get a list of the prerequirement checks that are successful, select **Show Succeeded.** **Note**: Oracle recommends that you use caution in checking the Ignore All option. If you check this option, then Oracle Universal Installer may not confirm that your system is able to install Oracle Audit Vault Server successfully. **See Also**: Chapter 2 for information about the system requirements
Summary	Review the information displayed on this screen, and click **Install.** Note: Starting with Oracle Audit Vault Server Release 10.3, you can save all the installation steps into a response file by clicking **Save Response File.** Later, this file can be used for a silent installation. See Section 4.7 and Appendix A for more information.

Screen	Action
Install product	This screen states the progress of an Oracle Audit Vault Server installation. After Oracle Audit Vault Server is installed, you are prompted to execute a root configuration script for new inventory as the `root` user. This screen displays the status information for the configuration assistants that configure the Oracle Audit Vault Server. Finally, a message is displayed at the end of Audit Vault Configuration Assistant process. Click **Next.** Follow the steps as indicated on the **Execute Configuration scripts** screen to run the `root.sh`, and, if required, the `orainstRoot.sh` configuration scripts as the `root` user. After running the scripts, click **OK** on the **Execute Configuration scripts** screen to continue.
Finish	This screen is shown automatically when all the configuration tools are successful. Review the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL information displayed in this screen and click **Close.** On the **Exit** page, click **Exit**. Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

Caution: After installation is complete, do not manually remove, or run `cron` jobs that remove `/tmp/.oracle` or `/var/tmp/.oracle` directories or their files while Oracle software is running. If you remove these files, then Oracle software can encounter intermittent hangs. Oracle Restart installations will fail with the following error:

```
CRS-0184: Cannot communicate with the CRS daemon.
```

See Section 4.9.6 for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

After you have completed the installation, proceed to Section 4.9 to perform the postinstallation tasks.

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

This section assumes that you performed the initial installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC). These initial installation procedures are described in *Oracle Real Application Clusters Installation Guide for Linux and UNIX*. These tasks include preinstallation tasks, configuring Oracle Audit Vault Server storage, installing Oracle Grid Infrastructure for a cluster, which includes Oracle Clusterware and Oracle Automatic Storage Management (system and storage administration), and installing Oracle RAC (database administration). 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 "Verifying System Readiness for Installing Oracle Database with CVU " in *Oracle Real Application Clusters Installation Guide for Linux and UNIX* for more information.

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

4.5 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.

> **Note:** Oracle ASM Release 11.2.0.3 requires Oracle Clusterware Release 11.2.0.3. Oracle Audit Vault 10.3 requires Cluster Ready Services (CRS) 11.2.0.3, which installs with Oracle Clusterware Release 11.2.0.3.

See Section 2.20 for important information about setting the correct locale.

Perform the following procedures to install Oracle Audit Vault.

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

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

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

   Oracle Universal Installer starts up and launches itself.

   If you need assistance at any time during installation, click **Help**.

   If you encounter problems during installation, 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/installActionsdate_time.log
   ```

2. The following table lists the various screens displayed and the options to select during an Oracle Audit Vault Server Basic Installation:

Screen	Action
Configure Security Updates	Enter your e-mail address, preferably your My Oracle Support (formerly Oracle*MetaLink*) e-mail address or user name in the **Email** field. Select the **I wish to receive security updates via My Oracle Support** check box if you want to receive security updates. Enter your My Oracle Support password in the **My Oracle Support Password** field. Click **Next**.
Select Installation Option	Select **Create and configure Oracle Audit Vault**, and click **Next** This option installs and configures Oracle Audit Vault Server.

Screen	Action
Select Install Type	Select **Advanced install**, and click **Next:** This installation method offers you more controls and options for the full Oracle Audit Vault Server installation along with more install screens.
Grid Installation Options	Select the type of Audit Vault installation you want to perform, and click **Next.** ▪ Single instance Audit Vault installation: This option installs a single instance of Oracle Audit Vault Server. ▪ Oracle Real Application Clusters database installation: This option installs Oracle Audit Vault Server in an Oracle Real Application Clusters (Oracle RAC) environment. When you select Oracle Real Application Clusters database installation, you must make node selections. If you are installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), the **Node Selection** screen appears from which to select the nodes on which Oracle Audit Vault will be installed. Local node will always be selected by default. If you are installing Oracle Audit Vault single instance on this local node only, select the **Local Only Installation** option, then click **Next**. If you are installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), select the nodes on which Oracle Audit Vault must be installed. Oracle recommends to install software on all the cluster nodes instead of a subset of nodes. After selecting these nodes, click **Next**. See Section 4.8.2 for more information about node selection.
Select Product Languages	This option enables you to select the language in which you want to run the product. Select the product Language from the Available Languages list, transfer it to the Selected Languages list. Click **Next.**
Specify Installation Location	Specify **Oracle Base**, **Software Location**, and click **Next.** The Oracle base directory is a top-level directory for Oracle software installations owned by an Oracle installation owner account. The default Oracle base path is `mountpoint/app/user`, where *user* is the user account running the installation. You can change the path based on your requirements. In the Software Location field, accept the default value or enter or browse to the Oracle home directory path in which you want to install Oracle Audit Vault Server. The directory path should not contain spaces. Click **Next.** Ensure that the Oracle home path for the Oracle Audit Vault Server home and the Oracle base path use only ASCII characters. At the time of this release, the use of non-ASCII characters for a Oracle Audit Vault Server home or Oracle base is not supported.
Create Inventory	You are prompted by the installer to specify the **Inventory Directory** path for the central inventory the first time you install any Oracle software on your computer. Select the **oraInventory Group Name** of the operating system group that should own the Oracle Inventory directory (the Oracle Inventory group). Click **Next.** **Note:** By default, the Oracle Inventory directory is not installed under the Oracle Base directory. This is because all Oracle software installations share a common Oracle Inventory, so there is only one Oracle Inventory for all users, whereas there is a separate Oracle Base for each user.

Screen	Action
Specify Audit Vault Details	Specify information for the following fields and click **Next**: See Section 4.8 for more information about each of these topics. ■ **Audit Vault Admin** The account name of the Oracle Audit Vault Administrator. The Oracle Audit Vault Administrator account name is required. ■ **Password** The password for the Oracle Audit Vault administrator account. ■ **Confirm Password** The confirming password for the Oracle Audit Vault Administrator account. ■ **Create a Separate Audit Vault Auditor** Accept the selected default check box to choose to create the Oracle Audit Vault Auditor account name to have a separation of duties between the Oracle Audit Vault Administrator and Oracle Auditor. Deselecting the check box disables the text fields for the Oracle Audit Vault Auditor user name and password. The Oracle Audit Vault Administrator in this case will be granted the role of Oracle Audit Vault Auditor and assume these duties. ■ **Audit Vault Auditor** The account name of the Oracle Audit Vault Auditor. ■ **Password** The password for the Oracle Audit Vault auditor account. ■ **Confirm Password** The confirming password for the Oracle Audit Vault Auditor account. ■ **Database Vault Owner** The account name of the Oracle Database Vault Owner. ■ **Password** The password for the Oracle Database Vault Owner account. ■ **Confirm Password** The confirming password for the Oracle Database Vault Owner account. ■ **Create a Separate Database Vault Account Manager** Accept the selected default check box to choose to create the Oracle Database Vault Account Manager account name to have a separation of duties between the Oracle Database Vault Owner and Oracle Database Vault Account Manager. Deselecting the check box disables the text fields for the Oracle Database Vault Account Manager user name and password. The Oracle Database Vault Owner in this case will be granted the role of Oracle Database Vault Account Manager and assume these duties. ■ **Account Manager** The account name of the Oracle Database Vault Account Manager. ■ **Password** The password for the Oracle Database Vault Account Manager account. ■ **Confirm Password** The confirming password for the Oracle Database Vault Account Manager account. See Section 4.8.1.4 for more information about Audit Vault Admin and Auditor user accounts and passwords See Section 4.8.1.5 for more information about Database Vault Owner and Account Manager user accounts and passwords.

Screen	Action
Specify Database Identifiers	Specify the following information, and click **Next**: ■ **Global Database Name** Specify the Global Database Name using the following syntax: *db_unique_name.db_domain* where: *db_unique_name* is the name of the database. It can contain a maximum of 30 characters as long as the first eight characters are unique and begin with an alphabetic character. The characters can include alphanumeric, underscore (_), dollar ($), and pound (#), no other special characters are permitted in a database name. *db_domain* is the computer environment used for the database. It should contain no more than 128 characters (alphanumeric, underscore (_), and pound (#)), inclusive of all periods. **Note:** Ensure that the combination of database name (first eight unique characters of database unique name), delimiter, and the database domain name does not exceed 128 characters. For example: sales.us.example.com where: *db_unique_name* is *sales* *db_domain* is *us.example.com* When you enter the Global Database Name, Oracle Universal Installer automatically populates the SID prefix with the database name. You can change this name in Advanced installation. Oracle Universal Installer limits the SID to 12 alphanumeric characters and the SID cannot contain an underscore (_), dollar ($), or pound (#). See Setting the ORACLE_HOSTNAME Environment Variable. ■ **Oracle Service Identifier (SID)** Oracle Service Identifier (SID) is a unique name for an Oracle database instance on a specific host. The SID helps in identifying the control file, and locating the files required to open the database. When you enter the Global Database Name, Oracle Universal Installer automatically populates the Oracle Service Identifier field with the database name. Oracle Univeral Installer limits the SID to 12 alphanumeric characters for single instance databases. For Oracle RAC databases, the SID prefix, which is the first 8 characters of the SID, must be a unique name for each database. The SID prefix cannot contain underscore (_), dollar ($), or pound (#).
Specify Memory Options	Specify the following memory details, and click **Next:** **Memory** Enable Automatic Memory Management option is selected by default. This option enables the database to automatically distribute memory between SGA and PGA. If you deselect this option, then the SGA and PGA must be sized manually.

Screen	Action
Specify Management Options	Select one of the following options, and click **Next:** ▪ Use an existing Oracle Enterprise Manager Grid Control for database management: This option is useful if you have Oracle Enterprise Manager installed. ▪ Use Oracle enterprise Manager Database Control for database management: This option enables you to manage Oracle Audit Vault Server locally. **See Also**: Section 1.8 for more information about database management options.
Specify Database Storage Options	Select one of the following options, and click **Next.** ▪ File System: Specify the database file location. ▪ Oracle Automatic Storage Management: Specify a password for the ASMSNMP user. **Note**: Installing Oracle data files on an Oracle ACFS file system is not supported. Oracle recommends that these data files are installed in Oracle ASM disk groups. **See Also**: Section 1.7 for more information about database storage options. **See Also**: Section 4.1.1 for more information about using Oracle Automatic Storage Management disk groups
Specify Recovery Options	Select one of the following options, and click **Next.** ▪ Do not enable automated backups ▪ Enable automated backups: If you select this option, then the backup job will use a specified recovery area storage. Select **File System** to use a file system directory for the fast recovery area, and then specify the fast recovery area path in the **Recovery Area location** field. Select **Oracle Automatic Storage Management** to use an Automatic Storage Management disk group for the fast recovery area. Specify your operating system user credentials to perform the backup job. **See Also**: Section 1.9 for more information about database backup and recovery options. **See Also**: Section 3.6 for more information about Oracle Automatic Storage Management
Select ASM Disk Group	This screen is displayed only if you select Oracle Automatic Storage Management as your storage option. Disk groups are created during the Oracle Grid Infrastructure installation. Disk groups are configured with the `SYSASM` privilege using `asmcmd` or `SQL create diskgroup` commands. An ASM disk group consists of multiple disk partitions. The table in this screen displays existing disk groups created during the Oracle Grid Infrastructure installation. Select the disk group that you want to use for database file storage.
Specify Schema Passwords	Enter and confirm passwords for the privileged database accounts, and click **Next.** **Note:** Optionally, you can use the same password for all accounts. However, Oracle recommends that you specify a different password for each account. You must remember the passwords that you specify. Refer to Section 4.9.3 for information about password guidelines.
Privileged Operating System Groups	The operating system groups are selected by default. You can also manually select the `OSDBA` and `OSOPER` groups. Click **Next.** **See Also**: Section 2.9 for information about operating system groups and users

Screen	Action
Perform Prerequisite Checks	This option checks if the minimum system requirements to perform the Oracle Audit Vault Server installation are met. If you click **Check Again,** then you can run the prerequisite check again to see if the minimum requirements are met to carry on with the Oracle Audit Vault Server installation. Click **Fix & Check Again,** if you want the installer to fix the problem and check the system requirements once more. **Note**: The Fix & Check Again option generates a script that you need to run as the `root` user. This generated script sets some of the system parameters to Oracle-recommended values. Oracle recommends that you do not modify the contents of this script. Refer to Section 2.4 for more information about fixup scripts. To get a list of failed requirements, select **ShowFailed** from the list. To get a list of all the prerequirement checks run by the OUI, select **Show All**. To get a list of the prerequirement checks that are successful, select **Show Succeeded.** **Note**: Oracle recommends that you use caution in checking the Ignore All option. If you check this option, then Oracle Universal Installer may not confirm that your system is able to install Oracle Audit Vault Server successfully. **See Also**: Chapter 2 for information about the system requirements
Summary	Review the information displayed on this screen, and click **Install.** Note: Starting with Oracle Audit Vault Server Release 10.3, you can save all the installation steps into a response file by clicking **Save Response File.** Later, this file can be used for a silent installation. See Section 4.7 and Appendix A for more information.
Install product	This screen states the progress of an Oracle Audit Vault Server installation. After Oracle Audit Vault Server is installed, you are prompted to execute a root configuration script for new inventory as the `root` user. This screen displays the status information for the configuration assistants that configure the Oracle Audit Vault Server. Finally, a message is displayed at the end of Audit Vault Configuration Assistant process. Click **Next.** Follow the steps as indicated on the **Execute Configuration scripts** screen to run the `root.sh`, and, if required, the `orainstRoot.sh` configuration scripts as the `root` user. After running the scripts, click **OK** on the **Execute Configuration scripts** screen to continue.
Finish	This screen is shown automatically when all the configuration tools are successful. Review the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL information displayed in this screen and click **Close.** On the **Exit** page, click **Exit**. Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

Caution: After installation is complete, do not manually remove, or run `cron` jobs that remove `/tmp/.oracle` or `/var/tmp/.oracle` directories or their files while Oracle software is running. If you remove these files, then Oracle software can encounter intermittent hangs. Oracle Restart installations will fail with the following error:

```
CRS-0184: Cannot communicate with the CRS daemon.
```

After you have completed the installation of Oracle Audit Vault Server, proceed to Section 4.9 to perform the postinstallation tasks.

See Section 4.9.6 for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

4.6 Advanced Installation - Software Only Installation

This section describes the advanced installation for a software only installation.

See Section 1.5 for information about why you would want to perform a software only installation to apply software patches during an initial Audit Vault Server installation.

There are two methods of performing a software only installation:

- Performing a Software Only Installation Using Oracle Universal Installer

  Run the installer from the command line and then select the "Install Oracle Audit Vault software only" option on the **Select Installation Option** screen of Oracle Universal Installer. This method is used in an upgrade procedure for upgrading from Oracle Audit Vault release 10.2.3.2 to Release 10.3. See Section 4.6.1 for more information.

- Performing Configuration After a Software Only Installation

  Run the installer from the command line with the `-noconfig` parameter option to perform a configuration after a software only installation. This method is used to apply preconfiguration patches to software components prior to running the configuration assistants. See Section 4.6.2 for more information.

4.6.1 Performing a Software Only Installation Using Oracle Universal Installer

Choose this software only installation method for performing an upgrade from Audit Vault Release 10.2.3.2 to Release 10.3.0.0. This installation procedure is described in detail in the Release 10.3 *Oracle Audit Vault Release Notes*. This software only installation method should also be used for installing Audit Vault on Oracle Data Guard sites.

4.6.2 Performing Configuration After a Software Only Installation

Choose this software only installation method for all other cases in which the configuration tools will be executed after the software only installation completes; in other words, use this method for preconfiguration patching of software components prior to running the configuration assistants.

Perform the following procedures to install Oracle Audit Vault Server software only.

1. Prepare the Audit Vault Server response file. You must create this response file because it is not supplied as part of the shiphome or Oracle home. Copy these lines from the following listing to a file, fill in the password information on each line for each configuration assistant, and then save the file to a name and directory of your choosing, such as `av_config.rsp`.

```
# Passwords for DBCA
oracle.assistants.server|S_HOSTUSERPASSWORD= <OS password needs to be given, if
automatic backup is choosen>
oracle.assistants.server|S_SYSPASSWORD=<sys password>
oracle.assistants.server|S_SYSTEMPASSWORD=<system password>
oracle.assistants.server|S_SYSMANPASSWORD=<sysman password>
oracle.assistants.server|S_DBSNMPPASSWORD=<DBSNMP password>
oracle.assistants.server|S_ASMSNMPPASSWORD= <ASMSNMP password, if ASM storage
```

```
is choosen>

# Passwords for DVCA
oracle.av.server|s_ownerPasswd=<DV owner password>
oracle.av.server|s_mgrPasswd=<DV manager password, if DV manager account is
choosen>

# Passwords for AVCA
oracle.av.server|s_adminPasswd=<AV admin password>
oracle.av.server|s_auditPasswd=<AV audit password, if AV auditor user is
choosen>
```

2. Run the Installer to install the Oracle Audit Vault Server software binaries using the following command and option:

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

   The `-noconfig` parameter indicates to install the software binaries only and do not run the configuration assistants.

   Proceed with this installation and configuration Audit Vault option. This will install the Audit Vault Server software only and prepare the `configToolAllCommands` file under *`$ORACLE_HOME`*`/cfgtoollogs` by saving interview values for later configuration. When this installation process is complete, exit the installer.

3. Download from My Oracle Support the Audit Vault Server 10.3.0.0 patches that must be applied before the configuration and unzip them into the *`$ORACLE_HOME`*`/av/patch` directory. The `/patch` directory should contain only the unarchived one-off patches and not the zip files.

   https://support.oracle.com/

   a. After signing in to My Oracle Support, click the **Patches & Updates** tab.

   b. Click **Product or Family (Advanced)** in the **Patch Search** panel.

   c. As you enter "Audit Vault" in the field that states "Type in comma separated values or choose from the list", choose "Oracle Audit Vault" from the list.

   d. In the **Select up to 10 field**, select the drop down arrow and select "Audit Vault 10.3.0.0.0. (Oracle Audit Vault)"

   e. Click **Search**.

   f. From the list of patches that display, select the patches and platform by clicking only the appropriate checkboxes to the right of the patch number, then select **Download** from the menu that displays. On the popup screen, click the name of the patch zip file, click **Save**, and specify a directory into which to save each patch zip file. If there are no patches available to download, the patch list that displays will be empty.

   g. Unzip each patch into its Audit Vault home location, *`OracleHome`*`/av/`*`patch`* directory.

4. Configure the Oracle Audit Vault binaries. Execute the following command as the installation user after setting the `ORACLE_HOME` environment variable and changing the current directory to the location of the `configToolAllCommands` utility. This utility installs the patches, runs the configuration assistants, and completes the Audit Vault Server installation. Use as the response file location, the location of the response file you prepared in Step 1.

```
setenv ORACLE_HOME /u01/app/oracle/product/10.3.0/av_1
cd directory-containing-the-configToolAllCommands utility
configToolAllCommands RESPONSE_FILE=response file location
```

For example:

```
setenv ORACLE_HOME /u01/app/oracle/product/10.3.0/av_1
cd $ORACLE_HOME/cfgtoollogs
configToolAllCommands RESPONSE_FILE=$ORACLE_HOME/av/av_config.rsp
```

5. Validate that the Oracle Audit Vault Server installation is successful and that the server is running. Issue the following command after having set the environment variables for the Oracle Audit Vault Server home, `PATH`, `LD_LIBRARY_PATH`, and `SID`. If successful, this command will indicate the server is running.

```
avctl show_av_status

Oracle Audit Vault 10g Database Control Release 10.3.0.0  Copyright (c) 1996,
 2011 Oracle Corporation.  All rights reserved.
https://hrdb.us.example.com:1158/av
Oracle Audit Vault 10g is running.
-----------------------------------
Logs are generated in directory /oracle/product/10.3.0/av_1/av/log
```

After you have completed the installation of Oracle Audit Vault Server, proceed to Section 4.9 to perform the postinstallation tasks.

4.7 Performing a Silent Installation Using a Response File

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

> **Note:** The Audit Vault silent installation does not support the Basic installation. Silent installation supports only the Advanced installation.

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

   Prepare the response file by entering values for all parameters that are missing in the response file, then save the file. For parameters that should not be changed, a comment is included in the file to indicate that you should not change the parameter value. Note that for both single instance and Oracle RAC 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 2.2.4 for more information.
4. Invoke Oracle Universal Installer using the following options:

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

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

4.8 Oracle 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 the following options:

- **Basic Install** – Simplifies the installation process and prompts for a minimal set of inputs, including the name of the Oracle Audit Vault database, the Oracle Audit Vault administrator and optionally the auditor user names and passwords. An Oracle RAC installation is not supported through the **Basic Install** option.
- **Advanced Install** – Offers the user more control and options for the installation process, including storage options and backup options. The **Advanced Install** option supports the installation of Audit Vault Server on a cluster.

This section includes the following topics:

4.8.1 Basic Install Configuration and Advanced Install: Specify Audit Vault Details Screens

This section describes the required fields in the **Basic Install Configuration** screen and the Advanced Install **Specify Audit Vault Details** screen. Topics include:

4.8.1.1 Oracle Base

If you have created a path for Oracle base in accordance with the Optimal Flexible Architecture rules for well-structured Oracle software environments, then OUI provides this path as the default Oracle base path. For OUI to recognize the path as an Oracle software path, it must be in the form `u0[1-9]/app`, and it must be writable by any member of the oraInventory (typically oinstall) group. The oraInventory group members have permissions to modify the oraInventory file, which is the central inventory for all Oracle software installations. Oracle recommends that you create an Oracle base path manually. The Optimal Flexible Architecture path for the Oracle base is `/u01/app/user`, where user is the name of the user account that you want to own the Oracle Audit Vault Server software.

4.8.1.2 Software Location

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

In addition, the special characters shown in Table 4–1 are allowed.

Table 4–1 Special Characters Allowed in the Oracle Audit Vault Home Location Name

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

4.8.1.3 Audit Vault SID

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

The Audit Vault SID cannot exceed 8 characters and must begin with an alphabetic character.

The Audit Vault SID cannot contain any of the characters shown in Table 4–2.

Table 4–2 Invalid Oracle Audit Vault SID and Oracle 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

Table 4–2 (Cont.) Invalid Oracle Audit Vault SID and Oracle Audit Vault Account

Symbol	Character Name
<	Less than sign
>	Greater than sign
/	Slash
\	Backslash
?	Question mark
,	Comma
.	Period
#	Number sign
_	Underscore
$	Dollar sign
	Space character

4.8.1.4 Oracle Audit Vault Server Accounts

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

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

Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Accounts

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

- *AV_ADMIN*`dvo` – The 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, the **Specify Audit Vault Details** screen includes prompts for the Database Vault Owner account name and password and a separate, optional Database Vault Account Manager account name and password.

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

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

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

Names	Names	Names	Names	Names
ACCESS	ADD	ALL	ALTER	AND
ANONYMOUS	ANY	AQ_ADMINISTRATOR_ ROLE	AQ_USER_ROLE	ARRAYLEN
AS	ASC	AUDIT	AUTHENTICATEDUSER	AV_ADMIN
AV_AGENT	AV_ARCHIVER	AV_AUDITOR	AV_SOURCE	AVSYS
BETWEEN	BY	CHAR	CHECK	CLUSTER
COLUMN	COMMENT	COMPRESS	CONNECT	CREATE
CTXAPP	CTXSYS	CURRENT	DATE	DBA
DBSNMP	DECIMAL	DEFAULT	DELETE	DELETE_CATALOG_ROLE
DESC	DIP	DISTINCT	DM_CATALOG_ROLE	DMSYS
DMUSER_ROLE	DROP	DV_ACCTMGR	DV_ADMIN	DVF
DV_OWNER	DV_PUBLIC	DV_REALM_OWNER	DV_REALM_RESOURCE	DV_SECANALYST
DVSYS	EJBCLIENT	ELSE	EXCLUSIVE	EXECUTE_CATALOG_ROLE
EXFSYS	EXISTS	EXP_FULL_DATABASE	FILE	FLOAT
FOR	FROM	GATHER_SYSTEM_ STATISTICS	GLOBAL_AQ_USER_ROLE	GRANT
GROUP	HAVING	HS_ADMIN_ROLE	IDENTIFIED	IMMEDIATE
IMP_FULL_ DATABASE	IN	INCREMENT	INDEX	INITIAL
INSERT	INTEGER	INTERSECT	INTO	IS
JAVA_ADMIN	JAVADEBUGPRIV	JAVA_DEPLOY	JAVAIDPRIV	JAVASYSPRIV
JAVAUSERPRIV	LBAC_DBA	LBACSYS	LEVEL	LIKE
LOCK	LOGSTDBY_ ADMINISTRATOR	LONG	MAXEXTENTS	MDDATA
MDSYS	MGMT_USER	MGMT_VIEW	MINUS	MODE
MODIFY	NOAUDIT	NOCOMPRESS	NOT	NOTFOUND
NOWAIT	NULL	NUMBER	OEM_ADVISOR	OEM_MONITOR

Names	Names	Names	Names	Names
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 4–1.

Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Passwords

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

For the advanced installation, the installer can choose individual passwords for each of these database accounts (`sys`, `system`, `sysman`, `dbsnmp`) or select to use the same password as the Oracle Audit Vault Administrator for all of these accounts. In addition, the **Specify Audit Vault Details** screen includes 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 Oracle Audit Vault Administrator and Oracle Audit Vault Auditor password cannot be the name of the Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Database Vault Owner, or Database Vault Account Manager. The Oracle Audit Vault Administrator user password is required, while the Oracle Audit Vault Auditor user password is only required when creating the separate, optional Oracle Audit Vault Auditor user.

There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one upper alphabetic character, one alphabetic character, one numeric character, and one of the special characters shown in Table 4–3.

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

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

Each password must be identical to its corresponding password confirmation.

4.8.1.5 Oracle Database Vault User Accounts

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.

Database Vault Owner and Database Vault Account Manager Accounts

The Database Vault Owner, Database Vault Account Manager, Oracle Audit Vault Administrator, and Oracle Audit Vault Auditor account names must be different from each other (applicable when a separate Oracle Audit Vault Auditor or 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 4.8.1.4.

Each account name cannot contain any of the characters shown in Table 4–1.

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 Oracle Audit Vault Administrator, Oracle 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 upper alphabetic character, one alphabetic character, one numeric character, and one of the special characters shown in Table 4–1. All other characters are not allowed.

Each password must be identical to its corresponding password confirmation.

4.8.2 Advanced Install: Node Selection Screen

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

See *Oracle Real Application Clusters Installation Guide for Linux and UNIX* for more information.

4.9 Required 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. Oracle 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 Oracle Audit Vault home is not supported.

Cloning of Oracle Audit Vault homes is not supported.

This section includes the following topics:

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

4.9.1 Download Patches

You can find mandatory Oracle Audit Vault patchsets on the My Oracle Support (formerly Oracle*MetaLink*) Web site.

To find and download patchsets for Oracle Audit Vault:

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

   https://support.oracle.com

2. Click the **Patches & Updates** tab.
3. Under **Patch Search**, click **Product or Family (Advanced Search)**.
4. Enter `Oracle Audit Vault` in the search field.
5. In the first **Select up to ten** list, expand the Oracle Audit Vault list and select **Audit Vault 10.3.0.0**. Click **Close**.
6. In the second **Select up to five** list, select your specific platform from the list, then click **Close**.
7. Click **Search**. In a moment, the patches associated with your selection appear.
8. Select the patch you want from the list by clicking its Patch ID link.
9. Click **View Read Me** to read about the patch details, and then click **Download** to download the patch to your computer.
10. Repeat Step 8 through Step 9 for each patch listed in the Patch Search Results section.
11. Use the unzip utility provided with Oracle Audit Vault Server 10.3 to uncompress the Oracle patch updates that you downloaded from My Oracle Support. The unzip utility is located in the `$ORACLE_HOME/bin` directory.

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

4.9.2 Download Critical Patch Updates

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

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

1. Follow Step 1 through Step 9 in Section 4.9.1 to find the critical patch updates for Oracle Audit Vault.
2. In the list of articles that appears, search for the phrase `Oracle Critical Patch Update`.
3. Select the most recent critical patch update article, and then read its instructions.

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

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

https://support.oracle.com

4.9.3 Reset User Passwords

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

For a basic installation, Oracle Audit Vault Server also uses the same Oracle Audit Vault Administrator password 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, Audit Vault Server uses the Database Vault Owner user password and the separate, optional Database Vault Account Manager user password for these users. You must change these passwords according to your company policies.

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

4.9.3.1 Using SQL*Plus to Reset Passwords

To reset user account passwords using SQL*Plus:

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

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

   In this example:

   The IDENTIFIED BY *password* clause resets the password.

   See Also:

   Oracle Database Security Guide for more information about:

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

4.9.3.2 Guidelines for Changing Passwords

Passwords for all Oracle system administration accounts except SYS, SYSTEM, SYSMAN, and DBSNMP are revoked after an Oracle Audit Vault Server installation. After the Audit Vault database is created during the installation, Oracle Database Configuration Assistant displays a screen with your Audit Vault database information and the Password Management button. For an Audit Vault installation, you should not need to unlock any locked accounts. Use the Password Management button to change the password only for the user names you use.

Apply the following guidelines when specifying passwords:

- Passwords must be between 8 and 30 characters long.
- Passwords must not start with a numeral.
- Passwords must not be the same as the user name.
- Passwords must not be Oracle reserved words.

- The SYS account password must not be change_on_install.
- The SYSTEM account password must not be manager.
- The SYSMAN account password must not be sysman.
- The DBSNMP account password must not be dbsnmp.
- If you choose to use the same password for all the accounts, then that password must not be change_on_install, manager, sysman, or dbsnmp.
- Passwords should have at least one alphabetic, one numeric, and one special character.
- Passwords should not be simple or obvious words, such as welcome, account, database, and user.
- Passwords should not have any consecutive repeating characters.

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

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

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

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

Use the following syntax to run DVCA:

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

In this example:

- action is the action to perform. The optionrac utility performs the action of updating the instance parameters for the Oracle RAC instance and optionally disabling SYSDBA operating system access for the instance.
- racnode is the host name of the Oracle RAC node on which the action is being performed. Do not include the domain name with the host name.
- oh is the Oracle home for the Oracle RAC instance. Provide the ORACLE_HOME path.
- jdbc_str is the JDBC connection string used to connect to the database. For example, in the following JDBC connection string, "jdbc:oracle:oci:@orcl1", orcl1 is the net service name in the tnsnames.ora file ($ORACLE_HOME/network/admin/tnsnames.ora).
- sys_password is the password for the SYS user. If you enter a cleartext password on the command line, then you must include the nodecrypt option. If you omit the password, then DVCA prompts you for it. For better security, Oracle strongly

recommends that you omit the password and then enter it interactively when you are prompted.

- `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
```

4.9.5 Download JDBC Driver Files for Source Database Connectivity

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

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

Section 4.9.5.1, Section 4.9.5.2, and Section 4.9.5.3 describe this download and copy process for each JDBC Driver.

4.9.5.1 Download SQL Server JDBC Driver Version 3.0 for SQL Server Connectivity

Oracle Audit Vault requires a JDBC connection to the SQL Server database. Audit Vault supports the use of Microsoft SQL Server JDBC Driver version 3.0 for this purpose. This driver provides high performance native access to Microsoft SQL Server 2000, 2005, and 2008 database data sources.

SQL Server JDBC Driver version 3.0 is not compatible with the Oracle Audit Vault 10.2.3.2.x Server and collection agents, which require version 1.2 of this driver. Version 1.2 is no longer available for download from Microsoft SQL Server.

To download SQL Server JDBC Driver version 3.0:

1. Go to the following Web site:
   `http://msdn.microsoft.com/en-us/sqlserver/aa937724`

2. Click the **Download Microsoft SQL Server JDBC Driver 3.0** link.
3. Select `1033\sqljdbc_3.0.1301.101_enu.tar.gz` and then click **Download**.
4. In a temporary directory, extract the files from this tar file.
5. Find the `sqljdbc.jar` file and place it in the `$ORACLE_HOME/jlib` directories in both the Audit Vault Server and Audit Vault collection agent homes. You can use this file for both Windows and UNIX systems.
6. Verify that the `sqljdbc.jar` file is present in the Oracle Audit Vault collection agent before you start the collection agent.

4.9.5.2 Download jConnect JDBC Driver for Sybase ASE Connectivity

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

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

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

Copy the `jconn3.jar` file to the Oracle Audit Vault Server and Oracle Audit Vault Agent home locations:

`$ORACLE_HOME``/jlib`

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

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

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

4.9.6 Log In to Oracle Audit Vault Console

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

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

   ```
   https://host:port/av
   ```

   In the preceding example:

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

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

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

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

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

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

4.9.7 Next Steps to Perform as an Oracle Audit Vault Administrator

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

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

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

4.10 Recommended Postinstallation Tasks

Oracle recommends that you perform the tasks described in the following section after completing an installation:

- Creating a Backup of the root.sh Script
- Setting the NLS_LANG Environment Variable
- Guidelines for Setting Semaphore Parameters

- Create a Fast Recovery Area Disk Group
- Guidelines for Changing Passwords

4.10.1 Creating a Backup of the root.sh Script

Oracle recommends that you back up the `root.sh` script after you complete an installation. If you install other products in the same Oracle home directory, then Oracle Universal Installer updates the contents of the existing `root.sh` script during the installation. If you require information contained in the original `root.sh` script, then you can recover it from the backed up `root.sh` file.

4.10.2 Setting the NLS_LANG Environment Variable

`NLS_LANG` is an environment variable that specifies the locale behavior for Oracle software. This variable sets the language and territory used by the client application and the database server. It also declares the character set of the client, which is the character set of data entered or displayed by an Oracle client program, such as SQL*Plus.

> **See Also:** Appendix F, "Configuring Oracle Database Globalization Support" in *Oracle Database Installation Guide for Linux* for more information about the `NLS_LANG` environment variable

4.10.3 Guidelines for Setting Semaphore Parameters

Refer to the following guidelines only if the default semaphore parameter values are too low to accommodate all Oracle processes:

> **Note:** Oracle recommends that you refer to the operating system documentation for more information about setting semaphore parameters.

1. Calculate the minimum total semaphore requirements using the following formula:

   ```
   sum (process parameters of all database instances on the system) + system and
   other application requirements
   ```

2. Set `semmns` (total semaphores systemwide) to this total.
3. Set `semmsl` (semaphores per set) to 256.
4. Set `semmni` (total semaphores sets) to `semmns / semmsl` rounded up to the nearest multiple of 1024.

4.10.4 Create a Fast Recovery Area Disk Group

During installation, by default you can create one disk group. If you plan to add an Oracle Audit Vault Server for a standalone server, then you should create the fast recovery area for database files.

4.10.4.1 About the Fast Recovery Area and the Fast Recovery Area Disk Group

The fast recovery area is a unified storage location for all Oracle Audit Vault Server files related to recovery. Database administrators can define the `DB_RECOVERY_FILE_`

DEST parameter to the path for the fast recovery area to enable on-disk backups, and rapid recovery of data. Enabling rapid backups for recent data can reduce requests to system administrators to retrieve backup tapes for recovery operations.

When you enable fast recovery in the init.ora file, all RMAN backups, archive logs, control file automatic backups, and database copies are written to the fast recovery area. RMAN automatically manages files in the fast recovery area by deleting obsolete backups and archive files no longer required for recovery.

Oracle recommends that you create a fast recovery area disk group. Oracle Clusterware files and Oracle Audit Vault Server files can be placed on the same disk group, and you can also place fast recovery files in the same disk group. However, Oracle recommends that you create a separate fast recovery disk group to reduce storage device contention.

The fast recovery area is enabled by setting DB_RECOVERY_FILE_DEST. The size of the fast recovery area is set with DB _RECOVERY_FILE_DEST. As a general rule, the larger the fast recovery area, the more useful it becomes. For ease of use, Oracle recommends that you create a fast recovery area disk group on storage devices that can contain at least three days of recovery information. Ideally, the fast recovery area should be large enough to hold a copy of all of your datafiles and control files, the online redo logs, and the archived redo log files needed to recover your database using the datafile backups kept under your retention policy.

Multiple databases can use the same fast recovery area. For example, assume you have created one fast recovery area disk group on disks with 150 GB of storage, shared by three different databases. You can set the size of the fast recovery for each database depending on the importance of each database. For example, if database1 is your least important database, database2 is of greater importance and database3 is of greatest importance, then you can set different DB_FILE_RECOVERY_DEST_SIZE settings for each database to meet your retention target for each database: 30 GB for database1, 50 GB for database2, and 70 GB for database3.

4.10.4.2 Creating the Fast Recovery Area Disk Group

To create a fast recovery file disk group:

1. Navigate to the Grid home bin directory, and start ASM Configuration Assistant (ASMCA). For example:

   ```
   $ cd /u01/grid/bin
   $ ./asmca
   ```

2. ASMCA opens at the Disk Groups tab. Click **Create** to create a new disk group.
3. The Create Disk Groups window opens.

   In the Disk Group Name field, enter a descriptive name for the fast recovery area group. For example: FRA.

   In the Redundancy section, select the level of redundancy you want to use.

   In the Select Member Disks field, select eligible disks to be added to the fast recovery area, and click **OK**.
4. The Diskgroup Creation window opens to inform you when disk group creation is complete. Click **OK**.
5. Click **Exit**.

See Also:

- "Setting the Fast Recovery Area Location and Initial Size" section in *Oracle Database Backup and Recovery User's Guide*
- *Oracle Automatic Storage Management Administrator's Guide*

5

Removing the Oracle Audit Vault Server Software

This chapter describes how to completely remove Oracle Audit Vault Server software and configuration files related to the specified Oracle home. It includes information about the following topics:

- Stopping the Oracle Audit Vault Server Software
- Reconfiguring Oracle Cluster Synchronization Services
- Removing Oracle Audit Vault Server Software Using the Deinstallation Tool

See Also:

- *Oracle Grid Infrastructure Installation Guide* and *Oracle Real Application Clusters Installation Guide* for information about removing an Oracle RAC installation.
- The "Dropping Disk Groups" section in the *Oracle Automatic Storage Management Administrator's Guide* for information about removing an Oracle ASM disk group.
- If you want to remove an individual product, refer to the product-specific documentation for requirements and restrictions.

5.1 Stopping the Oracle Audit Vault Server Software

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

Then, use the following procedure to stop the Oracle Audit Vault server software.

1. Stop the Oracle Audit Vault Console using the `avctl stop_av` command after setting the `PATH` environment variable to include `$ORACLE_HOME/bin`.

   The first command sets the `PATH` environment variable and the second command performs an `emctl stop dbconsole` operation. For example:

   - Bourne, Bash, or Korn shell

     ```
     $ export PATH=$PATH:$ORACLE_HOME/bin
     $ avctl stop_av
     ```

   - C Shell

     ```
     % setenv PATH ${PATH}:$ORACLE_HOME/bin
     ```

```
% avctl stop_av
```

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

2. Continue to Section 5.3.

5.2 Reconfiguring Oracle Cluster Synchronization Services

Oracle Cluster Synchronization Services (CSS) is a daemon process that is configured by the `root.sh` script when you configure an Oracle Grid Infrastructure instance. The CSS daemon runs out of the Oracle Grid Infrastructure home and is configured to start every time the system starts. This daemon process is required to enable synchronization between Oracle Automatic Storage Management (Oracle ASM) and database instances. It must be running if Oracle Audit Vault Server or an Oracle database is using Oracle ASM for database file storage.

Note: On cluster systems with Oracle RAC installations, the CSS daemon is configured during the Oracle Clusterware installation. If the system is running Oracle Clusterware, then refer to *Oracle Real Application Clusters Installation Guide* for information about removing Oracle RAC or Oracle Clusterware.

5.3 Removing Oracle Audit Vault Server Software Using the Deinstallation Tool

The `deinstall` command removes standalone Oracle Audit Vault Server installations, Oracle Clusterware and Oracle ASM from your server, and also Oracle Real Application Clusters (Oracle RAC) and Oracle Audit Vault Collection Agent installations.

The following sections describe the command, and provide information about additional options to use the command:

- About the Deinstallation Tool
- Example of Running the Deinstall Command
- Example of a Deinstallation Parameter File for Oracle Audit Vault Server
- Example of a Deinstallation Parameter File for Oracle Grid Infrastructure

Caution: If you have a standalone database on a node in a cluster and you have more than one database with the same global database name (GDN), then you cannot use the deinstall tool to remove one database only.

5.3.1 About the Deinstallation Tool

The Deinstallation Tool (`deinstall`) is available in the installation media before installation, and is available in Oracle home directories after installation. It is located in the path `$ORACLE_HOME/deinstall`.

The Deinstallation Tool (`deinstall`) is available in Oracle home directories after installation. It is located in the `$ORACLE_HOME/deinstall` directory.

The `deinstall` command uses the information you provide, plus information gathered from the software home to create a parameter file. You can alternatively supply a parameter file generated previously by the `deinstall` command using the `-checkonly` option, or by editing the response file template.

The command uses the following syntax, where variable content is indicated in italics:

```
deinstall -home complete path of Oracle home [-silent] [-checkonly] [-local]
[-paramfile complete path of input parameter property file] [-params name1=value
name2=value . . .] [-o complete path of directory for saving files] [-help | -h]
```

The default method for running the deinstall tool is from the deinstall directory in the Oracle home as the installation owner:

```
$ $ORACLE_HOME/deinstall/deinstall
```

Provide information about your servers as prompted or accept the defaults.

The `deinstall` command stops Oracle software, and removes Oracle software and configuration files on the operating system.

In addition, you can run the deinstall tool from other locations, or with a parameter file, or select other options to run the tool.

The options are:

- `-home`

  Use this flag to indicate the home path of the Oracle home that you want to check or deinstall. To deinstall Oracle software using the `deinstall` command in the Oracle home you plan to deinstall, provide a parameter file in another location, and do not use the `-home` flag.

  If you run deinstall from the `$ORACLE_HOME/deinstall` path, then the `-home` flag is not required because the tool knows from which home it is being run. If you use the standalone version of the tool, then `-home` is mandatory.

- `-silent`

  Use this flag to run the command in silent or response file mode. If you use the `-silent` flag, then you must use the `-paramfile` flag, and provide a parameter file that contains the configuration values for the Oracle home that you want to deinstall or deconfigure.

  You can generate a parameter file to use or modify by running `deinstall` with the `-checkonly` flag. The `deinstall` command then discovers information from the Oracle home that you want to deinstall and deconfigure. It generates the properties file, which you can then use with the `-silent` option.

  You can also modify the template file `deinstall.rsp.tmpl`, located in the `response` folder.

- `-checkonly`

  Use this flag to check the status of the Oracle software home configuration. Running the command with the `-checkonly` flag does not remove the Oracle configuration. The `-checkonly` flag generates a parameter file that you can use with the `deinstall` command.

- `-local`

  Use this flag on a multinode environment to deinstall Oracle software in a cluster.

When you run `deinstall` with this flag, it deconfigures and deinstalls the Oracle software on the local node (the node where `deinstall` is run). On remote nodes, it deconfigures Oracle software, but does not deinstall the Oracle software.

- `-paramfile` *`complete path of input parameter property file`*

  Use this flag to run `deinstall` with a parameter file in a location other than the default. When you use this flag, provide the complete path where the parameter file is located.

  The default location of the parameter file depends on the location of `deinstall`:

  – From the installation media or stage location: `$ORACLE_HOME/inventory/response`.

  – From a unzipped archive file from OTN: `/`*`ziplocation`*`/response`.

  – After installation from the installed Oracle home: `$ORACLE_HOME/deinstall/response`.

- `-params` [`name1=`*`value`* `name 2=`*`value`* `name3=`*`value`* `...`]

  Use this flag with a parameter file to override one or more values that you want to change in a parameter file you have already created.

- `-o` *`complete path of directory for saving response files`*

  Use this flag to provide a path other than the default location where the properties file (`deinstall.rsp.tmpl`) is saved.

  The default location of the parameter file depends on the location of `deinstall`:

  – From the installation media or stage location before installation: `$ORACLE_HOME/`

  – From a unzipped archive file from OTN: `/`*`ziplocation`*`/response/`.

  – After installation from the installed Oracle home: `$ORACLE_HOME/deinstall/response`.

- `-help | -h`

  Use the help option (`-help` or `-h`) to obtain additional information about the command option flags.

5.3.2 Example of Running the Deinstall Command

As the `deinstall` command runs, you are prompted to provide the home directory of the Oracle software that you want to remove from your system. Provide additional information as prompted.

Use the optional flag `-paramfile` to provide a path to a parameter file.

In the following example, the `deinstall` command is in the path `/u01/app/oracle/product/10.3.0/av_1/deinstall`, and it uses a parameter file in the software owner location `/home/usr/oracle`:

```
$ cd /u01/app/oracle/product/10.3.0/av_1/deinstall
$ ./deinstall -paramfile /home/usr/oracle/my_db_paramfile.tmpl
```

For the Oracle Grid Infrastructure home, use the deinstall script in the Oracle Grid Infrastructure for a standalone server home, which in this example is `/u01/app/oracle/product/10.3.0/grid`:

```
$ cd /u01/app/oracle/product/10.3.0/grid/deinstall
$ ./deinstall -paramfile /home/usr/oracle/my_grid_paramfile.tmpl
```

If you enter the deinstall command outside of the `$ORACLE_HOME/deinstall` folder, then help is displayed, unless you enter a `-home` flag and provide a path. If you run the deinstall command from the `$ORACLE_HOME/deinstall` folder, then deinstallation starts without prompting you for a home address.

5.3.3 Example of a Deinstallation Parameter File for Oracle Audit Vault Server

You can run the `deinstall` command on a standalone Oracle Audit Vault Server with the `-paramfile` option to use the values you specify in the parameter file. The following is an example of a parameter file, in which the Oracle Audit Vault Server binary owner is `oracle`, the Oracle Audit Vault Server home (Oracle home) is in the path `/u01/app/oracle/product/10.3.0/av_1/`, the Oracle base (where other Oracle software is installed) is `/u01/app/oracle/`, the central Oracle Inventory home (oraInventory) is `/u01/app/oraInventory`, the virtual IP address (VIP) is `192.0.2.1`, the local node (the node where you run the deinstallation session from) is `myserver`, and the OSDBA group is `dba`:

```
#Copyright (c) 2005, 2011 Oracle Corporation. All rights reserved.
#Mon Jul 18 06:48:39 UTC 2011
DISK_GROUPS.sidb=
ASM_HOME=
ASM_LOCAL_SID=
LOGDIR=/u01/app/oracle/product/10.3.0/av_1/oraInventory/logs/
ORACLE_BASE.sidb=/u01/app/oracle/
RECOVERY_LOC.sidb=
STORAGE_TYPE.sidb=FS
ORACLE_BASE=/u01/app/oracle/
INVENTORY_LOCATION=/u01/app/oraInventory
DB_TYPE.sidb=SI_DB
NODE_LIST.sidb=myserver
ARCHIVE_LOG_DESTINATION_LOC.sidb=
LOCAL_SID.sidb=sidb
DB_UNIQUE_NAME_LIST=sidb
ASM_FILES.sidb=
HOME_TYPE=SIDB
CRS_HOME=false
RAW_MAPPING_FILE.sidb=
SID_LIST.sidb=sidb
ORACLE_BINARY_OK=true
DATAFILE_LOC.sidb=/u01/app/oracle/oradata
local=false
LOCAL_NODE=myserver
CREATION_MODE.sidb=y
CONFIGFILE_LOC.sidb=
DIAG_DEST.sidb=/u01/app/oracle/
silent=false
ORACLE_HOME=/u01/app/oracle/product/10.3.0/av_1/
SPFILE_LOC.sidb=
```

5.3.4 Example of a Deinstallation Parameter File for Oracle Grid Infrastructure

You can run the `deinstall` command on an Oracle Grid Infrastructure for a standalone server home with the `-paramfile` option to use the values you specify in the parameter file.

The following is an example of a parameter file, in which the Oracle Grid Infrastructure binary owner is `oracle`, the Oracle Grid Infrastructure home is in the

path /u01/app/oracle/product/10.3.0/grid, the Oracle base (where other Oracle software is installed) is /u01/app/oracle/, the central Oracle Inventory home (oraInventory) is /u01/app/oraInventory, the local node (the node where you run the deinstallation session from) is myserver, and the OSDBA group is dba:

```
#Copyright (c) 2005, 2011 Oracle Corporation.  All rights reserved.
#Thu Jul 21 11:36:03 PST 2011
LOCAL_NODE=myserver
HOME_TYPE=SIHA
ASM_REDUNDANCY=EXTERNAL
ORACLE_BASE=/u01/app/oracle/
SCAN_PORT=0
silent=false
ASM_UPGRADE=false
ORA_CRS_HOME=/u01/app/oracle/product/10.3.0/grid
GPNPCONFIGDIR=$ORACLE_HOME
LOGDIR=/home/oracle/tmp/deinstall/logs/
ASM_DISCOVERY_STRING=/u02/stor/asm*
GPNPGCONFIGDIR=$ORACLE_HOME
ORACLE_OWNER=oracle
ASM_DISKSTRING=
CRS_STORAGE_OPTION=0
ORACLE_BINARY_OK=true
OCR_VOTINGDISK_IN_ASM=false
ASM_ORACLE_BASE=/u01/app/oracle
NETCFGJAR_NAME=netcfg.jar
ORA_DBA_GROUP=svrtech
JREDIR=/u01/app/oracle/grid/jdk/jre/
ORA_ASM_GROUP=dba
LANGUAGE_ID='AMERICAN_AMERICA.WE8ISO8859P1'
CSS_LEASEDURATION=400
ASM_HOME=/u01/app/oracle/grid
SHAREJAR_NAME=share.jar
HELPJAR_NAME=help4.jar
SILENT=false
local=false
INVENTORY_LOCATION=/u01/app/oraInventory
GNS_CONF=false
JEWTJAR_NAME=jewt4.jar
EMBASEJAR_NAME=oemlt.jar
ASM_
DISKS=/u02/stor/asm/asm0,/u02/stor/asm/asm2,/u02/stor/asm/asm3,/u02/stor/asm/asm1,
/u02/stor/asm/asm4,/u02/stor/asm/asm5,/u02/stor/asm/asm6,
/u02/stor/asm/asm7,/u02/stor/asm/asm8
ORACLE_HOME=/u01/app/oracle/grid
CRS_HOME=true
ASM_IN_HOME=true
EWTJAR_NAME=ewt3.jar
ASM_DROP_DISKGROUPS=false
ASM_LOCAL_SID=+ASM
JLIBDIR=/u01/app/oracle/grid/jlib
VNDR_CLUSTER=false
ASM_DISK_GROUP=DATA
```

A

Installing and Configuring Oracle Products Using Response Files

This appendix describes how to install and configure Oracle products using response files. It includes information about the following topics:

- How Response Files Work
- Creating the oraInst.loc File
- Preparing a Response File
- Running Oracle Universal Installer Using a Response File
- Silent-Mode Response File Error Handling

A.1 How Response Files Work

You can automate the installation and configuration of Oracle software, either fully or partially, by specifying a response file when you start Oracle Universal Installer. Oracle Universal Installer uses the values contained in the response file to provide answers to some or all of Oracle Universal Installer prompt. It includes information about the following topic:

- Reasons for Using Silent Mode or Response File Mode

Typically, Oracle Universal Installer runs in interactive mode, which means that it prompts you to provide information in graphical user interface (GUI) screens. When you use response files to provide this information, you run Oracle Universal Installer at a command prompt using either of the following modes:

- Silent mode

  If you include responses for all of the prompts in the response file and specify the `-silent` option when starting Oracle Universal Installer, then Oracle Universal Installer runs in silent mode. During a silent-mode installation, Oracle Universal Installer does not display any screens. Instead, it displays progress information in the terminal that you used to start it.

- Response file mode

  If you include responses for some or all of the prompts in the response file and omit the `-silent` option, then Oracle Universal Installer runs in response file mode. During a response file mode installation, Oracle Universal Installer displays all the screens, screens for which you specify information in the response file and also screens for which you did not specify the required information in the

response file. The advantage is that you can validate the values in the screens for which you have already provided the information in the response file and continue with the installation.

You define the settings for a silent or response file installation by entering values for the variables listed in the response file. For instance, to specify the Oracle home location for Oracle Audit Vault Server, you would supply the appropriate value for the `ORACLE_HOME` variable, as follows:

```
ORACLE_HOME=/u01/app/oracle/product/11.2.0/av_1
```

Another way of specifying the response file's variable settings is to pass them as command line arguments when you run Oracle Universal Installer. For example:

```
-silent directory_path
```

In this command, *`directory_path`* is the path of the Audit Vault directory on the DVD or on the hard drive.

This method is particularly useful if you do not want to embed sensitive information, such as passwords, in the response file. For example:

```
-silent "s_dlgRBOPassword=password" ...
```

Ensure that you enclose the variable and its setting in quotes.

> **See Also:** My Oracle Support Web site for more information on response files:
>
> https://support.oracle.com/

A.1.1 Reasons for Using Silent Mode or Response File Mode

The following table describes several reasons why you might want to run Oracle Universal Installer in silent mode or response file mode.

Mode	Uses
Silent	Use silent mode to: ▪ Complete an unattended installation, which you might schedule using operating system utilities such as `cron` ▪ Complete several similar installations on multiple systems without user interaction ▪ Install the software on a system that does not have X Window System software installed on it Oracle Universal Installer displays progress information in the terminal that you used to start it, but it does not display any of Oracle Universal Installer screens.
Response File	Use response file mode to complete similar Oracle software installations on more than one system, providing default answers to some, but not all of Oracle Universal Installer prompts. In response file mode, all the installer screens are displayed, but defaults for the fields in these screens are provided by the response file. You have to provide information for the fields in screens where you have not provided values in the response file.

A.2 Creating the oraInst.loc File

If you plan to install Oracle products using Oracle Universal Installer in silent or response file mode, then you must manually create the `oraInst.loc` file if it does not already exist. This file specifies the location of the Oracle Inventory directory where Oracle Universal Installer creates the inventory of Oracle products installed on the system.

> **Note:** If Oracle software has been installed previously on the system, the `oraInst.loc` file might already exist. If the file does exist, you do not need to create a file.

To create the `oraInst.loc` file, follow these steps:

1. Switch user to `root`:

   ```
   $ su - root
   ```

2. Create the `/etc/` directory if it does not exist:

   ```
   # mkdir /etc/
   ```

3. Change directory as follows:

   ```
   # cd /etc/
   ```

4. Use a text editor to create the `oraInst.loc` file, containing the following lines:

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

   In this example, `inventory_loc` is the location of the Oracle inventory; and the `inst_group` parameter shows the name of the Oracle inventory group (in this example, `oinstall`).

5. Enter the following commands to set the appropriate owner, group, and permissions on the `oraInst.loc` file:

   ```
   # chown oracle:oinstall oraInst.loc
   # chmod 664 oraInst.loc
   ```

A.3 Preparing a Response File

This section describes the following methods to prepare a response file for use during silent mode or response file mode installations:

- Editing a Response File Template
- Saving a Response File

A.3.1 Editing a Response File Template

Oracle provides response file templates for each product and installation type, and for each configuration tool. These files are located in the `/directory_path/response` directory, where `/directory_path/response` is the path of the Audit Vault directory on the DVD or on the hard drive.

Note: If you copied the software to a hard disk, the response files are located in the `directory_path/response` directory, where `/directory_path/response` is the path of the Audit Vault directory on the DVD or on the hard drive.

Table A–1 lists the response files provided with Oracle Audit Vault Server.

Table A–1 Response Files

Response File	Description
`av.rsp`	Silent installation of Oracle Audit Vault Server

To copy and modify a response file:

1. Copy the response file from the response file directory to a directory on your system:

   ```
   $ cp /directory_path/response/response_file.rsp local_directory
   ```

   In this example, *`directory_path`* is the path to the Audit Vault directory on the installation media. If you have copied the software to a hard drive, then you can edit the file in the `response` directory if you prefer.

2. Open the response file in a text editor:

   ```
   $ vi /local_dir/response_file.rsp
   ```

   Remember that you can specify sensitive information, such as passwords, at the command line rather than within the response file. Section A.1 explains this method.

3. Follow the instructions in the file to edit it.

   Note: Oracle Universal Installer or configuration assistant fails if you do not correctly configure the response file. Refer to Section A.5 for more information about troubleshooting a failed response file mode installation.

4. Change the permissions on the file to 700:

   ```
   $ chmod 700 /local_dir/response_file.rsp
   ```

   Note: A fully specified response file for an Oracle Audit Vault Server installation contains the passwords for database administrative accounts and for a user who is a member of the OSDBA group (required for automated backups). Ensure that only the Oracle software owner user can view or modify response files or consider deleting them after the installation succeeds.

A.3.2 Saving a Response File

You can use Oracle Universal Installer in interactive mode to save a response file, which you can edit and then use to complete silent mode or response file mode installations. This method is useful for custom or software-only installations.

You can save all the installation steps into a response file during installation. You can click the **Save Response File** button on the Summary page to do this. Later, this file can be used for a silent installation.

When you save the response file, you can either complete the installation, or you can exit from Oracle Universal Installer on the Summary page, before it starts to copy the software to the system.

If you save a response file during a silent installation, then Oracle Universal Installer saves the variable values that were specified in the original source response file into the new response file.

Note: Oracle Universal Installer does not save passwords in the response file.

To save a response file:

1. Complete the preinstallation tasks listed in Chapter 2.

   When you run Oracle Universal Installer to save a response file, it checks the system to verify that it meets the requirements to install the software. For this reason, Oracle recommends that you complete all of the required preinstallation tasks and save the response file while completing an installation.

2. If you have not installed Oracle software on this system previously, create the `oraInst.loc` file as described in Section A.2.

3. Ensure that the Oracle software owner user has permissions to create or write to the Oracle home path that you will specify when you run Oracle Universal Installer.

4. On each Oracle Universal Installer screen, specify the required information.

   See Also: Section 4.3 or Section 4.5 for information about the installation process

5. When Oracle Universal Installer displays the Summary screen, perform the following:

   1. Click **Save Response File** and specify a file name and location for the response file. Then, click **Save** to save the values to the file.

   2. Click **Finish** to continue with the installation.

      Click **Cancel** if you do not want to continue with the installation. The installation stops, but the saved response file is retained.

6. Before you use the saved response file on another system, edit the file and make any required changes.

   Use the instructions in the file as a guide when editing it.

A.4 Running Oracle Universal Installer Using a Response File

Now, you are ready to run Oracle Universal Installer at the command line, specifying the response file you created, to perform the installation. The Oracle Universal Installer executable, `runInstaller`, provides several options. For help information about the full set of these options, run the `runInstaller` command with the `-help` option, for example:

```
$ directory_path/runInstaller -help
```

The help information appears in a window after some time.

To run Oracle Universal Installer using a response file:

1. Complete the preinstallation tasks listed in Chapter 2.
2. Log in as the Oracle software owner user (typically, `oracle`).
3. If you are completing a response file mode installation, set the `DISPLAY` environment variable.

   Note: You do not have to set the `DISPLAY` environment variable if you are completing a silent-mode installation.

4. To start Oracle Universal Installer in silent or response file mode, enter a command similar to the following:

   ```
   $ /directory_path/runInstaller [-silent] [-noconfig] \
    -responseFile responsefilename
   ```

   Note: Do not specify a relative path to the response file. If you specify a relative path, then Oracle Universal Installer fails.

   In this example:

   - *directory_path* is the path of the Audit Vault directory on the DVD or on the hard drive.
   - `-silent` runs Oracle Universal Installer in silent mode.
   - `-noconfig` suppresses running the configuration assistants during installation, and a software-only installation is performed instead.
   - *responsefilename* is the full path and file name of the installation response file that you configured.
5. When the installation completes, log in as the `root` user and run the `root.sh` script:

   ```
   $ sudo sh
   password:
   # /oracle_home_path/root.sh
   ```

A.5 Silent-Mode Response File Error Handling

To determine if a silent-mode installation succeeds or fails, refer to the following log file:

/oraInventory_location`/logs/silentInstall`*date_time*`.log`

If necessary, refer to Section 2.12.2 for information about determining the location of the `oraInventory` directory.

A silent installation fails if:

- You do not specify a response file
- You specify an incorrect or incomplete response file

For example, a common problem is that while all the product-specific data is filled out correctly, the staging area location may be incorrect. If this is the case, check the `FROM_LOCATION` variable and ensure that it points to the `products.xml` file in the installation media. In the installation media, this `products.xml` is in the `stage/` directory.

- Oracle Universal Installer encounters an error, such as insufficient disk space

Oracle Universal Installer or configuration assistant validates the response file at run time. If the validation fails, the silent-mode installation or configuration process ends. Oracle Universal Installer treats values for parameters that are of the wrong context, format, or type as if no value was specified in the file.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

W

X