Oracle® Grid Infrastructure

Installation Guide

11*g* Release 2 (11.2) for HP-UX

E10815-02

April 2010

ORACLE®

Oracle Grid Infrastructure Installation Guide, 11*g* Release 2 (11.2) for HP-UX

E10815-02

Contents

C Oracle Grid Infrastructure for a Cluster Installation Concepts

D How to Complete Installation Prerequisite Tasks Manually

E How to Upgrade to Oracle Grid Infrastructure 11*g* Release 2

Index

List of Tables

Preface

Oracle Grid Infrastructure Installation Guide for HP-UX explains how to install and configure Oracle Clusterware, and how to configure a server and storage in preparation for an Oracle Real Application Clusters installation.

This preface contains the following topics:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

Oracle Grid Infrastructure Installation Guide for HP-UX provides configuration information for network and system administrators, and database installation information for database administrators (DBAs) who install and configure Oracle Clusterware.

For customers with specialized system roles who intend to install Oracle Real Application Clusters (Oracle RAC), this book is intended to be used by system administrators, network administrators, or storage administrators to complete the process of configuring a system in preparation for an Oracle Clusterware installation, and complete all configuration tasks that require operating system root privileges. When configuration and installation of Oracle Clusterware is completed successfully, a system administrator should only need to provide configuration information and to grant access to the database administrator to run scripts as `root` during Oracle RAC installation.

This guide assumes that you are familiar with Oracle database concepts. For additional information, refer to books in the Related Documents list.

Documentation Accessibility

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

accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, refer to the following Oracle resources:

Oracle Clusterware and Oracle Real Application Clusters Documentation

This installation guide reviews steps required to complete an Oracle Clusterware and Oracle Automatic Storage Management installation, and to perform preinstallation steps for Oracle RAC.

If you intend to install Oracle Database or Oracle RAC, then complete preinstallation tasks as described in this installation guide, complete grid infrastructure installation, and review those installation guides for additional information. You can install either Oracle databases for a standalone server on a grid infrastructure installation, or install an Oracle RAC database. If you want to install an Oracle Restart deployment of grid infrastructure, then refer to *Oracle Database Installation Guide for HP-UX*

Most Oracle error message documentation is only available in HTML format. If you only have access to the Oracle Documentation media, then browse the error messages by range. When you find a range, use your browser's "find in page" feature to locate a specific message. When connected to the Internet, you can search for a specific error message using the error message search feature of the Oracle online documentation.

Installation Guides

- *Oracle Diagnostics Pack Installation Guide*
- *Oracle Database Installation Guide for HP-UX*
- *Oracle Real Application Clusters Installation Guide for Linux and UNIX*

Operating System-Specific Administrative Guides

- *Oracle Database Administrator's Reference, 11g Release 2 (11.2) for UNIX Systems*

Oracle Clusterware and Oracle Automatic Storage Management Administrative Guides

- *Oracle Clusterware Administration and Deployment Guide*

- *Oracle Database Storage Administrator's Guide*

Oracle Real Application Clusters Administrative Guides

- *Oracle Real Application Clusters Administration and Deployment Guide*

- *Oracle Database 2 Day + Real Application Clusters Guide*

- *Oracle Database 2 Day DBA*

- *Getting Started with the Oracle Diagnostics Pack*

Generic Documentation

- *Oracle Database Administrator's Guide*

- *Oracle Database Concepts*

- *Oracle Database New Features Guide*

- *Oracle Database Net Services Administrator's Guide*

- *Oracle Database Reference*

Printed documentation is available for sale in the Oracle Store at the following Web site:

http://oraclestore.oracle.com/

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at the following Web site:

http://otn.oracle.com/membership/

If you already have a username and password for OTN, then you can go directly to the documentation section of the OTN Web site at the following Web site:

http://otn.oracle.com/documentation/

Oracle error message documentation is available only in HTML. You can browse the error messages by range in the Documentation directory of the installation media. When you find a range, use your browser's "find in page" feature to locate a specific message. When connected to the Internet, you can search for a specific error message using the error message search feature of the Oracle online documentation.

If you already have a username and password for OTN, then you can go directly to the documentation section of the OTN Web Site:

http://otn.oracle.com/documentation/

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.

Convention	Meaning
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.

What's New in Oracle Grid Infrastructure Installation and Configuration?

This section describes new features as they pertain to the installation and configuration of Oracle grid infrastructure (Oracle Clusterware and Automatic Storage Management), and Oracle Real Application Clusters (Oracle RAC). This guide replaces *Oracle Clusterware Installation Guide*. The topics in this section are:

- Desupported Options
- New Features for Release 2 (11.2)
- New Features for Release 1 (11.1)

Desupported Options

The following is a list of options desupported with this release:

Block and Raw Devices Not Supported with OUI

With this release, OUI no longer supports installation of Oracle Clusterware files on block or raw devices. Install Oracle Clusterware files either on Automatic Storage Management diskgroups, or in a supported shared file system.

New Features for Release 2 (11.2)

The following is a list of new features for installation of Oracle Clusterware and Oracle ASM 11*g* release 2 (11.2):

Oracle Automatic Storage Management and Oracle Clusterware Installation

With Oracle grid infrastructure 11*g* release 2 (11.2), Oracle Automatic Storage Management (Oracle ASM) and Oracle Clusterware are installed into a single home directory, which is referred to as the Grid Infrastructure home. Configuration assistants start after the installer interview process that configures Oracle ASM and Oracle Clusterware.

The installation of the combined products is called Oracle grid infrastructure. However, Oracle Clusterware and Oracle Automatic Storage Management remain separate products.

> **See Also:** *Oracle Database Installation Guide* for HP-UX for information about how to install Oracle grid infrastructure (Oracle ASM and Oracle Clusterware binaries) for a standalone server. This feature helps to ensure high availability for single-instance servers

Automatic Storage Management and Oracle Clusterware Files

With this release, Oracle Cluster Registry (OCR) and voting disks can be placed on Automatic Storage Management (ASM).

This feature enables ASM to provide a unified storage solution, storing all the data for the clusterware and the database, without the need for third-party volume managers or cluster filesystems.

For new installations, OCR and voting disk files can be placed either on ASM, or on a cluster file system or NFS system. Installing Oracle Clusterware files on raw or block devices is no longer supported, unless an existing system is being upgraded.

ASM Job Role Separation Option with SYSASM

The SYSASM privilege that was introduced in Oracle ASM 11*g* release 1 (11.1) is now fully separated from the SYSDBA privilege. If you choose to use this optional feature, and designate different operating system groups as the OSASM and the OSDBA groups, then the SYSASM administrative privilege is available only to members of the OSASM group. The SYSASM privilege also can be granted using password authentication on the Oracle ASM instance.

You can designate OPERATOR privileges (a subset of the SYSASM privileges, including starting and stopping ASM) to members of the OSOPER for ASM group.

Providing system privileges for the storage tier using the SYSASM privilege instead of the SYSDBA privilege provides a clearer division of responsibility between ASM administration and database administration, and helps to prevent different databases using the same storage from accidentally overwriting each other's files.

> **See Also:** *Oracle Database Storage Administrator's Guide*

Cluster Time Synchronization Service

Cluster node times should be synchronized. With this release, Oracle Clusterware provides Cluster Time Synchronization Service (CTSS), which ensures that there is a synchronization service in the cluster. If Network Time Protocol (NTP) is not found during cluster configuration, then CTSS is configured to ensure time synchronization.

Enterprise Manager Database Control Provisioning

Enterprise Manager Database Control 11*g* provides the capability to automatically provision Oracle grid infrastructure and Oracle RAC installations on new nodes, and then extend the existing Oracle grid infrastructure and Oracle RAC database to these provisioned nodes. This provisioning procedure requires a successful Oracle RAC installation before you can use this feature.

> **See Also:** *Oracle Real Application Clusters Administration and Deployment Guide* for information about this feature

Fixup Scripts and Grid Infrastructure Checks

With Oracle Clusterware 11*g* release 2 (11.2), the installer (OUI) detects when minimum requirements for installation are not completed, and creates shell script programs, called fixup scripts, to resolve many incomplete system configuration requirements. If OUI detects an incomplete task that is marked "fixable", then you can easily fix the issue by generating the fixup script by clicking the **Fix & Check Again** button.

The fixup script is generated during installation. You are prompted to run the script as root in a separate terminal session. When you run the script, it raises kernel values to

required minimums, if necessary, and completes other operating system configuration tasks.

You also can have Cluster Verification Utility (CVU) generate fixup scripts before installation.

Grid Plug and Play

In the past, adding or removing servers in a cluster required extensive manual preparation. With this release, you can continue to configure server nodes manually, or use Grid Plug and Play to configure them dynamically as nodes are added or removed from the cluster.

Grid Plug and Play reduces the costs of installing, configuring, and managing server nodes by starting a grid naming service within the cluster to allow each node to perform the following tasks dynamically:

- Negotiating appropriate network identities for itself

- Acquiring additional information it needs to operate from a configuration profile

- Configuring or reconfiguring itself using profile data, making hostnames and addresses resolvable on the network

Because servers perform these tasks dynamically, the number of steps required to add or delete nodes is minimized.

Intelligent Platform Management Interface (IPMI) Integration

Intelligent Platform Management Interface (IPMI) is an industry standard management protocol that is included with many servers today. IPMI operates independently of the operating system, and can operate even if the system is not powered on. Servers with IPMI contain a baseboard management controller (BMC) which is used to communicate to the server.

If IPMI is configured, then Oracle Cluster uses IPMI when node fencing is required and the server is not responding.

Oracle Clusterware Out-of-place Upgrade

With this release, you can install a new version of Oracle Clusterware into a separate home from an existing Oracle Clusterware installation. This feature reduces the downtime required to upgrade a node in the cluster. When performing an out-of-place upgrade, the old and new version of the software are present on the nodes at the same time, each in a different home location, but only one version of the software is active.

Oracle Clusterware Administration with Oracle Enterprise Manager

With this release, you can use Enterprise Manager Cluster Home page to perform full administrative and monitoring support for both standalone database and Oracle RAC environments, using High Availability Application and Oracle Cluster Resource Management.

When Oracle Enterprise Manager is installed with Oracle Clusterware, it can provide a set of users that have the Oracle Clusterware Administrator role in Enterprise Manager, and provide full administrative and monitoring support for High Availability application and Oracle Clusterware resource management. After you have completed installation and have Enterprise Manager deployed, you can provision additional nodes added to the cluster using Enterprise Manager.

SCAN for Simplified Client Access

With this release, the single client access name (SCAN) is the hostname to provide for all clients connecting to the cluster. The SCAN is a domain name registered to at least one and up to three IP addresses, either in the domain name service (DNS) or the Grid Naming Service (GNS). The SCAN eliminates the need to change clients when nodes are added to or removed from the cluster. Clients using the SCAN can also access the cluster using EZCONNECT.

SRVCTL Command Enhancements for Patching

With this release, you can use `srvctl` to shut down all Oracle software running within an Oracle home, in preparation for patching. Oracle grid infrastructure patching is automated across all nodes, and patches can be applied in a multi-node, multi-patch fashion.

Typical Installation Option

To streamline cluster installations, especially for those customers who are new to clustering, Oracle introduces the Typical Installation path. Typical installation defaults as many options as possible to those recommended as best practices.

Voting Disk Backup Procedure Change

In prior releases, backing up the voting disks using a `dd` command was a required postinstallation task. With Oracle Clusterware release 11.2 and later, backing up and restoring a voting disk using the `dd` command is not supported.

Backing up voting disks manually is no longer required, as voting disks are backed up automatically in the OCR as part of any configuration change and voting disk data is automatically restored to any added voting disks.

> **See Also:**   *Oracle Clusterware Administration and Deployment Guide*

New Features for Release 1 (11.1)

The following is a list of new features for release 1 (11.1)

Changes in Installation Documentation

With Oracle Database 11*g* release 1, Oracle Clusterware can be installed or configured as an independent product, and additional documentation is provided on storage administration. For installation planning, note the following documentation:

Oracle Database 2 Day + Real Application Clusters Guide

This book provides an overview and examples of the procedures to install and configure a two-node Oracle Clusterware and Oracle RAC environment.

Oracle Clusterware Installation Guide

This book (the guide that you are reading) provides procedures either to install Oracle Clusterware as a standalone product, or to install Oracle Clusterware with either Oracle Database, or Oracle RAC. It contains system configuration instructions that require system administrator privileges.

Oracle Real Application Clusters Installation Guide

This platform-specific book provides procedures to install Oracle RAC after you have completed successfully an Oracle Clusterware installation. It contains database configuration instructions for database administrators.

Oracle Database Storage Administrator's Guide

This book provides information for database and storage administrators who administer and manage storage, or who configure and administer Automatic Storage Management (ASM).

Oracle Clusterware Administration and Deployment Guide

This is the administrator's reference for Oracle Clusterware. It contains information about administrative tasks, including those that involve changes to operating system configurations and cloning Oracle Clusterware.

Oracle Real Application Clusters Administration and Deployment Guide

This is the administrator's reference for Oracle RAC. It contains information about administrative tasks. These tasks include database cloning, node addition and deletion, Oracle Cluster Registry (OCR) administration, use of SRVCTL and other database administration utilities, and tuning changes to operating system configurations.

Release 1 (11.1) Enhancements and New Features for Installation

The following is a list of enhancements and new features for Oracle Database 11*g* release 1 (11.1):

New SYSASM Privilege and OSASM operating system group for ASM Administration

This feature introduces a new SYSASM privilege that is specifically intended for performing ASM administration tasks. Using the SYSASM privilege instead of the SYSDBA privilege provides a clearer division of responsibility between ASM administration and database administration.

OSASM is a new operating system group that is used exclusively for ASM. Members of the OSASM group can connect as SYSASM using operating system authentication and have full access to ASM.

1

Typical Installation for Oracle Grid Infrastructure for a Cluster

This chapter describes the difference between a Typical and Advanced installation for Oracle grid infrastructure for a cluster, and describes the steps required to complete a Typical installation.

This chapter contains the following sections:

- Typical and Advanced Installation
- Preinstallation Steps Completed Using Typical Installation
- Preinstallation Steps Requiring Manual Tasks

1.1 Typical and Advanced Installation

You are given two installation options for Oracle grid infrastructure installations:

- **Typical Installation**: The Typical installation option is a simplified installation with a minimal number of manual configuration choices. Oracle recommends that you select this installation type for most cluster implementations.

- **Advanced Installation**: The Advanced Installation option is an advanced procedure that requires a higher degree of system knowledge. It enables you to select particular configuration choices, including additional storage and network choices, use of operating system group authentication for role-based administrative privileges, integration with IPMI, or more granularity in specifying Automatic Storage Management roles.

1.2 Preinstallation Steps Completed Using Typical Installation

With Oracle Clusterware 11*g* release 2 (11.2), during installation Oracle Universal Installer (OUI) generates Fixup scripts (`runfixup.sh`) that you can run to complete required preinstallation steps.

The fixup script is generated during installation. You are prompted to run the script as `root` in a separate terminal session. When you run the script, it completes the following configuration tasks:

- If necessary sets kernel parameters required for installation and runtime to at least the minimum value.

1.3 Preinstallation Steps Requiring Manual Tasks

Complete the following manual configuration tasks

- Verify System Requirements

- Check Network Requirements

- Check Operating System Packages

- Create Groups and Users

- Check Storage

- Prepare Storage for Automatic Storage Management

- Install Oracle Grid Infrastructure Software

> **See Also:** Chapter 2, "Advanced Installation Oracle Grid Infrastructure for a Cluster Preinstallation Tasks" and Chapter 3, "Configuring Storage for Grid Infrastructure for a Cluster and Oracle Real Application Clusters (Oracle RAC)" if you need any information about how to complete these tasks

1.3.1 Verify System Requirements

Enter the following commands to check available memory:

```
# /usr/contrib/bin/machinfo  | grep -i Memory
# /usr/sbin/swapinfo -a
```

The minimum required RAM is 4 GB. The minimum required swap space is 4 GB.

```
# bdf
```

This command checks the available space on file systems. If you use normal redundancy for Oracle Clusterware files, which is three Oracle Cluster Registry (OCR) locations and three voting disk locations, then you should have at least 2 GB of file space available on shared storage volumes reserved for Oracle grid infrastructure files.

If you plan to install on Oracle ASM, then to ensure high availability of Oracle Clusterware files on Oracle ASM, you need to have at least 2 GB of disk space for Oracle Clusterware files in three separate failure groups, with at least three physical disks. Each disk must have at least 1 GB of capacity to ensure that there is sufficient space to create Oracle Clusterware files.

Ensure you have at least 4.5 GB of space for the grid infrastructure for a cluster home (Grid home) This includes Oracle Clusterware and Automatic Storage Management (Oracle ASM) files and log files.

```
# bdf /tmp
```

Ensure that you have at least 1 GB of space in /tmp. If this space is not available, then increase the size, or delete unnecessary files in /tmp. If /tmp and the grid home are on the same filesystem, then add together their respective disk space requirements for the total minimum space required.

For more information, review the following section in Chapter 2:

"Checking the Hardware Requirements"

1.3.2 Check Network Requirements

Ensure that you have the following available:

- Single Client Access Name (SCAN) for the Cluster

- IP Address Requirements

■ Intended Use of Network Interfaces

1.3.2.1 Single Client Access Name (SCAN) for the Cluster

During Typical installation, you are prompted to confirm the default Single Client Access Name (SCAN), which is used to connect to databases within the cluster irrespective of which nodes they are running on. By default, the name used as the SCAN is also the name of the cluster. The default value for the SCAN is based on the local node name. If you change the SCAN from the default, then the name that you use must be globally unique throughout your enterprise.

In a Typical installation, the SCAN is also the name of the cluster. The SCAN and cluster name must be at least one character long and no more than 15 characters in length, must be alphanumeric, and may contain hyphens (-).

For example:

```
NE-Sa89
```

If you require a SCAN that is longer than 15 characters, then be aware that the cluster name defaults to the first 15 characters of the SCAN.

Refer to the following section for the SCAN address requirements.

1.3.2.2 IP Address Requirements

Before starting the installation, you must have at least two interfaces configured on each node: One for the private IP address and one for the public IP address.

> **Note:** Oracle recommends that you use a static hostname for all server node public hostnames.

1.3.2.2.1 IP Address Requirements for Manual Configuration The public and virtual IP addresses must be static addresses, configured before installation, and the virtual IP addresses for each node must not currently be in use. Oracle Clusterware manages private IP addresses in the private subnet on interfaces you identify as private during the installation interview.

Configure the following addresses:

■ A public IP address for each node

■ A virtual IP address for each node

■ A single client access name (SCAN) configured on the domain name server (DNS) for Round Robin resolution to three addresses (recommended) or at least one address.

The single client access name (SCAN) is a cluster alias used to provide service access for clients to the cluster. Because the SCAN is associated with the cluster as a whole, rather than to a particular node, the SCAN makes it possible to add or remove nodes from the cluster without needing to reconfigure clients. It also adds location independence for the databases, so that client configuration does not have to depend on which nodes are running a particular database. Clients can continue to access the cluster in the same way as with previous releases, but Oracle recommends that clients accessing the cluster use the SCAN.

> **Note:** If you manually configure addresses, then Oracle strongly recommends that you use DNS resolution for SCAN VIPs.

> **See Also:** , Appendix C, "Oracle Grid Infrastructure for a Cluster Installation Concepts"for more information about network addresses

1.3.2.3 Intended Use of Network Interfaces

During installation, you are asked to identify the planned use for each network interface that OUI detects on your cluster node. You must identify each interface as a public or private interface, and you must use the same private interfaces for both Oracle Clusterware and Oracle RAC. For interfaces that you plan to have used for other purposes--for example, an interface dedicated to a network file system--you must identify those instances as "do not use" interfaces, so that Oracle Clusterware ignores them.

You can bond separate interfaces to a common interface to provide redundancy, in case of a NIC failure, but Oracle recommends that you do not create separate interfaces for Oracle Clusterware and Oracle RAC. If you use more than one NIC for the private interconnect, then Oracle recommends that you use NIC bonding. Note that multiple private interfaces provide load balancing but not failover, unless bonded.

1.3.3 Check Operating System Packages

Refer to the tables listed in Section 2.7, "Identifying Software Requirements" for the list of required packages for your operating system.

1.3.4 Create Groups and Users

Enter the following commands to create default groups and users:

One system privileges group for all operating system-authenticated administration privileges, including Oracle RAC (if installed):

```
# groupadd -g 1000 oinstall
# groupadd -g 1200 dba
# useradd -u 1100 -g oinstall -G dba oracle
# mkdir -p  /u01/app/11.2.0/grid
# mkdir -p /u01/app/oracle
# chown -R oracle:oinstall /u01
# chmod -R 775 /u01/
```

1.3.5 Check Storage

You must have space available on Automatic Storage Management for Oracle Clusterware files (voting disks and Oracle Cluster Registries), and for Oracle Database files, if you install standalone or Oracle Real Application Clusters Databases. Creating Oracle Clusterware files on block or raw devices is no longer supported for new installations.

> **Note:** When using Oracle Automatic Storage Management (Oracle ASM) for either the Oracle Clusterware files or Oracle Database files, Oracle creates one Oracle ASM instance on each node in the cluster, regardless of the number of databases.

1.3.6 Prepare Storage for Automatic Storage Management

Review the relevant sections in Chapter 3.

> **See Also:** Chapter 3, "Configuring Storage for Grid Infrastructure for a Cluster and Oracle Real Application Clusters (Oracle RAC)" if you require detailed storage configuration information

1.3.7 Install Oracle Grid Infrastructure Software

1. Start OUI from the root level of the installation media. For example:

   ```
   ./runInstaller
   ```

2. Select Install and Configure Grid Infrastructure for a Cluster, then select Typical Installation. In the installation screens that follow, enter the configuration information as prompted.

   If you receive an installation verification error that cannot be fixed using a fixup script, then review Chapter 2, "Advanced Installation Oracle Grid Infrastructure for a Cluster Preinstallation Tasks" to find the section for configuring cluster nodes. After completing the fix, continue with the installation until it is complete.

   > **See Also:** Chapter 4, "Installing Oracle Grid Infrastructure for a Cluster"

2

Advanced Installation Oracle Grid Infrastructure for a Cluster Preinstallation Tasks

This chapter describes the system configuration tasks that you must complete before you start Oracle Universal Installer (OUI) to install Oracle grid infrastructure.

This chapter contains the following topics:

- Reviewing Upgrade Best Practices
- Installation Fixup Scripts
- Logging In to a Remote System Using X Terminal
- Creating Groups, Users and Paths for Oracle Grid Infrastructure
- Checking the Hardware Requirements
- Checking the Network Requirements
- Identifying Software Requirements
- Checking the Software Requirements
- Network Time Protocol Setting
- Automatic SSH Configuration During Installation
- Configuring Grid Infrastructure Software Owner User Environments
- Creating Required Symbolic Links
- Requirements for Creating an Oracle Clusterware Home Directory
- Requirements for Creating an Oracle Grid Infrastructure Home Directory

2.1 Reviewing Upgrade Best Practices

> **Caution:** Always create a backup of existing databases before starting any configuration change.

If you have an existing Oracle installation, then document version numbers, patches, and other configuration information, and review upgrade procedures for your existing installation. Review Oracle upgrade documentation before proceeding with installation, to decide how you want to proceed.

You can upgrade Oracle ASM 11*g* release 1 (11.1) without shutting down an Oracle RAC database by performing a rolling upgrade either of individual nodes, or of a set of nodes in the cluster. However, if you have a standalone database on a cluster that uses Oracle ASM, then you must shut down the standalone database before upgrading. If you are upgrading from Oracle ASM 10*g*, then you must shut down the entire Oracle ASM cluster to perform the upgrade.

If you have an existing Oracle Automatic Storage Management (Oracle ASM) installation, then review Oracle upgrade documentation. The location of the Oracle ASM home changes in this release, and you may want to consider other configuration changes to simplify or customize storage administration. If you have an existing Oracle ASM home from a previous release, then it should be owned by the same user that you plan to use to upgrade Oracle Clusterware.

During rolling upgrades of the operating system, Oracle supports using different operating system binaries when both versions of the operating system are certified with the Oracle Database release you are using.

> **Note:** Using mixed operating system versions is only supported for the duration of an upgrade, over the period of a few hours. Oracle does not support operating a cluster with mixed operating systems for an extended period. Oracle does not support running Oracle grid infrastructure and Oracle Real Application Clusters on heterogeneous platforms (servers with different chip architectures) in the same cluster.

To find the most recent software updates, and to find best practices recommendations about preupgrade, postupgrade, compatibility, and interoperability, refer to "Oracle Upgrade Companion." "Oracle Upgrade Companion" is available through Note 785351.1 on My Oracle Support:

https://metalink.oracle.com

2.2 Installation Fixup Scripts

With Oracle Clusterware 11*g* release 2, Oracle Universal Installer (OUI) detects when the minimum requirements for an installation are not met, and creates shell scripts, called fixup scripts, to finish incomplete system configuration steps. If OUI detects an incomplete task, then it generates fixup scripts (`runfixup.sh`). You can run the fixup script after you click the **Fix and Check Again** Button.

You also can have CVU generate fixup scripts before installation.

> **See Also:** *Oracle Clusterware Administration and Deployment Guide* for information about using the `cluvfy` command

The Fixup script does the following:

- If necessary sets kernel parameters to values required for successful installation, including:
  - Shared memory parameters.
  - Open file descriptor and UDP send/receive parameters.
- Sets permissions on the Oracle Inventory (central inventory) directory.

If you have SSH configured between cluster member nodes for the user account that you will use for installation, then you can check your cluster configuration before installation and generate a fixup script to make operating system changes before starting the installation.

To do this, log in as the user account that will perform the installation, navigate to the staging area where the runcluvfy command is located, and use the following command syntax, where *node* is a comma-delimited list of nodes you want to make cluster members:

$ ./runcluvfy.sh stage -pre crsinst -n *node* -fixup -verbose

For example, if you intend to configure a two-node cluster with nodes node1 and node2, enter the following command:

```
$ ./runcluvfy.sh stage -pre crsinst -n node1,node2 -fixup -verbose
```

2.3 Logging In to a Remote System Using X Terminal

During installation, you are required to perform tasks as root or as other users on remote terminals. Complete the following procedure for user accounts that you want to enable for remote display.

> **Note:**   If you log in as another user (for example, `oracle`), then repeat this procedure for that user as well.

To enable remote display, complete one of the following procedures:

- If you are installing the software from an X Window System workstation or X terminal, then:

  1. Start a local terminal session, for example, an X terminal (`xterm`).

  2. If you are installing the software on another system and using the system as an X11 display, then enter a command using the following syntax to enable remote hosts to display X applications on the local X server:

     ```
     # xhost + RemoteHost
     ```

     where `RemoteHost` is the fully qualified remote hostname. For example:

     ```
     # xhost + somehost.example.com
     somehost.example.com being added to the access control list
     ```

  3. If you are not installing the software on the local system, then use the `ssh`, command to connect to the system where you want to install the software:

     ```
     # ssh -Y RemoteHost
     ```

     where `RemoteHost` is the fully qualified remote hostname. The `-Y` flag ("yes") enables remote X11 clients to have full access to the original X11 display.

     For example:

     ```
     # ssh -Y somehost.example.com
     ```

  4. If you are not logged in as the `root` user, then enter the following command to switch the user to `root`:

     ```
     $ su - root
     ```

```
password:
#
```

- If you are installing the software from a PC or other system with X server software installed, then:

> **Note:** If necessary, refer to your X server documentation for more information about completing this procedure. Depending on the X server software that you are using, you may need to complete the tasks in a different order.

1. Start the X server software.

2. Configure the security settings of the X server software to permit remote hosts to display X applications on the local system.

3. Connect to the remote system where you want to install the software as the Oracle grid infrastructure for a cluster software owner (`grid`, `oracle`) and start a terminal session on that system, for example, an X terminal (`xterm`).

4. Open another terminal on the remote system, and log in as the `root` user on the remote system, so you can run scripts as `root` when prompted.

2.4 Creating Groups, Users and Paths for Oracle Grid Infrastructure

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

-

> **Note:** During a grid infrastructure installation, both Oracle Clusterware and Automatic Storage Management are installed. You no longer can have separate Oracle Clusterware installation owners and Automatic Storage Management installation owners.

2.4.1 Determining If the Oracle Inventory and Oracle Inventory Group Exists

When you install Oracle software on the system for the first time, OUI creates the `oraInst.loc` file. This file identifies the name of the Oracle Inventory group (by default, `oinstall`), and the path of the Oracle Central Inventory directory. An `oraInst.loc` file 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 (the OINSTALL group privilege).

If you have an existing Oracle central 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 you have an Oracle Inventory on your system:

1. Enter the following command:

```
# more /var/opt/oracle/oraInst.loc
```

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

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

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`).

2. Ensure that Oracle Inventory group members are granted the HP-UX privileges RTPRIO, MLOCK, and RTSCHED. For example:

```
# /usr/bin/getprivgrp oinstall
oinstall: RTPRIO MLOCK RTSCHED
```

If the group is not granted these privileges, then add these privileges as described in the next section.

If the Oracle Inventory group you plan to use does not exist, then you receive an error in response to the `getprivgrp` command. For example:

```
$ grep wronggroup /etc/group
usage: getprivgrp [-g | group-name]
```

2.4.2 Creating the Oracle Inventory Group If an Oracle Inventory Does Not Exist

If the `oraInst.loc` file does not exist, then complete the following tasks:

1. Create the Oracle Inventory group by entering a command similar to the following:

```
# /usr/sbin/groupadd -g 1000 oinstall
```

The preceding command creates the group `oinstall`, with the group ID number 1000. Members of the OINSTALL group are granted privileges to write to the Oracle central inventory (`oraInventory`).

By default, if an oraInventory group does not exist, then the installer lists the primary group of the installation owner for the grid infrastructure for a cluster as the oraInventory group. Ensure that this group is available as a primary group for all planned Oracle software installation owners.

> **Note:** Group and user IDs must be identical on all nodes in the cluster. Check to make sure that the group and user IDs you want to use are available on each cluster member node, and confirm that the primary group for each grid infrastructure for a cluster installation owner has the same name and group ID.

2. If it does not already exist, create the `/etc/privgroup` file. Add a line similar to the following to grant Oracle installation owners the RTPRIO, MLOCK, and RTSCHED privileges:

```
oinstall RTPRIO MLOCK RTSCHED
```

If `/etc/privgroup` exists, then add these privileges to the Oracle Inventory group. For example:

```
# /usr/sbin/setprivgrp oinstall RTPRIO MLOCK RTSCHED
```

Confirm the grant of privileges to the group. For example:

```
# /usr/bin/getprivgrp oinstall
oinstall: RTPRIO MLOCK RTSCHED
```

3. Repeat this procedure on all of the other nodes in the cluster.

2.4.3 Creating the Oracle Grid Infrastructure User

You must create a software owner for Oracle Clusterware 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 separate grid infrastructure administrative privileges from Oracle Database administrative privileges.

  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.

2.4.3.1 Understanding Restrictions for Oracle Software Installation Owners

If you intend to use multiple Oracle software owners for different Oracle Database homes, then Oracle recommends that you create a separate software owner for Oracle grid infrastructure software (Oracle Clusterware and Oracle ASM), and use that owner to run the Oracle grid infrastructure installation.

If you plan to install Oracle Database or Oracle RAC, then Oracle recommends that you create separate users for the Oracle grid infrastructure and the Oracle Database installations. If you use one installation owner, then when you want to perform administration tasks, you must change the value for $ORACLE_HOME to the instance you want to administer (ASM, in the grid infrastructure home, or the database in the Oracle home), using command syntax such as the following example, where grid is the Oracle grid infrastructure home:

ORACLE_HOME=/u01/app/11.2.0/grid; export ORACLE_HOME

If you try to administer an instance using `sqlplus`, `lsnrctl`, or `asmcmd` commands while $ORACLE_HOME is set to a different binary path, then you will encounter errors. When starting srvctl from a database home, $ORACLE_HOME should be set. or `srvctl` fails. But if you are using `srvctl` in the grid infrastructure home, then $ORACLE_HOME is ignored, and the oracle home path does not affect `srvctl` commands. You always have to change $ORACLE_HOME to the instance that you want to administer.

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, and are also granted permissions for various Oracle Clusterware resources, OCR keys, directories in the Oracle Clusterware

home to which DBAs need write access, and other necessary privileges. In Oracle documentation, this group is represented as `oinstall` in code examples.

Each Oracle software owner must be a member of the same central inventory group. You cannot have more than one central inventory for Oracle installations. If an Oracle software owner has a different central inventory group, then you may corrupt the central inventory.

> **Caution:** For grid infrastructure for a cluster installations, the Grid home must not be placed under one of the Oracle base directories, or under Oracle home directories of Oracle Database installation owners, or in the home directory of an installation owner. During installation, ownership of the path to the Grid home is changed to `root`. This change causes permission errors for other installations.

2.4.3.2 Determining if an Oracle Software Owner User Exists

To determine whether an Oracle software owner user named `oracle` or `grid` exists, enter a command similar to the following (in this case, to determine if `oracle` exists):

```
# id oracle
```

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

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

Determine whether you want to use the existing user, or create another user. The user and group ID numbers must be the same on each node you intend to make a cluster member node.

To use the existing user, ensure that the user's primary group is the Oracle Inventory group (`oinstall`). If this user account will be used for Oracle Database installations, and you plan to have a different user account as the owner of the Oracle Clusterware and Oracle ASM binaries, then ensure that the Oracle account is also a member of the group you plan to designate as the OSDBA for ASM group (the group whose members are permitted to write to Oracle ASM storage).

2.4.3.3 Creating or Modifying an Oracle Software Owner User for Oracle Grid Infrastructure

If the Oracle software owner (`oracle`, `grid`) user does not exist, or if you require a new Oracle software owner user, then create it. If you want to use an existing user account, then modify it to ensure that the user ID and group IDs are the same on each cluster member node. The following procedures uses `grid` as the name of the Oracle software owner, and `dba` as the OSASM group. To create separate system privilege groups to separate administration privileges, complete group creation before you create the user Section 2.4.5, "Creating Job Role Separation Operating System Privileges Groups and Users," on page 2-9.

1. To create a grid installation owner account where you have an existing system privileges group (in this example, `dba`), whose members you want to have granted the `SYSASM` privilege to administer the Oracle ASM instance, enter a command similar to the following:

   ```
   # /usr/sbin/useradd -u 1100 -g oinstall -G dba grid
   ```

   In the preceding command:

- The -u option specifies the user ID. Using this command flag is optional, as you can allow the system to provide you with an automatically generated user ID number. However, you must make note of the user ID number of the user you create for Oracle grid infrastructure, as you require it later during preinstallation, and you must have the same user ID number for this user on all nodes of the cluster.

- The -g option specifies the primary group, which must be the Oracle Inventory group. For example: oinstall.

- The -G option specified the secondary group, which in this example is dba.

  The secondary groups must include the OSASM group, whose members are granted the SYSASM privilege to administer the Oracle ASM instance. You can designate a unique group for the SYSASM system privileges, separate from database administrator groups, or you can designate one group as the OSASM and OSDBA group, so that members of that group are granted the SYSASM and SYSDBA privileges to grant system privileges to administer both the Oracle ASM instances and Oracle Database instances. In code examples, this group is asmadmin.

  If you are creating this user to own both Oracle grid infrastructure and an Oracle Database installation, then this user must have the OSDBA for ASM group as a secondary group. In code examples, this group name is asmdba. Members of the OSDBA for ASM group are granted access to Oracle ASM storage. You must create an OSDBA for ASM group if you plan to have multiple databases accessing Oracle ASM storage, or you must use the same group as the OSDBA for all databases, and for the OSDBA for ASM group.

Use the usermod command to change existing user id numbers and groups.

For example:

```
# id oracle
uid=501(oracle) gid=501(oracle) groups=501(oracle)
# /usr/sbin/usermod -u 1001 -g 1000 -G 1000,1001 oracle
# id oracle
uid=1001(oracle) gid=1000(oinstall) groups=1000(oinstall),1001(oracle)
```

2. Set the password of the user that will own Oracle grid infrastructure. For example:

```
# passwd grid
```

3. Repeat this procedure on all of the other nodes in the cluster.

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, as 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.

2.4.4 Creating the Oracle Base Directory Path

The Oracle base directory for the grid installation owner is the location where diagnostic and administrative logs, and other logs associated with Oracle ASM and Oracle Clusterware are stored.

If you have created a path for the Oracle Clusterware home that is compliant with Oracle Optimal Flexible Architecture (OFA) guidelines for Oracle software paths then you do not need to create an Oracle base directory. When OUI finds an OFA-compliant path, it creates the Oracle base directory in that 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 (`oinstall`) group. The Optimal Flexible Architecture path for the Oracle base is `/u01/app/`*user*, where *user* is the name of the Oracle software installation owner. In addition, Oracle recommends that you create the grid home using the path `/u01/app/11.2.0/ `*user*, where *user* is the name of the Grid installation owner.

Oracle recommends that you create an Oracle base path manually, particularly if you have separate grid infrastructure for a cluster and Oracle Database software owners, so that you can separate log files.

For example:

```
# mkdir -p  /u01/app/11.2.0/grid/
# chown -R grid:oinstall /u01/
# chmod -R 775 /u01/
# mkdir -p /u01/app/oracle
# chown oracle:oinstall /u01/app/oracle
```

> **Note:** Placing Oracle grid infrastructure for a cluster binaries on a cluster file system is not supported.

2.4.5 Creating Job Role Separation Operating System Privileges Groups and Users

A Job Role Separation privileges configuration of Oracle ASM is a configuration with groups and users that divide administrative access privileges to the Oracle ASM installation from other administrative privileges users and groups associated with other Oracle installations. Administrative privileges access is granted by membership in separate operating system groups, and installation privileges are granted by using different installation owners for each Oracle installation.

> **Note:** This configuration is optional, to restrict user access to Oracle software by responsibility areas for different administrator users.

If you prefer, you can allocate operating system user privileges so that you can use one administrative user and one group for operating system authentication for all system privileges on the storage and database tiers.

For example, you can designate the `oracle` user to be the installation owner for all Oracle software, and designate `oinstall` to be the group whose members are granted all system privileges for Oracle Clusterware, Automatic Storage Management, and all Oracle Databases on the servers, and all privileges as installation owners. This group must also be the Oracle Inventory group.

Oracle recommends that you use at least two groups: A system privileges group whose members are granted administrative system privileges, and an installation owner group (the oraInventory group) to provide separate installation privileges the `OINSTALL` privilege. To simplify using the defaults for Oracle tools such as Cluster Verification Utility, if you do choose to use a single operating system group to grant all system privileges and the right to write to the oraInventory, then that group name should be `oinstall`.

- Overview of Creating Job Role Separation Groups and Users
- Creating Database Groups and Users with Job Role Separation

> **Note:** To use a directory service, such as Network Information Services (NIS), refer to your operating system documentation for further information.

2.4.5.1 Overview of Creating Job Role Separation Groups and Users

This section provides an overview of how to create users and groups to use Job Role Separation. Log in as `root` to create these groups and users.

- Users for Oracle Installations with Job Role Separation
- Database Groups for Job Role Separation Installations
- ASM Groups for Job Role Separation Installations

2.4.5.1.1 Users for Oracle Installations with Job Role Separation Oracle recommends that you create the following operating system groups and users for all installations where you create separate software installation owners:

One software owner to own each Oracle software product (typically, `oracle`, for the database software owner user, and `grid` for Oracle grid infrastructure.

You must create at least one software owner the first time you install Oracle software on the system. This user owns the Oracle binaries of the Oracle grid infrastructure software, and you can also make this user the owner of the Oracle Database or Oracle RAC binaries.

Oracle software owners must have the Oracle Inventory group as their primary group, so that each Oracle software installation owner can write to the central inventory (`oraInventory`), and so that OCR and Oracle Clusterware resource permissions are set correctly. The database software owner must also have the OSDBA group and (if you create it) the OSOPER group as secondary groups. In Oracle documentation, when Oracle software owner users are referred to, they are called `oracle` users.

Oracle recommends that you create separate software owner users to own each Oracle software installation. Oracle particularly recommends that you do this if you intend to install multiple databases on the system.

In Oracle documentation, a user created to own the Oracle grid infrastructure binaries is called the `grid` user. This user owns both the Oracle Clusterware and Oracle Automatic Storage Management binaries.

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

2.4.5.1.2 Database Groups for Job Role Separation Installations The following operating system groups and user are required if you are installing Oracle Database:

- The OSDBA group (typically, `dba`)

  You must create this group the first time you install Oracle Database software on the system. This group identifies operating system user accounts that have database administrative privileges (the `SYSDBA` privilege). If you do not create separate OSDBA, OSOPER and OSASM groups for the Oracle ASM instance, then

operating system user accounts that have the `SYSOPER` and `SYSASM` privileges must be members of this group. The name used for this group in Oracle code examples is `dba`. 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.

To specify a group name other than the default `dba` group, then you must choose the Advanced installation type to install the software or start Oracle Universal Installer (OUI) as a user that is not a member of this group. In this case, OUI prompts you to specify the name of this group.

Members of the OSDBA group formerly were granted `SYSASM` privileges on Oracle ASM instances, including mounting and dismounting disk groups. This privileges grant is removed with 11*g* release 2, if different operating system groups are designated as the OSDBA and OSASM groups. If the same group is used for both OSDBA and OSASM, then the privilege is retained.

- The OSOPER group for Oracle Database (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). By default, members of the OSDBA group also have all privileges granted by the `SYSOPER` privilege.

  To use the OSOPER group to create a database administrator group with fewer privileges than the default `dba` group, then you must choose the Advanced installation type to install the software or start OUI as a user that is not a member of the `dba` group. In this case, OUI prompts you to specify the name of this group. The usual name chosen for this group is `oper`.

2.4.5.1.3 ASM Groups for Job Role Separation Installations `SYSASM` is a new system privilege that enables the separation of the Oracle ASM storage administration privilege from SYSDBA. With Oracle Automatic Storage Management 11*g* release 2 (11.2), members of the database OSDBA group are not granted `SYSASM` privileges, unless the operating system group designated as the OSASM group is the same group designated as the OSDBA group.

Select separate operating system groups as the operating system authentication groups for privileges on Oracle ASM. Before you start OUI, create the following groups and users for Oracle ASM

- The Oracle Automatic Storage Management Group (typically `asmadmin`)

  This is a required group. Create this group as a separate group if you want to have separate administration privilege groups for Oracle ASM and Oracle Database administrators. In Oracle documentation, the operating system group whose members are granted privileges is called the OSASM group, and in code examples, where there is a group specifically created to grant this privilege, it is referred to as `asmadmin`.

  If you have multiple databases on your system, and use multiple OSDBA groups so that you can provide separate SYSDBA privileges for each database, then you should create a separate OSASM group, and use a separate user from the database users to own the grid infrastructure installation (Oracle Clusterware and Oracle ASM). 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 disk groups, and other storage administration tasks. `SYSASM` privileges provide no access privileges on an RDBMS instance.

- The ASM Database Administrator group (OSDBA for ASM, typically `asmdba`)

Members of the ASM Database Administrator group (OSDBA for ASM) are granted read and write access to files managed by Oracle ASM. The grid infrastructure installation owner and all Oracle Database software owners must be a member of this group, and all users with OSDBA membership on databases that have access to the files managed by Oracle ASM must be members of the OSDBA group for ASM.

- Members of the ASM Operator Group (OSOPER for 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 ASM 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.

  To use the ASM Operator group to create an ASM administrator group with fewer privileges than the default `asmadmin` group, then you must choose the Advanced installation type to install the software, In this case, OUI prompts you to specify the name of this group. In code examples, this group is `asmoper`.

  If you want to have an OSOPER for ASM group, then the grid infrastructure for a cluster software owner must be a member of this group.

2.4.5.2 Creating Database Groups and Users with Job Role Separation

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

- Creating the OSDBA Group to Prepare for Database Installations

- Creating an OSOPER Group for Database Installations

- Creating the OSASM Group

- Creating the OSOPER for ASM Group

- Creating the OSDBA for ASM Group for Database Access to Oracle ASM

- When to Create the Oracle Software Owner User

- Determining if an Oracle Software Owner User Exists

- Creating an Oracle Software Owner User

- Modifying an Existing Oracle Software Owner User

- Creating Identical Database Users and Groups on Other Cluster Nodes

2.4.5.2.1 Creating the OSDBA Group to Prepare for Database Installations If you intend to install Oracle Database to use with the grid infrastructure installation, then 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 Database 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 Database installation

If the OSDBA group does not exist, or if you require a new OSDBA group, then create it as follows. Use the group name `dba` unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 1200 dba
```

2.4.5.2.2 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. 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 Database 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, then create it as follows. Use the group name `oper` unless a group with that name already exists.

```
# /usr/sbin/groupadd -g 1201 oper
```

2.4.5.2.3 Creating the OSASM Group If the OSASM group does not exist or if you require a new OSASM group, then create it as follows. Use the group name `asmadmin` unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 1000 asmadmin
```

2.4.5.2.4 Creating the OSOPER for ASM Group Create an OSOPER for ASM group if you want to identify a group of operating system users, such as database administrators, whom you want to grant a limited set of Oracle ASM storage tier administrative privileges, including the ability to start up and shut down the Oracle ASM storage. For most installations, it is sufficient to create only the OSASM group, and provide that group as the OSOPER for ASM group during the installation interview.

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

```
# /usr/sbin/groupadd -g 1301 asmoper
```

2.4.5.2.5 Creating the OSDBA for ASM Group for Database Access to Oracle ASM You must create an OSDBA for ASM group to provide access to the Oracle ASM instance. This is necessary if OSASM and OSDBA are different groups.

If the OSDBA for ASM group does not exist or if you require a new OSDBA for ASM group, then create it as follows. Use the group name `asmdba` unless a group with that name already exists:

```
# /usr/sbin/groupadd -g 1300 asmdba
```

2.4.5.2.6 When to Create the Oracle Software Owner User You must create an Oracle software owner user in the following circumstances:

- 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 Database 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 Database software, such as `oracle`.

2.4.5.2.7 Determining if an Oracle Software Owner User Exists To determine whether an Oracle software owner user named `oracle` or `grid` exists, enter a command similar to the following (in this case, to determine if `oracle` exists):

```
# id oracle
```

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

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

Determine whether you want to use the existing user, or create another user. To use the existing user, then ensure that the user's primary group is the Oracle Inventory group and that it is a member of the appropriate OSDBA and OSOPER groups. Refer to one of the following sections for more information:

- To modify an existing user, refer to Section 2.4.5.2.9, "Modifying an Existing Oracle Software Owner User," on page 2-14.

- To create a user, refer to the following section.

> **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, as 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.

2.4.5.2.8 Creating an Oracle Software Owner User If the Oracle software owner user does not exist, or if you require a new Oracle software owner user, then create it as follows. 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 1101 -g oinstall -G dba,asmdba oracle
   ```

   In the preceding command:

   - The -u option specifies the user ID. Using this command flag is optional, as you can allow the system to provide you with an automatically generated user ID number. However, you must make note of the `oracle` user ID number, as you require it later 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, the OSDBA for ASM group, and, if required, the OSOPER for ASM group. For example: `dba, asmdba,` or `dba, asmdba, asmoper`

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

   ```
   # passwd oracle
   ```

2.4.5.2.9 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 OSDBA for ASM groups, then enter a command similar to the following to modify it. Specify the primary group using the `-g` option and any required secondary group using the `-G` option:

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

Repeat this procedure on all of the other nodes in the cluster.

2.4.5.2.10 Creating Identical Database Users and Groups on Other Cluster Nodes

> **Note:** You must complete the following procedures only if you are
> using local users and groups. If you are using users and groups
> defined in a directory service such as NIS, then they are already
> identical on each cluster node.

Oracle software owner users and the Oracle Inventory, OSDBA, and OSOPER groups
must exist and be identical on all cluster nodes. To create these identical users and
groups, you must identify the user ID and group IDs assigned them on the node
where you created them, and then create the user and groups with the same name and
ID on the other cluster nodes.

Identifying Existing User and Group IDs

To determine the user ID (UID) of the `grid` or `oracle` users, and the group IDs (GID)
of the existing Oracle groups, follow these steps:

1. Enter a command similar to the following (in this case, to determine a user ID for
   the `oracle` user):

   ```
   # id oracle
   ```

   The output from this command is similar to the following:

   ```
   uid=502(oracle) gid=501(oinstall) groups=502(dba),503(oper),506(asmdba)
   ```

2. From the output, identify the user ID (UID) for the user and the group identities
   (GIDs) for the groups to which it belongs. Ensure that these ID numbers are
   identical on each node of the cluster. The user's primary group is listed after `gid`.
   Secondary groups are listed after `groups`.

Creating Users and Groups on the Other Cluster Nodes

To create users and groups on the other cluster nodes, repeat the following procedure
on each node:

1. Log in to the next cluster node as `root`.

2. Enter commands similar to the following to create the `oinstall`, `asmadmin`, and
   `asmdba` groups, and if required, the `asmoper`, `dba`, and `oper` groups. Use the `-g`
   option to specify the correct GID for each group.

   ```
   # /usr/sbin/groupadd -g 1000 oinstall
   # /usr/sbin/groupadd -g 1100 asmadmin
   # /usr/sbin/groupadd -g 1200 dba
   # /usr/sbin/groupadd -g 1201 oper
   # /usr/sbin/groupadd -g 1300 asmdba
   # /usr/sbin/groupadd -g 1301 asmoper
   ```

   > **Note:** If the group already exists, then use the `groupmod` command
   > to modify it if necessary. If you cannot use the same group ID for a
   > particular group on this node, then view the `/etc/group` file on all
   > nodes to identify a group ID that *is* available on every node. You must
   > then change the group ID on all nodes to the same group ID.

3. To create the oracle or grid infrastructure (grid) user, enter a command similar to the following (in this example, to create the oracle user):

   ```
   # /usr/sbin/useradd -u 1100 -g oinstall -G asmdba,dba oracle
   ```

   In the preceding command:

   - The -u option specifies the user ID, which must be the user ID that you identified in the previous subsection

   - 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 can include the OSASM, OSDBA, OSDBA for ASM, and OSOPER or OSOPER for ASM groups. For example:

     - A grid installation owner: OSASM (asmadmin), whose members are granted the SYSASM privilege

     - An Oracle Database installation owner without SYSASM privileges access: OSDBA (dba), OSDBA for ASM (asmdba), OSOPER for ASM (asmoper)

   > **Note:** If the user already exists, then use the usermod command to modify it if necessary. If you cannot use the same user ID for the user on every node, then view the /etc/passwd file on all nodes to identify a user ID that *is* available on every node. You must then specify that ID for the user on all of the nodes.

4. Set the password of the user. For example:

   ```
   # passwd oracle
   ```

5. Complete user environment configuration tasks for each user as described in the section Configuring Grid Infrastructure Software Owner User Environments on page 2-29.

2.5 Checking the Hardware Requirements

- Select servers with the same chip architecture; running 32-bit and 64-bit Oracle software versions in the same cluster stack is not supported.

- Ensure that the server is started with run level 3 or run level 5.

- Ensure servers run the same operating system binary and the same processor architecture. Oracle grid infrastructure installations and Oracle Real Application Clusters (Oracle RAC) support servers with different hardware in the same cluster.

Each system must meet the following minimum hardware requirements:

- At least 4 GB of physical RAM.

- At least 1024 x 768 display resolution, so that Oracle Universal Installer (OUI) displays correctly

- Swap space equivalent to the multiple of the available RAM, as indicated in the following table:

Table 2–1   Swap Space Required as a Multiple of RAM

Available RAM	Swap Space Required
Between 4 GB and 8 GB	2 times the size of RAM
Between 8 GB and 32 GB	1.5 times the size of RAM
More than 32 GB	32 GB

- 1 GB of space in the /tmp directory

- 5 GB of space for the grid infrastructure for a cluster home (Grid home) This includes Oracle Clusterware and Automatic Storage Management (ASM) files and log files.

- 8.2 GB of space for Oracle Database binaries, if planned.

- 2.72 GB for Enterprise Edition data files, or 2.76 for Enterprise Edition and custom install options.

If you are installing Oracle Database, then you require additional space, either on a file system or in an Automatic Storage Management disk group, for the Fast Recovery Area if you choose to configure automated database backups.

> **See Also:**   *Oracle Database Storage Administrator's Guide*

To ensure that each system meets these requirements, follow these steps:

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

    On HP PA-RISC systems:

    ```
    # grep "Physical:" /var/adm/syslog/syslog.log
    ```

    On HP Itanium systems:

    ```
    # /usr/contrib/bin/machinfo  | grep -i Memory
    ```

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

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

    ```
    # /usr/sbin/swapinfo -a
    ```

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

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

    ```
    # bdf /tmp
    ```

    If there is less than 1 GB of disk space available in the /tmp directory, then complete one of the following steps:

    - Delete unnecessary files from the /tmp directory to make available the disk space required.

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

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

```
# bdf
```

2.6 Checking the Network Requirements

Review the following sections to check that you have the networking hardware and internet protocol (IP) addresses required for an Oracle Real Application Clusters (Oracle RAC) installation:

- Network Hardware Requirements
- IP Address Requirements
- DNS Configuration for Domain Delegation to Grid Naming Service
- Grid Naming Service Configuration Example
- Manual IP Address Configuration Example
- Network Interface Configuration Options
- Node Time Requirements
- Configuring the Name Service Switch to Tolerate Public Network Failures

> **Note:** For the most up-to-date information about supported network protocols and hardware for Oracle RAC installations, refer to the Certify pages on the My Oracle Support Web site at the following URL:
>
> https://metalink.oracle.com

2.6.1 Network Hardware Requirements

The following is a list of requirements for network configuration:

- Each node must have at least two ports: one for the public network interface, and one for the private network interface (the interconnect).

  If you want to use more than one NIC for the public network or for the private network, then Oracle recommends that you use NIC bonding.

- The public interface names associated with the network adapters for each network must be the same on all nodes, and the private interface names associated with the network adaptors should be the same on all nodes.

  For example: With a two-node cluster, you cannot configure network adapters on node1 with lan0 as the public interface, but on node2 have lan1 as the public interface. Public interface names must be the same, so you must configure lan0 as public on *both* nodes. You should configure the private interfaces on the same network adapters as well. If lan1 is the private interface for node1, then lan1 should be the private interface for node2.

- For the public network, each network adapter must support TCP/IP.

- For the private network, the interconnect must support the user datagram protocol (UDP) using high-speed network adapters and switches that support TCP/IP (Gigabit Ethernet or better required).

> **Note:** UDP is the default interconnect protocol for Oracle RAC, and TCP is the interconnect protocol for Oracle Clusterware. You must use a switch for the interconnect. Oracle recommends that you use a dedicated switch.
>
> Oracle does not support token-rings or crossover cables for the interconnect.

- For the private network, the endpoints of all designated interconnect interfaces must be completely reachable on the network. There should be no node that is not connected to every private network interface. You can test whether an interconnect interface is reachable using a `ping` command.

2.6.2 IP Address Requirements

Before starting the installation, you must have at least two interfaces configured on each node: One for the private IP address and one for the public IP address.

You can configure IP addresses with one of the following options:

- Dynamic IP address assignment using Oracle Grid Naming Service (GNS). If you select this option, then network administrators assign static IP address for the physical hostname and dynamically allocated IPs for the Oracle Clusterware managed VIP addresses. In this case, IP addresses for the VIPs are assigned by a DHCP and resolved using a multicast domain name server configured as part of Oracle Clusterware within the cluster. If you plan to use GNS, then you must have the following:

  - A DHCP service running on the public network for the cluster

  - Enough addresses on the DHCP to provide 1 IP address for each node's virtual IP, and 3 IP addresses for the cluster used by the Single Client Access Name (SCAN) for the cluster

- Static IP address assignment. If you select this option, then network administrators assign a fixed IP address for each physical hostname in the cluster and for IPs for the Oracle Clusterware managed VIPs. In addition, domain name server (DNS) based static name resolution is used for each node. Selecting this option requires that you request network administration updates when you modify the cluster.

  > **Note:** Oracle recommends that you use a static hostname for all server node public hostnames.
  >
  > Public IP addresses and virtual IP addresses must be in the same subnet.

2.6.2.1 IP Address Requirements with Grid Naming Service

If you enable Grid Naming Service (GNS), then name resolution requests to the cluster are delegated to the GNS, which is listening on the GNS virtual IP address. You define this address in the DNS domain before installation. The DNS must be configured to delegate resolution requests for cluster names (any names in the subdomain delegated to the cluster) to the GNS. When a request comes to the domain, GNS processes the requests and responds with the appropriate addresses for the name requested.

To use GNS, before installation the DNS administrator must establish DNS Lookup to direct DNS resolution of a subdomain to the cluster. If you enable GNS, then you must

have a DHCP service on the public network that allows the cluster to dynamically allocate the virtual IP addresses as required by the cluster.

> **Note:**   If you have vendor clusterware installed, then you cannot choose to use GNS, because the vendor clusterware does not support it.

2.6.2.2 IP Address Requirements for Manual Configuration

If you do not enable GNS, then the public and virtual IP addresses for each node must be static IP addresses, configured before installation for each node, but not currently in use. Public and virtual IP addresses must be on the same subnet.

Oracle Clusterware manages private IP addresses in the private subnet on interfaces you identify as private during the installation interview.

The cluster must have the following addresses configured:

- A public IP address for each node

- A virtual IP address for each node

- A single client access name (SCAN) configured on the domain name server (DNS) for Round Robin resolution to three addresses (recommended) or at least one address.

The single client access name (SCAN) is a name used to provide service access for clients to the cluster. Because the SCAN is associated with the cluster as a whole, rather than to a particular node, the SCAN makes it possible to add or remove nodes from the cluster without needing to reconfigure clients. It also adds location independence for the databases, so that client configuration does not have to depend on which nodes are running a particular database. Clients can continue to access the cluster in the same way as with previous releases, but Oracle recommends that clients accessing the cluster use the SCAN.

The SCAN addresses must be on the same subnet as virtual IP addresses and public IP addresses. For high availability and scalability, Oracle recommends that you configure the SCAN to use Round Robin resolution to three addresses. The name for the SCAN cannot begin with a numeral. For installation to succeed, the SCAN must resolve to at least one address.

> **Note:**   Oracle strongly recommends that you do not configure SCAN VIP addresses in the hosts file. Use DNS resolution for SCAN VIPs. If you use the hosts file to resolve SCANs, then you will only be able to resolve to one IP address and you will have only one SCAN address.

> **See Also:**   Appendix C, "Oracle Grid Infrastructure for a Cluster Installation Concepts" for more information about network addresses

2.6.3 DNS Configuration for Domain Delegation to Grid Naming Service

If you plan to use GNS, then before grid infrastructure installation, you must configure your domain name server (DNS) to send to GNS name resolution requests for the subdomain GNS serves, which are the cluster member nodes.

You must configure the DNS to send GNS name resolution requests using delegation. Configure delegation using the following procedure:

1. In the DNS, create an entry for the GNS virtual IP address. For example:

   ```
   gns-server.clustername.com: 192.0.2.1
   ```

   The address you provide must be routable.

2. In the DNS, create an entry similar to the following for the delegated domain, where `clusterdomain.example.com` is the subdomain you want to delegate:

   ```
   clusterdomain.example.com: NS gns-server.clustername.com
   ```

   When using GNS, you must configure the `resolve.conf` on the nodes in the cluster to contain name server entries that are resolvable to corporate DNS servers. The total timeout period configured—a combination of options attempts (retries) and options timeout (exponential backoff)—should be less than 30 seconds. For example, where xxx.xxx.xxx.42 and xxx.xxx.xxx.15 are valid name server addresses in your network, provide an entry similar to the following in `/etc/resolv.conf`:

   ```
   options attempts: 2
   options timeout: 1

   search clusterdomain.example.com example.com
   nameserver xxx.xxx.xxx.42
   nameserver xxx.xxx.xxx.15
   ```

   `/etc/nsswitch.conf` controls name service lookup order. In some system configurations, the Network Information System (NIS) can cause problems with Oracle SCAN address resolution. Oracle recommends that you place the `nis` entry at the end of the search list. For example:

   ```
   /etc/nsswitch.conf
       hosts:    files   dns   nis
   ```

2.6.4 Grid Naming Service Configuration Example

If you use GNS, then you need to specify a static IP address for the GNS VIP address, and delegate a subdomain to be delegated to that static GNS IP address.

As nodes are added to the cluster, your organization's DHCP server can provide addresses for these nodes dynamically. These addresses are then registered automatically in GNS, and GNS provides resolution within the subdomain to cluster node addresses registered with GNS.

Because allocation and configuration of addresses is performed automatically with GNS, no further configuration is required. Oracle Clusterware provides dynamic network configuration as nodes are added to or removed from the cluster. The following example is provided only for information.

With a two node cluster where you have defined the GNS VIP, after installation you might have a configuration similar to the following for a two-node cluster, where the cluster name is `mycluster`, the GNS parent domain is `example.com`, the subdomain is `grid.example.com`, 192.0.2 in the IP addresses represent the cluster public IP address network, and 192.168.0 represents the private IP address subnet:

Table 2–2   Grid Naming Service Example Network

Identity	Home Node	Host Node	Given Name	Type	Address	Address Assigned By	Resolved By
GNS VIP	None	Selected by Oracle Clusterware	mycluster-gns.example.com	virtual	192.0.2.1	Fixed by net administrator	DNS
Node 1 Public	Node 1	node1	node1[1]	Public	192.0.2.101	Fixed	GNS
Node 1 VIP	Node 1	Selected by Oracle Clusterware	node1-vip	Virtual	192.0.2.104	DHCP	GNS
Node 1 Private	Node 1	node1	node1-priv	Private	192.168.0.1	Fixed or DHCP	GNS
Node 2 Public	Node 2	node2	node2[1]	Public	192.0.2.102	Fixed	GNS
Node 2 VIP	Node 2	Selected by Oracle Clusterware	node2-vip	Virtual	192.0.2.105	DHCP	GNS
Node 2 Private	Node 2	node2	node2-priv	Private	192.168.0.2	Fixed or DHCP	GNS
SCAN VIP 1	none	Selected by Oracle Clusterware	mycluster-scan.grid.example.com	virtual	192.0.2.201	DHCP	GNS
SCAN VIP 2	none	Selected by Oracle Clusterware	mycluster-scan.grid.example.com	virtual	192.0.2.202	DHCP	GNS
SCAN VIP 3	none	Selected by Oracle Clusterware	mycluster-scan.grid.example.com	virtual	192.0.2.203	DHCP	GNS

[1] Node hostnames may resolve to multiple addresses, including any private IP addresses or VIP addresses currently running on that host.

2.6.5 Manual IP Address Configuration Example

If you choose not to use GNS, then before installation you must configure public, virtual, and private IP addresses. Also, check that the default gateway can be accessed by a ping command. To find the default gateway, use the route command, as described in your operating system's help utility.

For example, with a two node cluster where each node has one public and one private interface, and you have defined a SCAN domain address to resolve on your DNS to one of three IP addresses, you might have the configuration shown in the following table for your network interfaces:

Table 2–3   Manual Network Configuration Example

Identity	Home Node	Host Node	Given Name	Type	Address	Address Assigned By	Resolved By
Node 1 Public	Node 1	node1	node1[1]	Public	192.0.2.101	Fixed	DNS
Node 1 VIP	Node 1	Selected by Oracle Clusterware	node1-vip	Virtual	192.0.2.104	Fixed	DNS and hosts file
Node 1 Private	Node 1	node1	node1-priv	Private	192.168.0.1	Fixed	DNS and hosts file, or none
Node 2 Public	Node 2	node2	node2[1]	Public	192.0.2.102	Fixed	DNS
Node 2 VIP	Node 2	Selected by Oracle Clusterware	node2-vip	Virtual	192.0.2.105	Fixed	DNS and hosts file
Node 2 Private	Node 2	node2	node2-priv	Private	192.168.0.2	Fixed	DNS and hosts file, or none
SCAN VIP 1	none	Selected by Oracle Clusterware	mycluster-scan	virtual	192.0.2.201	Fixed	DNS
SCAN VIP 2	none	Selected by Oracle Clusterware	mycluster-scan	virtual	192.0.2.202	Fixed	DNS
SCAN VIP 3	none	Selected by Oracle Clusterware	mycluster-scan	virtual	192.0.2.203	Fixed	DNS

[1] Node hostnames may resolve to multiple addresses.

You do not need to provide a private name for the interconnect. If you want name resolution for the interconnect, then you can configure private IP names in the hosts file or the DNS. However, Oracle Clusterware assigns interconnect addresses on the interface defined during installation as the private interface (lan1, for example), and to the subnet used for the private subnet.

The addresses to which the SCAN resolves are assigned by Oracle Clusterware, so they are not fixed to a particular node. To enable VIP failover, the configuration shown in the preceding table defines the SCAN addresses and the public and VIP addresses of both nodes on the same subnet, 192.0.2.

> **Note:**   All host names must conform to the RFC 952 standard, which permits alphanumeric characters. Host names using underscores ("_") are not allowed.

2.6.6 Network Interface Configuration Options

The precise configuration you choose for your network depends on the size and use of the cluster you want to configure, and the level of availability you require.

If certified Network-attached Storage (NAS) is used for Oracle RAC and this storage is connected through Ethernet-based networks, then you must have a third network

interface for NAS I/O. Failing to provide three separate interfaces in this case can cause performance and stability problems under load.

2.6.7 Node Time Requirements

Before starting the installation, ensure that each member node of the cluster is set as closely as possible to the same date and time. Oracle strongly recommends using the Network Time Protocol feature of most operating systems for this purpose, with all nodes using the same reference Network Time Protocol server.

2.6.8 Configuring the Name Service Switch to Tolerate Public Network Failures

On HP-UX, if you do not use Grid Naming Service, then to tolerate a complete public network failure, you should specify network addresses in `/etc/nsswitch.conf`, to avoid VIP failover or public address network failure response times being dependent on the network timeouts.

In the `/etc/nsswitch.conf` file, `files` must precede other entries for `host`, and preferably precede other entries in `nsswitch.conf`.

2.7 Identifying Software Requirements

Depending on the products that you intend to install, verify that the following software is installed on the system. The procedure following the table describes how to check these requirements.

> **Note:** Oracle Universal Installer performs checks on your system to verify that it meets the listed requirements. To ensure that these checks pass, verify the requirements before you start Oracle Universal Installer.
>
> The parameters in the following table are minimum patch revisions required for installation; later patch revisions are not tested, but are expected to work. There may be more recent versions of the patches listed installed on the system. If a listed patch is not installed, then determine if a more recent version is installed before installing the version listed. The installer will check for superseding patches.

The following is the list of supported HP-UX platforms and requirements at the time of release:

- Software Requirements List for HP-UX Itanium Platforms
- Software Requirements List for HP-UX PA-RISC (64-bit)

2.7.1 Software Requirements List for HP-UX Itanium Platforms

Table 2–4   HP-UX Itanium Requirements

Item	Requirement
Operating system	■　HP-UX 11iV3 patch Bundle Sep/ 2008 (B.11.31.0809.326a)

Table 2–4   (Cont.) HP-UX Itanium Requirements

Item	Requirement

HP-UX 11.31 packages and bundles	`PHCO_40381 11.31 Disk Owner Patch`
	`PHKL_38038 vm cumulative patch`
	`PHKL_38938 11.31 SCSI cumulative I/O patch`
	`PHKL_39351  Scheduler patch : post wait hang`
	`PHSS_36354 11.31 assembler patch`
	`PHSS_37042  11.31 hppac (packed decimal)`
	`PHSS_37959  Libcl patch for alternate stack issue fix`
	`(QXCR1000818011)`
	`PHSS_39094 11.31 linker + fdp cumulative patch`
	`PHSS_39100 11.31 Math Library Cumulative Patch`
	`PHSS_39102 11.31 Integrity Unwind Library`
	`PHSS_38141 11.31 aC++ Runtime`

Oracle Clusterware	**All HP-UX 11.31 installations** No additional requirements for Oracle Clusterware. At the time of this release, Hyper Messaging Protocol (HMP) is not supported. Only HP Serviceguard A.11.19 is supported with Oracle Clusterware 11*g* release 2 (11.2). **Note:** HP Serviceguard is optional. It is required only if you want to use shared logical volumes for Oracle Clusterware or database files.
Oracle JDBC/OCI Drivers	■ HPUX JDK 1. 6.0.05 ■ HPUX JDK 5.0.15
Oracle Messaging Gateway	Oracle Messaging Gateway supports the integration of Oracle Streams Advanced Queuing (AQ) with the following software: IBM MQ Series V. 6.0, client and server ■ MQSERIES.MQM-CL-HPUX ■ MQSERIES.MQM-SERVER TIBCO Rendezvous 7.2 If you require a CSD for WebSphere MQ, then refer to the following Web site for download and installation information: `http://www-306.ibm.com/software/integration/wmq/support`
Oracle ODBC	The Oracle ODBC driver on HP UX Itanium is certified with ODBC Driver Manager 2.2.14. You can download and install the Driver Manager from the following URL: `http://www.unixodbc.org` You do not require ODBC Driver Manager to install Oracle Databases. To use ODBC, you must also install gcc 3.4.5 or later.
VERITAS File System	PHKL_39773: 11.31 VRTS 5.0 GARP6 VRTSvxfs Kernel Patch **Note:** This patch is required only if you want to use a VERITAS File System 5.0.

2.7.2 Software Requirements List for HP-UX PA-RISC (64-bit)

Table 2–5   HP-UX PA-RISC (64-bit) Requirements

Item	Requirement
Operating system	■ HP-UX 11iV3 (11.31) patch Bundle Sep/ 2008 (B.11.31.0809.326a)
HP-UX 11.31 packages and bundles	`PHKL_39773` (11.31 VRTS 5.0 GARP6 VRTSvxfs Kernel Patch. This patch is needed only when VxFS 5.0 is installed. The patch has no other dependencies. It is included in the September 2009 update of HP-UX 11.31.) `PHCO_40381` (64 BIT DISKOWNER PATCH - lvmchk funtionality) `PHKL_38038` - VM patch - hot patching/Core file creation directory `PHKL_38938` (11.31 SCSI cumulative I/O patch) `PHKL_39351` (11.31 scheduler cumulative patch `PHSS_37959` (Libcl patch for alternate stack issue fix (QXCR1000818011) `PHSS_38141` (11.31 aC++ Runtime) `PHSS_39094` (11.31 linker + fdp cumulative patch)
C/C++ Compiler Patches for Pro*C/C++, Oracle Call Interface, Oracle C++ Call Interface, and Oracle XML Developer's Kit (XDK) with Oracle Database 11*g* release 2 (11.2)	C++ compiler ■ aC++ A.03.85 (Swlist Bundle - C.11.31.04) - September 2008 C Compiler ■ HP ANSI C B.11.31.04 (Swlist Bundle - C.11.31.04) - September 2008 C Compiler Patches ■ PHSS_39080 Gcc Compiler ■ Gcc 4.2.3
COBOL (optional)	Micro Focus Server Express 5.1
Oracle Clusterware	**All HP-UX 11.31 installations** No additional requirements for Oracle Clusterware. At the time of this release, Hyper Messaging Protocol (HMP) is not supported. Only HP Serviceguard A.11.19 is supported with Oracle Clusterware 11*g* release 2 (11.2). **Note:** HP Serviceguard is optional. It is required only if you want to use shared logical volumes for Oracle Clusterware or database files.

Table 2–5   (Cont.) HP-UX PA-RISC (64-bit) Requirements

Item	Requirement
Oracle Messaging Gateway (optional)	Oracle Messaging Gateway supports the integration of Oracle Streams Advanced Queuing (AQ) with the following software:
	IBM MQ Series V. 6.0, client and server
	■ MQSERIES.MQM-CL-HPUX
	■ MQSERIES.MQM-SERVER
	TIBCO Rendezvous 7.2
	If you require a CSD for WebSphere MQ, then refer to the following Web site for download and installation information:
	http://www-306.ibm.com/software/integration/wmq/support
Oracle ODBC	At the time of this release, Oracle ODBC is not supported for HP-UX on PA-RISC.
Oracle JDBC/OCI Drivers	■ HPUX JDK 1. 6.0.05
	■ HPUX JDK 5.0.15

2.8 Checking the Software Requirements

To ensure that the system meets these requirements, follow these steps:

1. To determine which version of HP-UX is installed, enter the following command:

```
# uname -a
"HP-UX hostname B.11.31 U ia64 4156074294 unlimited-user license"
```

In this example, the version of HP-UX 11i is 11.31.

2. Verify that the system meets the minimum patch bundle requirements using the following command:

```
# /usr/sbin/swlist -l bundle |grep QPK
```

The QPK (Quality Pack) bundles have version numbers of the form B.11.31.0809.326a (for the September 2008 release), B.11.31.0903.334a (for the March 2009 release), and so on. If a required bundle, product, or fileset is not installed, then you must install it. Refer to your operating system or software documentation for information about installing products.

3. If a required patch is not installed, then download it from the following Web site and install it:

```
http://itresourcecenter.hp.com
```

If the Web site shows a more recent version of the patch, then download and install that version.

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

```
http://www-306.ibm.com/software/
```

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

2.9 Network Time Protocol Setting

Oracle Clusterware 11*g* release 2 (11.2) requires time synchronization across all nodes within a cluster when Oracle RAC is deployed. You have two options for time synchronization: an operating system configured network time protocol (NTP), or Oracle Cluster Time Synchronization Service. Oracle Cluster Time Synchronization Service is designed for organizations whose cluster servers are unable to access NTP services. If you use NTP, then the Oracle Cluster Time Synchronization daemon (ctssd) starts up in observer mode. If you do not have NTP daemons, then `ctssd` starts up in active mode and synchronizes time among cluster members without contacting an external time server.

> **Note:** Before starting the installation of the grid infrastructure, Oracle recommends that you ensure the clocks on all nodes are set to the same time.

If you have NTP daemons on your server but you cannot configure them to synchronize time with a time server, and you want to use Cluster Time Synchronization Service to provide synchronization service in the cluster, then deactivate and deinstall the Network Time Protocol (NTP).

To deactivate the NTP service, you must stop the existing `ntpd` service, disable it from the initialization sequences and remove the `ntp.conf` file. To complete these steps, run the following commands as the `root` user

```
# /sbin/init.d/xntpd stop
# rm /etc/ntp.conf
```

or, `mv /etc/ntp.conf` to `/etc/ntp.conf.org`.

When the installer finds that the NTP protocol is not active, the Cluster Time Synchronization Service is installed in active mode and synchronizes the time across the nodes. If NTP is found configured, then the Cluster Time Synchronization Service is started in observer mode, and no active time synchronization is performed by Oracle Clusterware within the cluster.

To confirm that `ctssd` is active after installation, enter the following command as the Grid installation owner:

```
$ crsctl check ctss
```

If you are using NTP, and you prefer to continue using it instead of Cluster Time Synchronization Service, then you need to modify the NTP initialization file to enable slewing, which prevents time from being adjusted backward. Restart the network time protocol daemon after you complete this task.

To do this on HP-UX, open the file `/etc/rc.config.d/netdaemons` using a text editor, and add the line `export XNTPD_ARGS="-x"` to the file. After you add the `XNTPD_ARGS` line, load the setting by shutting down and restarting `xntpd` using the commands `/sbin/init.d/xntpd stop` and `/sbin/init.d/xntpd start`.

2.10 Automatic SSH Configuration During Installation

To install Oracle software, Secure Shell (SSH) connectivity must be set up between all cluster member nodes. OUI uses the `ssh` and `scp` commands during installation to run remote commands on and copy files to the other cluster nodes. You must configure SSH so that these commands do not prompt for a password.

> **Note:** SSH is used by Oracle configuration assistants for configuration operations from local to remote nodes. It is also used by Enterprise Manager.

You can configure SSH from the Oracle Universal Installer (OUI) interface during installation for the user account running the installation. The automatic configuration creates passwordless SSH connectivity between all cluster member nodes. Oracle recommends that you use the automatic procedure if possible.

To enable the script to run, you must remove `stty` commands from the profiles of any Oracle software installation owners, and remove other security measures that are triggered during a login, and that generate messages to the terminal. These messages, mail checks, and other displays prevent Oracle software installation owners from using the SSH configuration script that is built into the Oracle Universal Installer. If they are not disabled, then SSH must be configured manually before an installation can be run.

> **See Also:** Section 2.11.5, "Preventing Installation Errors Caused by stty Commands" for information about how to remove stty commands in user profiles

2.11 Configuring Grid Infrastructure Software Owner User Environments

You run the installer software with the Oracle grid infrastructure installation owner user account (`oracle` or `grid`). However, before you start the installer, you must configure the environment of the installation owner user account. Also, create other required Oracle software owners, if needed.

This section contains the following topics:

2.11.1 Environment Requirements for Oracle Grid Infrastructure Software Owner

You must make the following changes to configure the Oracle grid infrastructure software owner environment:

- Set the installation software owner user (`grid`, `oracle`) 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 644 permissions.

- Set ulimit settings for file descriptors and processes for the installation software owner (`grid`, `oracle`)

- Set the software owner's environment variable DISPLAY environment variables in preparation for the Oracle grid infrastructure installation

> **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.

2.11.2 Procedure for Configuring Oracle Software Owner Environments

To set the Oracle software owners' environments, follow these steps, for each software owner (`grid`, `oracle`):

1. Start a new terminal session; for example, start an X terminal (`xterm`).

2. Enter the following command to ensure that X Window applications can display on this system:

```
$ xhost + hostname
```

The *hostname* is the name of the local host.

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 software owner user.

4. If you are not logged in as the user, then switch to the software owner user you are configuring. For example, with the `grid` user:

```
$ su - grid
```

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

```
$ echo $SHELL
```

6. Open the user's shell startup file in any text editor:

   ■ Bourne shell (`sh`) or Korn shell (`ksh`):

   ```
   $ vi .profile
   ```

   ■ C shell (`csh` or `tcsh`):

   ```
   % vi .login
   ```

7. If the `ORACLE_SID`, `ORACLE_HOME`, or `ORACLE_BASE` environment variable is set in the file, then remove the appropriate lines from the file.

8. Save the file, and exit from the text editor.

9. To run the shell startup script, enter one of the following commands:

   ■ Bourne or Korn shell:

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

   ■ C shell:

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

10. If you are not installing the software on the local system, then enter a command similar to the following to direct X applications to display on the local system:

   ■ Bourne or Korn shell:

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

   ■ C shell:

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

   In this example, `local_host` is the host name or IP address of the system that you want to use to display OUI (your workstation or PC).

11. 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 `TEMP` and `TMPDIR` environment variables to specify a temporary directory on this file system:

> **Note:** You cannot use a shared file system as the location of the temporary file directory (typically /tmp) for Oracle RAC installation. If you place /tmp on a shared file system, then the installation fails.

   a. Use the `bdf` command to identify a suitable file system with sufficient free space.

   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:

```
$ su - root
# mkdir /mount_point/tmp
# chmod a+wr /mount_point/tmp
# exit
```

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

     * Bourne or Korn shell:

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

     * C shell:

```
% setenv TEMP /mount_point/tmp
% setenv TMPDIR /mount_point/tmp
```

12. Enter the following command to ensure that the ORACLE_HOME and TNS_ADMIN environment variables are not set:

■ Bourne 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, the 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, Oracle recommends that you unset the ORACLE_HOME environment variable and choose the default path suggested by the Installer.

2.11.3 Setting Resource Limits for the Oracle Software Installation Users

To improve the performance of the software on HP-UX systems, you must increase the following resource limits for the Oracle software owner users (`grid`, `oracle`):

Process Resource Shell Limit	Kctune Parameter	Hard Limit
Hard limit for the number of files that a process is allowed to have open simultaneously	`maxfiles_lim`	4096
Maximum size of the stack segment of the process	`maxssiz_64bit`	268435456
Maximum number of processes available to a single user	`nproc`	4200

Increase the shell limits as needed.

1. On each node, to increase the shell limits, on HP-UX use the `smh` tool (`/usr/sbin/smh`) to increase values as necessary, or use the command line tool tool /usr/sbin/kctune to display the current Kernel Tunables. To tune an individual parameter, use the following command syntax:

   ```
   /usr/sbin/kctune name=value
   ```

2. Depending on your shell environment, make the following changes to the default shell startup file, to change ulimit setting for all Oracle installation owners (note that these examples show the users `oracle` and `grid`):

   - For the Bourne, Bash, or Korn shell, add lines similar to the following to the `/etc/profile` file:

     ```
     if [ $USER = "oracle" ] || [ $USER = "grid" ]; then
             if [ $SHELL = "/bin/ksh" ]; then
                     ulimit -p 16384
                     ulimit -n 65536
             else
                     ulimit -u 16384 -n 65536
             fi
             umask 022
     fi
     ```

   - For the C shell (`csh` or `tcsh`), add the following lines to the `/etc/csh.login` file:

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

3. Repeat this procedure on all other nodes in the cluster, and for all Oracle software owners that you intend to use to install Oracle software.

2.11.4 Setting Display and X11 Forwarding Configuration

If you are on a remote terminal, and the local node has only one visual (which is typical), then use the following syntax to set the DISPLAY environment variable:

Bourne, Korn, and Bash shells

```
$ export DISPLAY=hostname:0
```

C shell:

```
$ setenv DISPLAY hostname:0
```

For example, if you are using the Bash shell, and if your hostname is `node1`, then enter the following command:

```
$ export DISPLAY=node1:0
```

To ensure that X11 forwarding will not cause the installation to fail, create a user-level SSH client configuration file for the Oracle software owner user, as follows:

1. Using any text editor, edit or create the software installation owner's `~/.ssh/config` file.

2. Make sure that the ForwardX11 attribute is set to `no`. For example:

```
Host *
      ForwardX11 no
```

2.11.5 Preventing Installation Errors Caused by stty Commands

During an Oracle grid infrastructure installation, OUI uses SSH to run commands and copy files to the other nodes. During the installation, hidden files on the system (for example, `.bashrc` or `.cshrc`) will cause makefile and other installation errors if they contain `stty` commands.

To avoid this problem, you must modify these files in each Oracle installation owner user home directory to suppress all output on STDERR, as in the following examples:

- Bourne, Bash, or Korn shell:

```
if [ -t 0 ]; then
   stty intr ^C
fi
```

- C shell:

```
test -t 0
if ($status == 0) then
   stty intr ^C
endif
```

> **Note:** When SSH is not available, the Installer uses the `rsh` and `rcp` commands instead of `ssh` and `scp`.
>
> If there are hidden files that contain `stty` commands that are loaded by the remote shell, then OUI indicates an error and stops the installation.

2.12 Creating Required Symbolic Links

> **Note:** This task is required only if the Motif 2.1 Development Environment package (X11MotifDevKit.MOTIF21-PRG) is not installed.

To enable you to successfully relink Oracle products after installing this software, enter the following commands to create required X library symbolic links in the `/usr/lib` directory:

```
# cd /usr/lib
```

```
# ln -s libX11.3 libX11.sl
# ln -s libXIE.2 libXIE.sl
# ln -s libXext.3 libXext.sl
# ln -s libXhp11.3 libXhp11.sl
# ln -s libXi.3 libXi.sl
# ln -s libXm.4 libXm.sl
# ln -s libXp.2 libXp.sl
# ln -s libXt.3 libXt.sl
# ln -s libXtst.2 libXtst.sl
```

2.13 Requirements for Creating an Oracle Clusterware Home Directory

During installation, you are prompted to provide a path to a home directory to store Oracle Clusterware binaries. Ensure that the directory path you provide meets the following requirements:

- It should be created in a path separate from existing Oracle homes.

- It should not be located in a user home directory.

- It should be created either as a subdirectory in a path where all files can be owned by root, or in a unique path.

- Before installation, it should be owned by the installation owner of Oracle Clusterware (typically `oracle` for a single installation owner for all Oracle software, or `crs` for role-based Oracle installation owners), and set to 750 permissions.

For installations with Oracle Clusterware only, Oracle recommends that you create a path compliant with Oracle Optimal Flexible Architecture (OFA) guidelines, so that Oracle Universal Installer (OUI) can select that directory during installation. For OUI to recognize the path as an Oracle software path, it must be in the form u0[*1-9*]/app.

When OUI finds an OFA-compliant path, it creates the Oracle Clusterware and Oracle Central Inventory (oraInventory) directories for you.

Create an Oracle Clusterware path. For example:

```
# mkdir -p  /u01/app
# chown -R crs:oinstall /u01
```

Alternatively, if you later intend to install Oracle Database software, then create an Oracle base path. OUI automatically creates an OFA-compliant path for Oracle Clusterware derived from the Oracle base path. 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 Database software. For example:

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

> **Note:** If you choose to create an Oracle Clusterware home manually, then do not create the Oracle Clusterware home under Oracle base. Creating an Oracle Clusterware installation in an Oracle base directory will cause succeeding Oracle installations to fail.

> **See Also:** Section 2.4, "Creating Groups, Users and Paths for Oracle Grid Infrastructure" for information about creating groups, users, and software homes for additional Oracle software installations

2.14 Requirements for Creating an Oracle Grid Infrastructure Home Directory

During installation, you are prompted to provide a path to a home directory to store Oracle grid infrastructure software. Ensure that the directory path you provide meets the following requirements:

- It should be created in a path outside existing Oracle homes, including Oracle Clusterware homes.

- It should not be located in a user home directory.

- It should be created either as a subdirectory in a path where all files can be owned by `root`, or in a unique path.

- If you create the path before installation, then it should be owned by the installation owner of Oracle grid infrastructure (typically `oracle` for a single installation owner for all Oracle software, or `grid` for role-based Oracle installation owners), and set to 775 permissions.

Oracle recommends that you install Oracle grid infrastructure on local homes, rather than using a shared home on shared storage.

For installations with Oracle grid infrastructure only, Oracle recommends that you create a path compliant with Oracle Optimal Flexible Architecture (OFA) guidelines, so that Oracle Universal Installer (OUI) can select that directory during installation. For OUI to recognize the path as an Oracle software path, it must be in the form u0[*1-9*]/app.

When OUI finds an OFA-compliant path, it creates the Oracle grid infrastructure and Oracle Inventory (`oraInventory`) directories for you.

To create an Oracle grid infrastructure path manually, ensure that it is in a separate path, not under an existing Oracle base path. For example:

```
# mkdir -p  /u01/app/11.2.0/grid
# chown grid:oinstall /u01/app/11.2.0/grid
# chmod -R 775 /u01/app/11.2.0/grid
```

With this path, if the installation owner is named grid, then by default OUI creates the following path for the grid home:

```
/u01/app/11.2.0/grid
```

Create an Oracle base path for database installations, owned by the Oracle Database installation owner account. The OFA path for an Oracle base is `/u01/app/user`, where *user* is the name of the Oracle software installation owner account. For example, use the following commands to create an Oracle base for the database installation owner account `oracle`:

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

> **Note:** If you choose to create an Oracle grid infrastructure home manually, then do not create the Oracle grid infrastructure home for a cluster under either the grid installation owner Oracle base or the Oracle Database installation owner Oracle base. Creating an Oracle Clusterware installation in an Oracle base directory will cause succeeding Oracle installations to fail.
>
> Oracle grid infrastructure homes can be placed in a local home on servers, even if your existing Oracle Clusterware home from a prior release is in a shared location.
>
> Homes for Oracle grid infrastructure for a standalone server (Oracle Restart) can be under Oracle base. Refer to *Oracle Database Installation Guide* for your platform for more information about Oracle Restart.

Configuring Storage for Grid Infrastructure for a Cluster and Oracle Real Application Clusters (Oracle RAC)

This chapter describes the storage configuration tasks that you must complete before you start the installer to install Oracle Clusterware and Automatic Storage Management (ASM), and that you must complete before adding an Oracle Real Application Clusters (Oracle RAC) installation to the cluster.

This chapter contains the following topics:

- Reviewing Oracle Grid Infrastructure Storage Options
- Shared File System Storage Configuration
- Automatic Storage Management Storage Configuration
- Desupport of Block and Raw Devices

3.1 Reviewing Oracle Grid Infrastructure Storage Options

This section describes supported options for storing Oracle grid infrastructure for a cluster storage options. It contains the following sections:

- Overview of Oracle Clusterware and Oracle RAC Storage Options
- General Storage Considerations for Oracle Grid Infrastructure and Oracle RAC
- Supported Storage Options
- After You Have Selected Disk Storage Options

> **See Also:** The Oracle Certify site for a list of supported vendors for Network Attached Storage options:
>
> http://www.oracle.com/technology/support/metalink/
>
> Refer also to the Certify site on My Oracle Support for the most current information about certified storage options:
>
> https://metalink.oracle.com/

3.1.1 Overview of Oracle Clusterware and Oracle RAC Storage Options

There are two ways of storing Oracle Clusterware files:

- **Automatic Storage Management (Oracle ASM)**: You can install Oracle Clusterware files (OCR and voting disks) in Oracle ASM diskgroups.

Oracle ASM is the required database storage option for Typical installations, and for Standard Edition Oracle RAC installations. It is an integrated, high-performance database file system and disk manager for Oracle Clusterware and Oracle Database files. It performs striping and mirroring of database files automatically.

Only one Oracle ASM instance is permitted for each node regardless of the number of database instances on the node.

■ **A supported shared file system**: Supported file systems include the following:

– **A supported cluster file system** Note that if you intend to use a cluster file system for your data files, then you should create partitions large enough for the database files when you create partitions for Oracle grid infrastructure.

See Also: The Certify page on My Oracle Support for supported cluster file systems

– **Network File System (NFS)**: Note that if you intend to use NFS for your data files, then you should create partitions large enough for the database files when you create partitions for Oracle grid infrastructure. NFS mounts differ for software binaries, Oracle Clusterware files, and database files.

Note: You can no longer use OUI to install Oracle Clusterware or Oracle Database files on block or raw devices.

See Also: My Oracle Support for supported file systems and NFS or NAS filers

3.1.2 General Storage Considerations for Oracle Grid Infrastructure and Oracle RAC

For all installations, you must choose the storage option to use for Oracle grid infrastructure (Oracle Clusterware and Oracle ASM), and Oracle Real Application Clusters databases (Oracle RAC). To enable automated backups during the installation, you must also choose the storage option to use for recovery files (the Fast Recovery Area). You do not have to use the same storage option for each file type.

3.1.2.1 General Storage Considerations for Oracle Clusterware

Oracle Clusterware voting disks are used to monitor cluster node status, and Oracle Cluster Registry (OCR) files contain configuration information about the cluster. You can place voting disks and OCR files either in an ASM diskgroup, or on a cluster file system or shared network file system. Storage must be shared; any node that does not have access to an absolute majority of voting disks (more than half) will be restarted.

3.1.2.2 General Storage Considerations for Oracle RAC

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

■ You can choose any combination of the supported storage options for each file type provided that you satisfy all requirements listed for the chosen storage options.

■ Oracle recommends that you choose Oracle ASM as the storage option for database and recovery files.

- For Standard Edition Oracle RAC installations, Oracle ASM is the only supported storage option for database or recovery files.

- If you intend to use Oracle ASM with Oracle RAC, and you are configuring a new Oracle ASM instance, then your system must meet the following conditions:

  - All nodes on the cluster have Oracle Clusterware and Oracle ASM 11*g* release 2 (11.2) installed as part of an Oracle grid infrastructure for a cluster installation.

  - Any existing Oracle ASM instance on any node in the cluster is shut down.

- Raw or block devices are supported only when upgrading an existing installation using the partitions already configured. On new installations, using raw or block device partitions is not supported by Automatic Storage Management Configuration Assistant (ASMCA) or Oracle Universal Installer (OUI), but is supported by the software if you perform manual configuration.

     See Also: *Oracle Database Upgrade Guide* for information about how to prepare for upgrading an existing database

- If you do not have a storage option that provides external file redundancy, then you must configure at least three voting disk areas to provide voting disk redundancy.

3.1.3 Supported Storage Options

The following table shows the storage options supported for storing Oracle Clusterware and Oracle RAC files.

Table 3–1 Supported Storage Options for Oracle Clusterware and Oracle RAC

Storage Option	OCR and Voting Disks	Oracle Clusterware binaries	Oracle RAC binaries	Oracle Database Files	Oracle Recovery Files
Automatic Storage Management	Yes	No	No	Yes	Yes
Local file system	No	Yes	Yes	No	No
NFS file system on a certified NAS filer	Yes	Yes	Yes	Yes	Yes
Shared disk partitions (block devices or raw devices)	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.	No	No	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.	No
Shared Logical Volume Manager (SLVM)	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.	No	No	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.	No

Use the following guidelines when choosing storage options:

- You can choose any combination of the supported storage options for each file type provided that you satisfy all requirements listed for the chosen storage options.

- You can use Oracle ASM 11*g* release 2 (11.2) to store Oracle Clusterware files. You cannot use Oracle ASM releases prior to 11*g* release 2 (11.2) to do this.

- If you do not have a storage option that provides external file redundancy, then you must configure at least three voting disk locations and at least three Oracle Cluster Registry locations to provide redundancy.

3.1.4 After You Have Selected Disk Storage Options

When you have determined your disk storage options, configure shared storage:

- **To use a file system**, refer to Section 3.2, "Shared File System Storage Configuration."

- **To use Automatic Storage Management**, refer to Section 3.3, "Automatic Storage Management Storage Configuration."

3.2 Shared File System Storage Configuration

The installer does not suggest a default location for the Oracle Cluster Registry (OCR) or the Oracle Clusterware voting disk. If you choose to create these files on a file system, then review the following sections to complete storage requirements for Oracle Clusterware files:

- Requirements for Using a Shared File System

- Deciding to Use a Cluster File System for Oracle Clusterware Files

- Deciding to Use NFS for Data Files

- Configuring Storage NFS Mount and Buffer Size Parameters

- Checking NFS Mount and Buffer Size Parameters for Oracle Clusterware

- Checking NFS Mount and Buffer Size Parameters for Oracle RAC

- Creating Directories for Oracle Clusterware Files on Shared File Systems

- Creating Directories for Oracle Database Files on Shared File Systems

---

> **Note:** The OCR is a file that contains the configuration information and status of the cluster. Oracle Universal Installer (OUI) automatically initializes the OCR during the Oracle Clusterware installation. Database Configuration Assistant uses the OCR for storing the configurations for the cluster databases that it creates.

3.2.1 Requirements for Using a Shared File System

To use a shared file system for Oracle Clusterware, Oracle ASM, and Oracle RAC, the file system must comply with the following requirements:

- To use an NFS file system, it must be on a certified NAS device. Log in to My Oracle Support at the following URL, and click the Certify tab to find a list of certified NAS devices.

  https://metalink.oracle.com/

- If you choose to place your Oracle Cluster Registry (OCR) files on a shared file system, then Oracle recommends that one of the following is true:

  - The disks used for the file system are on a highly available storage device, (for example, a RAID device).

– At least two file systems are mounted, and use the features of Oracle Clusterware 11*g* release 2 (11.2) to provide redundancy for the OCR.

■ If you choose to place your database files on a shared file system, then one of the following should be true:

– The disks used for the file system are on a highly available storage device, (for example, a RAID device).

– The file systems consist of at least two independent file systems, with the database files on one file system, and the recovery files on a different file system.

■ The user account with which you perform the installation (`oracle` or `grid`) must have write permissions to create the files in the path that you specify.

Note: Upgrading from Oracle9*i* release 2 using the raw device or shared file for the OCR that you used for the SRVM configuration repository is not supported.

If you are upgrading Oracle Clusterware, and your existing cluster uses 100 MB OCR and 20 MB voting disk partitions, then you can continue to use those partition sizes.

All storage products must be supported by both your server and storage vendors.

Use Table 3–2 and Table 3–3 to determine the minimum size for shared file systems:

Table 3–2   Oracle Clusterware Shared File System Volume Size Requirements

File Types Stored	Number of Volumes	Volume Size
Voting disks with external redundancy	3	At least 280 MB for each voting disk volume.
Oracle Cluster Registry (OCR) with external redundancy	1	At least 280 MB for each OCR volume
Oracle Clusterware files (OCR and voting disks) with redundancy provided by Oracle software.	1	At least 280 MB for each OCR volume At least 280 MB for each voting disk volume

Table 3–3   Oracle RAC Shared File System Volume Size Requirements

File Types Stored	Number of Volumes	Volume Size
Oracle Database files	1	At least 1.5 GB for each volume
Recovery files	1	At least 2 GB for each volume
Note: Recovery files must be on a different volume than database files		

In Table 3–2 and Table 3–3, the total required volume size is cumulative. For example, to store all Oracle Clusterware files on the shared file system with normal redundancy, you should have at least 2 GB of storage available over a minimum of three volumes (three separate volume locations for the OCR and two OCR mirrors, and one voting disk on each volume). You should have a minimum of three physical disks, each at

least 500 MB, to ensure that voting disks and OCR files are on separate physical disks. If you add Oracle RAC using one volume for database files and one volume for recovery files, then you should have at least 3.5 GB available storage over two volumes, and at least 5.5 GB available total for all volumes.

3.2.2 Deciding to Use a Cluster File System for Oracle Clusterware Files

For new installations, Oracle recommends that you use Automatic Storage Management (Oracle ASM) to store voting disk and OCR files.

3.2.3 Deciding to Use NFS for Data Files

Network-attached storage (NAS) systems use NFS to access data. You can store data files on a supported NFS system.

NFS file systems must be mounted and available over NFS mounts before you start installation. Refer to your vendor documentation to complete NFS configuration and mounting.

Be aware that the performance of Oracle software and databases stored on NAS devices depends on the performance of the network connection between the Oracle server and the NAS device.

For this reason, Oracle recommends that you connect the server to the NAS device using a private dedicated network connection, which should be Gigabit Ethernet or better.

3.2.4 Configuring Storage NFS Mount and Buffer Size Parameters

If you are using NFS for the Grid home or Oracle RAC home, then you must set up the NFS mounts on the storage so that they allow `root` on the clients mounting to the storage to be considered `root` instead of being mapped to an anonymous user, and allow `root` on the client server to create files on the NFS filesystem that are owned by `root`.

On NFS, you can obtain `root` access for clients writing to the storage by enabling `root=access_list` on the server side. For example, to set up Oracle Clusterware file storage in the path `/vol/grid`, with nodes node1, node 2, and node3 in the domain `mycluster.example.com`, add a line similar to the following to the `/etc/dfs/dfstab` file:

```
share -F nfs -o
rw=node1.mycluster.example.com,node2,mycluster.example.com,node3.mycluster.example
.com,root=node1.mycluster.example.com,node2.mycluster.example.com,node3.mycluster.
example.com /vol/grid
```

> **Note:** Enter share settings as a single line.

If the domain or DNS is secure so that no unauthorized system can obtain an IP address on it, then you can grant root access by domain, rather than specifying particular cluster member nodes:

For example:

```
/vol/grid/ *.mycluster.example.com
```

Oracle recommends that you use a secure DNS or domain, and grant `root` access to cluster member nodes using the domain, as using this syntax allows you to add or remove nodes without the need to reconfigure the NFS server.

If you use Grid Naming Service (GNS), then the subdomain allocated for resolution by GNS within the cluster is a secure domain. Any server without a correctly signed Grid Plug and Play (GPnP) profile cannot join the cluster, so an unauthorized system cannot obtain or use names inside the GNS subdomain.

> **Caution:** Granting `root` access by domain can be used to obtain unauthorized access to systems. System administrators should refer to their operating system documentation for the risks associated with using `root=access`.

After changing `/etc/dfs/dfstab`, reload the file system mount using the following command:

```
# /usr/sbin/shareall
```

3.2.5 Checking NFS Mount and Buffer Size Parameters for Oracle Clusterware

On the cluster member nodes, you must set the values for the NFS buffer size parameters `rsize` and `wsize` to 32768.

The NFS client-side mount options are:

```
rw,bg,vers=3,proto=tcp,noac,hard,nointr,timeo=600,rsize=32768,wsize=32768,suid
```

If you have Oracle grid infrastructure binaries on an NFS mount, then you must include the `suid` option.

The NFS client-side mount options for Oracle Clusterware files (OCR and voting disk files) are:

```
rw,bg,vers=3,proto=tcp,noac,forcedirectio,hard,nointr,timeo=600,rsize=32768,wsize=32768,suid
```

Update the `/etc/fstab` file on each node with an entry containing the NFS mount options for your platform. For example, if your platform is x86-64, and you are creating a mount point for Oracle Clusterware files, then update the `/etc/fstab` files with an entry similar to the following:

```
nfsserver:/vol/grid  /u02/oracle/cwfiles nfs \
rw,bg,vers=3,proto=tcp,noac,forcedirectio,hard,nointr,timeo=600,rsize=32768,wsize=32768,suid
```

Note that mount point options are different for Oracle software binaries, compared to Oracle Clusterware files (OCR and voting disks) and data files.

To create a mount point for binaries only, provide an entry similar to the following for a binaries mount point:

```
nfs-server:/vol/bin /u02/oracle/grid nfs \
rw,bg,vers=3,proto=tcp,noac,hard,nointr,timeo=600,rsize=32768,wsize=32768,suid
```

> **See Also:** My Oracle Support bulletin 359515.1, "Mount Options for Oracle Files When Used with NAS Devices" for the most current information about mount options, available from the following URL:
>
> https://metalink.oracle.com

> **Note:** Refer to your storage vendor documentation for additional information about mount options.

3.2.6 Checking NFS Mount and Buffer Size Parameters for Oracle RAC

If you use NFS mounts, then you must mount NFS volumes used for storing database files with special mount options on each node that has an Oracle RAC instance. When mounting an NFS file system, Oracle recommends that you use the same mount point options that your NAS vendor used when certifying the device. Refer to your device documentation or contact your vendor for information about recommended mount-point options.

Update the /etc/fstab file on each node with an entry similar to the following:

```
nfs-server:/vol/DATA/oradata  /u02/oradata     nfs\
rw,bg,hard,nointr,rsize=32768,wsize=32768,proto=tcp,noac,forcedirectio,vers=3,suid
```

The mandatory mount options comprise the minimum set of mount options that you must use while mounting the NFS volumes. These mount options are essential to protect the integrity of the data and to prevent any database corruption. Failure to use these mount options may result in the generation of file access errors. Refer to your operating system or NAS device documentation for more information about the specific options supported on your platform.

> **See Also:** My Oracle Support note 359515.1 for updated NAS mount option information, available at the following URL:
>
> https://metalink.oracle.com

3.2.7 Creating Directories for Oracle Clusterware Files on Shared File Systems

Use the following instructions to create directories for Oracle Clusterware files. You can also configure shared file systems for the Oracle Database and recovery files.

> **Note:** For NFS storage, you must complete this procedure only if you want to place the Oracle Clusterware files on a separate file system from the Oracle base directory.

To create directories for the Oracle Clusterware files on separate file systems from the Oracle base directory, follow these steps:

1. If necessary, configure the shared file systems to use and mount them on each node.

> **Note:** The mount point that you use for the file system must be identical on each node. Ensure that the file systems are configured to mount automatically when a node restarts.

2. Use the `bdf` command to determine the free disk space on each mounted file system.

3. From the display, identify the file systems to use. Choose a file system with a minimum of 600 MB of free disk space (one OCR and one voting disk, with external redundancy).

   If you are using the same file system for multiple file types, then add the disk space requirements for each type to determine the total disk space requirement.

4. Note the names of the mount point directories for the file systems that you identified.

5. If the user performing installation (typically, `grid` or `oracle`) has permissions to create directories on the storage location where you plan to install Oracle Clusterware files, then OUI creates the Oracle Clusterware file directory.

   If the user performing installation does not have write access, then you must create these directories manually using 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 the directory. For example, where the user is `oracle`, and the Oracle Clusterware file storage area is `cluster`:

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

   > **Note:** After installation, directories in the installation path for the Oracle Cluster Registry (OCR) files should be owned by `root`, and not writable by any account other than `root`.

When you have completed creating a subdirectory in the mount point directory, and set the appropriate owner, group, and permissions, you have completed NFS configuration for Oracle grid infrastructure.

3.2.8 Creating Directories for Oracle Database Files on Shared File Systems

Use the following instructions to create directories for shared file systems for Oracle Database and recovery files (for example, for an Oracle RAC database).

1. If necessary, configure the shared file systems and mount them on each node.

   > **Note:** The mount point that you use for the file system must be identical on each node. Ensure that the file systems are configured to mount automatically when a node restarts.

2. Use the `bdf` command to determine the free disk space on each mounted file system.

3. From the display, identify the file systems:

File Type	File System Requirements
Database files	Choose either: ■ A single file system with at least 1.5 GB of free disk space. ■ Two or more file systems with at least 1.5 GB of free disk space in total.
Recovery files	Choose a file system with at least 2 GB of free disk space.

If you are using the same file system for multiple file types, then add the disk space requirements for each type to determine the total disk space requirement.

4. Note the names of the mount point directories for the file systems that you identified.

5. If the user performing installation (typically, `oracle`) has permissions to create directories on the disks where you plan to install Oracle Database, then DBCA creates the Oracle Database file directory, and the Recovery file directory.

If the user performing installation does not have write access, then you must create these directories manually using 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
```

■ Recovery file directory (Fast Recovery Area):

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

By making members of the `oinstall` group owners of these directories, this permits them to be read by multiple Oracle homes, including those with different OSDBA groups.

When you have completed creating subdirectories in each of the mount point directories, and set the appropriate owner, group, and permissions, you have completed NFS configuration for Oracle Database shared storage.

3.3 Automatic Storage Management Storage Configuration

Review the following sections to configure storage for Automatic Storage Management:

■ Configuring Storage for Automatic Storage Management

■ Using Diskgroups with Oracle Database Files on ASM

■ Migrating Existing Oracle ASM Instances

3.3.1 Configuring Storage for Automatic Storage Management

This section describes how to configure storage for use with Automatic Storage Management.

■ Identifying Storage Requirements for Automatic Storage Management

- [Creating Files on a NAS Device for Use with Automatic Storage Management](#)

- [Using an Existing Automatic Storage Management Disk Group](#)

- [Configuring Disk Devices for Oracle ASM](#)

3.3.1.1 Identifying Storage Requirements for Automatic Storage Management

To identify the storage requirements for using Automatic Storage Management, you must determine how many devices and the amount of free disk space that you require. To complete this task, follow these steps:

1. Determine whether you want to use Automatic Storage Management for Oracle Clusterware files (OCR and voting disks), Oracle Database files, recovery files, or all files except for Oracle Clusterware or Oracle Database binaries. Oracle Database files include data files, control files, redo log files, the server parameter file, and the password file.

   > **Note:** You do not have to use the same storage mechanism for Oracle Clusterware, Oracle Database files and recovery files. You can use a shared file system for one file type and Automatic Storage Management for the other.
   >
   > If you choose to enable automated backups and you do not have a shared file system available, then you must choose Automatic Storage Management for recovery file storage.

   If you enable automated backups during the installation, then you can select Automatic Storage Management as the storage mechanism for recovery files by specifying an Automatic Storage Management disk group for the Fast Recovery Area. Depending on how you choose to create a database during the installation, you have the following options:

   - If you select an installation method that runs ASMCA in interactive mode, then you can decide whether you want to use the same Automatic Storage Management disk group for database files and recovery files, or use different failure groups for each file type.

   - If you select an installation method that runs DBCA in noninteractive mode, then you must use the same Automatic Storage Management disk group for database files and recovery files.

2. Choose the Automatic Storage Management redundancy level to use for the Automatic Storage Management disk group.

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

   - External redundancy

     An external redundancy disk group requires a minimum of one disk device. The effective disk space in an external redundancy disk group is the sum of the disk space in all of its devices.

     Because Automatic Storage Management does not mirror data in an external redundancy disk group, Oracle recommends that you use external redundancy with storage devices such as RAID, or other similar devices that provide their own data protection mechanisms.

- **Normal redundancy**

  In a normal redundancy disk group, to increase performance and reliability, Automatic Storage Management by default uses two-way mirroring. A normal redundancy disk group requires a minimum of two disk devices (or two failure groups). The effective disk space in a normal redundancy disk group is half the sum of the disk space in all of its devices.

  For Oracle Clusterware files, Normal redundancy disk groups provide 3 voting disk files, 1 OCR and 2 copies (one primary and one secondary mirror). With normal redundancy, the cluster can survive the loss of one failure group.

  For most installations, Oracle recommends that you select normal redundancy.

- **High redundancy**

  In a high redundancy disk group, Automatic Storage Management uses three-way mirroring to increase performance and provide the highest level of reliability. A high redundancy disk group requires a minimum of three disk devices (or three failure groups). The effective disk space in a high redundancy disk group is one-third the sum of the disk space in all of its devices.

  For Oracle Clusterware files, High redundancy disk groups provide 5 voting disk files, 1 OCR and 3 copies (one primary and two secondary mirrors). With high redundancy, the cluster can survive the loss of two failure groups.

  While high redundancy disk groups do provide a high level of data protection, you should consider the greater cost of additional storage devices before deciding to select high redundancy disk groups.

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

   Use Table 3–4 and Table 3–5 to determine the minimum number of disks and the minimum disk space requirements for installing Oracle Clusterware files, and installing the starter database, where you have voting disks in a separate disk group:

Table 3–4   Total Oracle Clusterware Storage Space Required by Redundancy Type

Redundancy Level	Minimum Number of Disks	Oracle Cluster Registry (OCR) Files	Voting Disk Files	Both File Types
External	1	280 MB	280 MB	560 MB
Normal	3	560 MB	840 MB	1.4 GB[1]
High	5	840 MB	1.4 GB	2.3 GB

[1] If you create a diskgroup during installation, then it must be at least 2 GB.

> **Note:**   If the voting disk files are in a disk group, be aware that disk groups with Oracle Clusterware files (OCR and voting disks) have a higher minimum number of failure groups than other disk groups.
>
> If you create a diskgroup as part of the installation in order to install the OCR and voting disk files, then the installer requires that you create these files on a diskgroup with at least 2 GB of available space.

Table 3–5   Total Oracle Database Storage Space Required by Redundancy Type

Redundancy Level	Minimum Number of Disks	Database Files	Recovery Files	Both File Types
External	1	1.5 GB	3 GB	4.5 GB
Normal	2	3 GB	6 GB	9 GB
High	3	4.5 GB	9 GB	13.5 GB

4. For Oracle Clusterware installations, you must also add additional disk space for the Automatic Storage Management metadata. You can use the following formula to calculate the additional disk space requirements (in MB):

total = [2 * ausize * disks] + [redundancy * (ausize * (nodes * (clients + 1) + 30) + (64 * nodes) + 533)]

Where:

- redundancy = Number of mirrors: external = 1, normal = 2, high = 3.

- ausize = Metadata AU size in megabytes.

- nodes = Number of nodes in cluster.

- clients - Number of database instances for each node.

- disks - Number of disks in disk group.

For example, for a four-node Oracle RAC installation, using three disks in a normal redundancy disk group, you require an additional X MB of space:

[2 * 1 * 3] + [2 * (1 * (4 * (4 + 1)+ 30)+ (64 * 4)+ 533)] = 1684 MB

To ensure high availability of Oracle Clusterware files on Oracle ASM, you need to have at least 2 GB of disk space for Oracle Clusterware files in three separate failure groups, with at least three physical disks. Each disk must have at least 1 GB of capacity to ensure that there is sufficient space to create Oracle Clusterware files.

5. For Oracle RAC installations, you must also add additional disk space for the Automatic Storage Management metadata. You can use the following formula to calculate the additional disk space requirements (in MB):

total = [2 * *ausize* * *disks*] + [*redundancy* * (*ausize* * (*nodes* * (*clients* + 1) + 30) + (64 * *nodes*) + 533)]

Where:

- *ausize* = Metadata AU size in megabytes.

- *clients* = Number of database instances for each node.

- *disks* = Number of disks in disk group.

- *nodes* = Number of nodes in cluster.

- *redundancy* = Number of mirrors: external = 1, normal = 2, high = 3.

For example, for a four-node Oracle RAC installation, using three disks in a normal redundancy disk group, you require an additional 1684 MB of disk space:

[2 * 1 * 3] + [2 * (1 * (4 * (4+1) + 30) + (64 * 4) + 533)] = 1684 MB

If an Automatic Storage Management 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 installation.

6. Optionally, identify failure groups for the Automatic Storage Management disk group devices.

   If you intend to use a normal or high redundancy disk group, then you can further protect your database against hardware failure by associating a set of disk devices in a custom failure group. By default, each device comprises its own 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.

   To protect against failures of this type, you could 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:** Define custom failure groups after installation, using the GUI tool ASMCA, the command line tool `asmcmd`, or SQL commands.
   >
   > If you define custom failure groups, then for failure groups containing database files only, you must specify a minimum of two failure groups for normal redundancy disk groups and three failure groups for high redundancy disk groups.
   >
   > For failure groups containing database files and clusterware files, including voting disks, you must specify a minimum of three failure groups for normal redundancy disk groups, and five failure groups for high redundancy disk groups.
   >
   > Disk groups containing voting files must have at least 3 failure groups for normal redundancy or at least 5 failure groups for high redundancy. Otherwise, the minimum is 2 and 3 respectively. The minimum number of failure groups applies whether or not they are custom failure groups.

7. 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. Use the following guidelines when identifying appropriate disk devices:

   - All of the devices in an Automatic Storage Management 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. Automatic Storage Management expects each disk group device to be on a separate physical disk.

   - Although you can specify a logical volume as a device in an Automatic Storage Management disk group, Oracle does not recommend their use. Non-shared logical volumes are not supported with Oracle RAC. If you want to use logical volumes for your Oracle RAC database, then you must use shared logical volumes created by a cluster-aware logical volume manager.

3.3.1.2 Creating Files on a NAS Device for Use with Automatic Storage Management

If you have a certified NAS storage device, then you can create zero-padded files in an NFS mounted directory and use those files as disk devices in an Automatic Storage Management disk group.

To create these files, follow these steps:

1. If necessary, create an exported directory for the disk group files on the NAS device.

   Refer to the NAS device documentation for more information about completing this step.

2. Switch user to `root`.

3. Create a mount point directory on the local system.

4. To ensure that the NFS file system is mounted when the system restarts, add an entry for the file system in the mount file `/etc/fstab`.

   > **See Also:** My Oracle Support note 359515.1 for updated NAS mount option information, available at the following URL:
   >
   > https://metalink.oracle.com

   For more information about editing the mount file for the operating system, refer to the `man` pages. For more information about recommended mount options, refer to the section Section 3.2.6, "Checking NFS Mount and Buffer Size Parameters for Oracle RAC."

5. Mount the NFS file system on the local system

6. Choose a name for the disk group to create. For example: `sales1`.

7. Create a directory for the files on the NFS file system, using the disk group name as the directory name.

8. Use commands similar to the following to create the required number of zero-padded files in this directory:

   ```
   # dd if=/dev/zero of=/mnt/nfsdg/disk1 bs=1024k count=1000
   ```

   This example creates 1 GB files on the NFS file system. You must create one, two, or three files respectively to create an external, normal, or high redundancy disk group.

9. Enter commands similar to the following to change the owner, group, and permissions on the directory and files that you created, where the installation owner is `grid`, and the OSASM group is `asmadmin`:

   ```
   # chown -R grid:asmadmin /mnt/nfsdg
   # chmod -R 660 /mnt/nfsdg
   ```

10. If you plan to install Oracle RAC or a standalone Oracle Database, then during installation, edit the Automatic Storage Management disk discovery string to specify a regular expression that matches the file names you created. For example:

    ```
    /mnt/nfsdg/sales1/
    ```

3.3.1.3 Using an Existing Automatic Storage Management Disk Group

To store either database or recovery files in an existing Automatic Storage Management disk group, then you have the following choices, depending on the installation method that you select:

- If you select an installation method that runs Database Configuration Assistant in interactive mode, then you can decide whether you want to create a disk group, or to use an existing one.

  The same choice is available to you if you use Database Configuration Assistant after the installation to create a database.

- If you select an installation method that runs Database Configuration Assistant in noninteractive mode, then you must choose an existing disk group for the new database; you cannot create a disk group. However, you can add disk devices to an existing disk group if it has insufficient free space for your requirements.

  > **Note:** The Automatic Storage Management instance that manages the existing disk group can be running in a different Oracle home directory.

To determine if an existing Automatic Storage Management disk group exists, or to determine if there is sufficient disk space in a disk group, you can use the ASM command line tool (`asmcmd`), Oracle Enterprise Manager Grid Control or Database Control. Alternatively, you can use the following procedure:

1. View the contents of the `oratab` file to determine if an Automatic Storage Management instance is configured on the system:

   ```
   $ more /etc/oratab
   ```

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

   ```
   +ASM2:oracle_home_path
   ```

   In this example, `+ASM2` is the system identifier (SID) of the Automatic Storage Management instance, with the node number appended, and `oracle_home_path` is the Oracle home directory where it is installed. By convention, the SID for an Automatic Storage Management instance begins with a plus sign.

2. Set the `ORACLE_SID` and `ORACLE_HOME` environment variables to specify the appropriate values for the Automatic Storage Management instance.

3. Connect to the Automatic Storage Management instance and start the instance if necessary:

   ```
   $ $ORACLE_HOME/bin/asmcmd
   ASMCMD> startup
   ```

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

   ```
   ASMCMD> lsdb
   ```

   or:

   ```
   $ORACLE_HOME/bin/asmcmd -p lsdg
   ```

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.

3.3.1.4 Configuring Disk Devices for Oracle ASM

To configure disks for use with ASM on HP-UX, follow these steps:

1. If necessary, install the shared disks that you intend to use for the ASM disk group.

2. To make sure that the disks are available, enter the following command on every node:

```
# /usr/sbin/ioscan -fun -C disk
```

The output from this command is similar to the following:

```
Class  I  H/W Path    Driver S/W State   H/W Type     Description
=============================================================================
disk   0  0/0/1/0.6.0 sdisk  CLAIMED     DEVICE       HP    DVD-ROM 6x/32x
                      /dev/rdsk/c0t6d0  /dev/rdsk/c0t6d0
disk   1  0/0/1/1.2.0 sdisk  CLAIMED     DEVICE       SEAGATE ST39103LC
                      /dev/rdsk/c1t2d0  /dev/rdsk/c1t2d0
```

This command displays information about each disk attached to the system, including character raw device names (`/dev/rdsk/`).

> **Note:** On HP-UX 11*i* v.3, you can also use agile view to review mass storage devices, including character raw devices (`/dev/rdisk/disk`*xyz*). For example:
>
> ```
> #>ioscan -funN -C disk
> Class     I  H/W Path  Driver S/W State   H/W Type     Description
> ===================================================================
> disk      4  64000/0xfa00/0x1   esdisk   CLAIMED      DEVICE
> HP 73.4GST373454LC
>               /dev/disk/disk4   /dev/rdisk/disk4
> disk    907  64000/0xfa00/0x2f  esdisk   CLAIMED      DEVICE
> COMPAQ  MSA1000 VOLUME
>               /dev/disk/disk907   /dev/rdisk/disk907
> ```

3. If the `ioscan` command does not display device name information for a device that you want to use, enter the following command to install the special device files for any new devices:

```
# /usr/sbin/insf -e
```

4. For each disk that you want to add to a disk group, enter the following command on any node to verify that it is not already part of an LVM volume group:

```
# /sbin/pvdisplay /dev/dsk/cxtydz
```

If this command displays volume group information, the disk is already part of a volume group. The disks that you choose must not be part of an LVM volume group.

> **Note:** If you are using different volume management software, for example VERITAS Volume Manager, refer to the appropriate documentation for information about verifying that a disk is not in use.

5. Enter commands similar to the following on every node to change the owner, group, and permissions on the character raw device file for each disk that you want to add to a disk group, so that the owner is the grid infrastructure owner (in this example, `grid`), and the group that has access is the OSASM group (in this example, `asmadmin`):

```
# chown grid:asmadmin /dev/rdsk/cxtydz
# chmod 660 /dev/rdsk/cxtydz
```

> **Note:** If you are using a multi-pathing disk driver with ASM, make sure that you set the permissions only on the correct logical device name for the disk.
>
> If the nodes are configured differently, the device name for a particular device might be different on some nodes. Make sure that you specify the correct device names on each node.

3.3.2 Using Diskgroups with Oracle Database Files on ASM

Review the following sections to configure Automatic Storage Management storage for Oracle Clusterware and Oracle Database Files:

- Identifying and Using Existing Oracle Database Diskgroups on ASM
- Creating Diskgroups for Oracle Database Data Files

3.3.2.1 Identifying and Using Existing Oracle Database Diskgroups on ASM

The following section describes how to identify existing diskgroups and determine the free disk space that they contain.

- Optionally, identify failure groups for the Automatic Storage Management disk group devices.

  If you intend to use a normal or high redundancy disk group, then you can further protect your database against hardware failure by associating a set of disk devices in a custom failure group. By default, each device comprises its own 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.

  To protect against failures of this type, you could 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 and three failure groups for high redundancy.

3.3.2.2 Creating Diskgroups for Oracle Database Data Files

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. Use the following guidelines when identifying appropriate disk devices:

- All of the devices in an Automatic Storage Management 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. Automatic Storage Management expects each disk group device to be on a separate physical disk.

- Although you can specify a logical volume as a device in an Automatic Storage Management disk group, Oracle does not recommend their use. Logical volume managers can hide the physical disk architecture, preventing Automatic Storage Management from optimizing I/O across the physical devices. They are not supported with Oracle RAC.

3.3.3 Migrating Existing Oracle ASM Instances

If you have an Oracle ASM installation from a prior release installed on your server, or in an existing Oracle Clusterware installation, then you can use Automatic Storage Management Configuration Assistant (ASMCA, located in the path `Grid_home`/bin) to upgrade the existing Oracle ASM instance to 11*g* release 2 (11.2), and subsequently configure failure groups, and ASM volumes.

> **Note:** You must first shut down all database instances and applications on the node with the existing Oracle ASM instance before upgrading it.

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

On an existing Oracle Clusterware or Oracle RAC installation, if the prior version of Oracle ASM instances on all nodes is 11*g* release 1, then you are provided with the option to perform a rolling upgrade of Oracle ASM instances. If the prior version of Oracle ASM instances on an Oracle RAC installation are from a release prior to 11*g* release 1, then rolling upgrades cannot be performed. Oracle ASM on all nodes will be upgraded to 11*g* release 2 (11.2).

3.4 Desupport of Block and Raw Devices

With the release of Oracle Database 11*g* release 2 (11.2) and Oracle RAC 11*g* release 2 (11.2), using Database Configuration Assistant or the installer to store Oracle Clusterware or Oracle Database files on block or raw devices is not supported.

If you intend to upgrade an existing Oracle RAC database, or an Oracle RAC database with Oracle ASM instances, then you can use an existing raw or block device partition, and perform a rolling upgrade of your existing installation. Performing a new installation using block or raw devices is not allowed.

4

Installing Oracle Grid Infrastructure for a Cluster

This chapter describes the procedures for installing Oracle grid infrastructure for a cluster. Oracle grid infrastructure consists of Oracle Clusterware and Automatic Storage Management. If you plan afterward to install Oracle Database with Oracle Real Application Clusters (Oracle RAC), then this is phase one of a two-phase installation.

This chapter contains the following topics:

- Preparing to Install Oracle Grid Infrastructure with OUI
- Installing Grid Infrastructure
- Installing Grid Infrastructure Using a Software-Only Installation
- Confirming Oracle Clusterware Function
- Confirming Oracle ASM Function for Oracle Clusterware Files

4.1 Preparing to Install Oracle Grid Infrastructure with OUI

Before you install Oracle grid infrastructure with the installer, use the following checklist to ensure that you have all the information you will need during installation, and to ensure that you have completed all tasks that must be done before starting your installation. Check off each task in the following list as you complete it, and write down the information needed, so that you can provide it during installation.

❏ **Shut Down Running Oracle Processes**

You may need to shut down running Oracle processes:

Installing on a node with a standalone database not using Oracle ASM: You do not need to shut down the database while you install Oracle grid infrastructure software.

Installing on a node that already has a standalone Oracle Database 11g release 2 (11.2) installation running on Oracle ASM: Stop the existing Oracle ASM instances. After the software is installed, start the Oracle ASM instances again.

Installing on an Oracle RAC Database node: This installation requires an upgrade of Oracle Clusterware, as Oracle Clusterware is required to run Oracle RAC. As part of the upgrade, you must shut down the database one node at a time as the rolling upgrade proceeds from node to node.

> **Note:** If you are upgrading an Oracle RAC 9*i* release 2 (9.2) node, and the TNSLSNR is listening to the same port on which the SCAN listens (default 1521), then the TNSLSNR should be shut down.

If a Global Services Daemon (GSD) from Oracle9*i* Release 9.2 or earlier is running, then stop it before installing Oracle grid infrastructure by running the following command:

```
$ Oracle_home/bin/gsdctl stop
```

where `Oracle_home` is the Oracle Database home that is running the GSD.

> **Note:** If you receive a warning to stop all Oracle services after starting OUI, then run the command
>
> `Oracle_home/bin/localconfig delete`
>
> where `Oracle_home` is the existing Oracle Clusterware home.

❏ **Prepare for Automatic Storage Management and Oracle Clusterware Upgrade If You Have Existing Installations**

During installation, you can upgrade existing Oracle Clusterware and cluster Oracle ASM installations.

When all member nodes of the cluster are running Oracle grid infrastructure 11*g* release 2 (11.2), then the new clusterware becomes the active version.

If you intend to install Oracle RAC, then you must first complete the upgrade to Oracle grid infrastructure 11*g* release 2 (11.2) on all cluster nodes before you install the Oracle Database 11*g* release 2 (11.2) version of Oracle RAC.

> **Note:** All Oracle grid infrastructure upgrades (upgrades of existing Oracle Clusterware and Oracle ASM installations) are out-of-place upgrades.

❏ **Determine the Oracle Inventory (oraInventory) location**

If you have already installed Oracle software on your system, then OUI detects the existing Oracle Inventory (oraInventory) directory from the `/var/opt/oracle/oraInst.loc` file, and uses this location. This directory is the central inventory of Oracle software installed on your system. Users who have the Oracle Inventory group as their primary group are granted the OINSTALL privilege to write to the central inventory.

If you are installing Oracle software for the first time on your system, and your system does not have an oraInventory directory, then the installer designates the installation owner's primary group as the Oracle Inventory group. Ensure that this group is available as a primary group for all planned Oracle software installation owners.

> **Note:** The oraInventory directory cannot be placed on a shared file system.

> **See Also:** The preinstallation chapters in Chapter 2 for information about creating the Oracle Inventory, and completing required system configuration

❏ **Obtain root account access**

During installation, you are asked to run configuration scripts as the `root` user. You must run these scripts as `root`, or be prepared to have your system administrator run them for you. You must run the `root.sh` script on the first node and wait for it to finish. If your cluster has four or more nodes, then `root.sh` can be run concurrently on all nodes but the first and last.

❏ **Decide if you want to install other languages**

During installation, you are asked if you want translation of user interface text into languages other than the default, which is English.

> **Note:** If the language set for the operating system is not supported by the installer, then by default the installer runs in the English language.

> **See Also:** *Oracle Database Globalization Support Guide* for detailed information on character sets and language configuration

❏ **Determine your cluster name, public node names, the SCAN, virtual node names, GNS VIP and planned interface use for each node in the cluster**

During installation, you are prompted to provide the public and virtual hostname, unless you use a third party cluster software. In that case, the public hostname information will be filled in. You are also prompted to identify which interfaces are public, private, or interfaces in use for another purpose, such as a network file system.

If you use Grid Naming Service (GNS), then OUI displays the public and virtual hostname addresses labeled as "AUTO" because they are configured automatically.

> **Note:** If you configure IP addresses manually, then avoid changing host names after you complete the Oracle grid infrastructure installation, including adding or deleting domain qualifications. A node with a new hostname is considered a new host, and must be added to the cluster. A node under the old name will appear to be down until it is removed from the cluster.

If you use third-party clusterware, then use your vendor documentation to complete setup of your public and private domain addresses.

When you enter the public node name, use the primary host name of each node. In other words, use the name displayed by the `hostname` command.

In addition:

– Provide a cluster name with the following characteristics:

* It must be globally unique throughout your host domain.

* It must be at least one character long and less than 15 characters long.

        *   It must consist of the same character set used for host names, in accordance with RFC 1123: Hyphens (-), and single-byte alphanumeric characters (a to z, A to Z, and 0 to 9). If you use third-party vendor clusterware, then Oracle recommends that you use the vendor cluster name.

– If you are not using Grid Naming Service (GNS), then determine a virtual host name for each node. A virtual host name is a public node name that is used to reroute client requests sent to the node if the node is down. Oracle Database uses VIPs for client-to-database connections, so the VIP address must be publicly accessible. Oracle recommends that you provide a name in the format *hostname*-vip. For example: `myclstr2-vip`.

– Provide SCAN addresses for client access to the cluster. These addresses should be configured as round robin addresses on the domain name service (DNS). Oracle recommends that you supply three SCAN addresses.

Note: The following is a list of additional information about node IP addresses:

- For the local node only, OUI automatically fills in public and VIP fields. If your system uses vendor clusterware, then OUI may fill additional fields.

- Host names and virtual host names are not domain-qualified. If you provide a domain in the address field during installation, then OUI removes the domain from the address.

- Interfaces identified as private for private IP addresses should not be accessible as public interfaces. Using public interfaces for Cache Fusion can cause performance problems.

– Identify public and private interfaces. OUI configures public interfaces for use by public and virtual IP addresses, and configures private IP addresses on private interfaces.

The private subnet that the private interfaces use must connect all the nodes you intend to have as cluster members.

❏ **Identify shared storage for Oracle Clusterware files and prepare storage if necessary**

During installation, you are asked to provide paths for the following Oracle Clusterware files. These files must be shared across all nodes of the cluster, either on Automatic Storage Management, or on a supported file system:

– Voting disks are files that Oracle Clusterware uses to verify cluster node membership and status.

Voting disk files must be owned by the user performing the installation (`oracle` or `grid`), and must have permissions set to 640.

– Oracle Cluster Registry files (OCR) contain cluster and database configuration information for Oracle Clusterware.

Before installation, OCR files must be owned by the user performing the installation (`grid` or `oracle`). That installation user must have `oinstall` as its primary group. During installation, OUI changes ownership of the OCR files to `root`.

If your file system does not have external storage redundancy, then Oracle recommends that you provide two additional locations for the OCR disk, and two additional locations for the voting disks, for a total of six partitions (three for OCR, and three for voting disks). Creating redundant storage locations protects the OCR and voting disk in the event of a failure. To completely protect your cluster, the storage locations given for the copies of the OCR and voting disks should have completely separate paths, controllers, and disks, so that no single point of failure is shared by storage locations.

When you select to store the OCR on Oracle ASM, the default configuration is to create the OCR on one ASM diskgroup. If you create the disk group with normal or high redundancy, then the OCR is protected from physical disk failure.

To protect the OCR from logical disk failure, create another ASM diskgroup after installation and add the OCR to the second diskgroup using the `ocrconfig` command.

> **See Also:** Chapter 2, "Advanced Installation Oracle Grid Infrastructure for a Cluster Preinstallation Tasks" and *Oracle Database Storage Administrator's Guide* for information about adding disks to diskgroups

❏ **Ensure cron jobs do not run during installation**

If the installer is running when daily cron jobs start, then you may encounter unexplained installation problems if your cron job is performing cleanup, and temporary files are deleted before the installation is finished. Oracle recommends that you complete installation before daily cron jobs are run, or disable daily cron jobs that perform cleanup until after the installation is completed.

❏ **Have IPMI Configuration completed and have IPMI administrator account information**

If you intend to use IPMI, then ensure BMC interfaces are configured, and have an administration account username and password to provide when prompted during installation.

For nonstandard installations, if you must change configuration on one or more nodes after installation (for example, if you have different administrator usernames and passwords for BMC interfaces on cluster nodes), then decide if you want to reconfigure the BMC interface, or modify IPMI administrator account information after installation.

❏ **Ensure that the Oracle home path you select for the grid infrastructure home uses only ASCII characters**

This restriction includes installation owner user names, which are used as a default for some home paths, as well as other directory names you may select for paths.

❏ **Unset Oracle environment variables**. If you have set ORA_CRS_HOME as an environment variable, then unset it before starting an installation or upgrade. You should never use ORA_CRS_HOME as an environment variable.

If you have had an existing installation on your system, and you are using the same user account to install this installation, then unset the following environment variables: ORA_CRS_HOME; ORACLE_HOME; ORA_NLS10; TNS_ADMIN

4.2 Installing Grid Infrastructure

This section provides you with information about how to use the installer to install Oracle grid infrastructure. It contains the following sections:

- Running OUI to Install Grid Infrastructure
- Installing Grid Infrastructure Using a Cluster Configuration File

4.2.1 Running OUI to Install Grid Infrastructure

Complete the following steps to install grid infrastructure (Oracle Clusterware and Automatic Storage Management) on your cluster. At any time during installation, if you have a question about what you are being asked to do, click the **Help** button on the OUI page.

1. Change to the /Disk1 directory on the installation media, or where you have downloaded the installation binaries, and start the `runInstaller` command. For example:

   ```
   $ cd /home/grid/oracle_sw/Disk1
   $ ./runInstaller
   ```

2. Select **Typical** or **Advanced** installation.

3. Provide information or run scripts as `root` when prompted by OUI. If you need assistance during installation, click **Help**. Click **Details** to see the log file. If `root.sh` fails on any of the nodes, then you can fix the problem and follow the steps in Section 6.4, "Deconfiguring Oracle Clusterware Without Removing Binaries," rerun `root.sh` on that node, and continue.

   > **Note:** You must run the `root.sh` script on the first node and wait for it to finish. If your cluster has four or more nodes, then `root.sh` can be run concurrently on all nodes but the first and last. As with the first node, the `root.sh` script on the last node must be run separately.

4. After you run `root.sh` on all the nodes, OUI runs Net Configuration Assistant (`netca`) and Cluster Verification Utility. These programs run without user intervention.

5. Automatic Storage Management Configuration Assistant (`asmca`) configures Oracle ASM during the installation.

When you have verified that your Oracle grid infrastructure installation is completed successfully, you can either use it to maintain high availability for other applications, or you can install an Oracle database.

If you intend to install Oracle Database 11*g* release 2 (11.2) with Oracle RAC, then refer to *Oracle Real Application Clusters Installation Guide for HP-UX*.

> **See Also:** *Oracle Real Application Clusters Administration and Deployment Guide* for information about using cloning and node addition procedures, and *Oracle Clusterware Administration and Deployment Guide* for cloning Oracle grid infrastructure

4.2.2 Installing Grid Infrastructure Using a Cluster Configuration File

During installation of grid infrastructure, you are given the option either of providing cluster configuration information manually, or of using a cluster configuration file. A

cluster configuration file is a text file that you can create before starting OUI, which provides OUI with information about the cluster name and node names that it requires to configure the cluster.

Oracle suggests that you consider using a cluster configuration file if you intend to perform repeated installations on a test cluster, or if you intend to perform an installation on many nodes.

To create a cluster configuration file manually:

1. On the installation media, navigate to the directory `/response`.

2. Using a text editor, open the response file `crs_install.rsp`.

3. Follow the directions in that section for creating a cluster configuration file.

4.3 Installing Grid Infrastructure Using a Software-Only Installation

> **Note:** Oracle recommends that only advanced users should perform the software-only installation, as this installation method provides no validation of the installation, and as this installation option requires manual postinstallation steps to enable the grid infrastructure software.

A software-only installation consists of installing Oracle grid infrastructure for a cluster on one node.

If you use the Install Grid Infrastructure Software Only option during installation, then this installs the software binaries on the local node. To complete the installation for your cluster, you must perform the additional steps of configuring Oracle Clusterware and Oracle ASM, creating a clone of the local installation, deploying this clone on other nodes, and then adding the other nodes to the cluster.

To perform a software-only installation:

4.3.1 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. For example:

```
$ cd /home/grid/oracle_sw/Disk1
$ ./runInstaller
```

2. Complete a software-only installation of Oracle grid infrastructure on the first node.

3. When the software has been installed, run the `orainstRoot.sh` script when prompted.

4. The `root.sh` script output provides information about how to proceed, depending on the configuration you plan to complete in this installation. Make note of this information.

   However, ignore the instruction to run the `roothas.pl` script. You must not run this script until completing relink, installing software on other nodes, and completing other required cluster configuration steps.

5. To relink Oracle Clusterware with the Oracle RAC option enabled, run commands similar to the following (in this example, the Grid home is /u01/app/11.2.0/grid):

```
$ cd /u01/app/11.2.0/grid
$ export ORACLE_HOME='pwd'
$ cd rdbms/lib
$ make -f ins_rdmbs.mk rac_on ioracle
```

6. On each remaining node, verify that the cluster node meets installation requirements using the command `runcluvfy.sh stage -pre crsinst`. Ensure that you have completed all storage and server preinstallation requirements.

7. Use Oracle Universal Installer as described in steps 1 through 4 to install the Oracle grid infrastructure software on every remaining node that you want to include in the cluster, and complete a software-only installation of Oracle grid infrastructure on every node.

8. If required relink the Oracle RAC binaries as described in step 5 on every node where you installed the Oracle grid infrastructure software.

4.3.2 Configuring the Software Binaries

When you install or copy Oracle grid infrastructure software on any node, you can defer configuration for a later time. This section provides the procedure for completing configuration after the software is installed or copied on nodes.

To configure and activate software-only grid infrastructure for a cluster installations, complete the following tasks:

1. Using a text editor, modify the template file `/Grid_home/crs/install/crsconfig_params` to create a parameter file for the installer to use to configure the cluster. For example:

```
ORACLE_OWNER=grid
ORA_DBA_GROUP=oinstall
ORA_ASM_GROUP=asm
LANGUAGE_ID='AMERICAN_AMERICA.WE8ISO8859P1'
ORACLE_HOME=/u01/crs
ORACLE_BASE=/u01/crsbase
OCR_LOCATIONS=/u02/stor1/ocr,/u03/stor2/ocr
CLUSTER_NAME=example_cluster
HOST_NAME_LIST=node1,node2
NODE_NAME_LIST=node1,node2
VOTING_DISKS=/u02/stor1/vdsk,/u03/stor2/vdsk,/u04/stor3/vdsk
CRS_STORAGE_OPTION=2
CRS_NODEVIPS='node1-vip/255.255.252.0/lan0,node2-vip/255.255.252.0/lan0'
NODELIST=node1,node2
NETWORKS="lan0"/192.0.2.64:public,"lan1"/192.0.2.65:cluster_interconnect
SCAN_NAME=example-scan.domain
SCAN_PORT=1522
```

2. On all nodes, place the `crsconfig_params` file in the path `Grid_home/crs/install/crsconfig_params`, where `Grid_home` is the path to the Oracle grid infrastructure home for a cluster. For example:

```
$ cp crsconfig_params /u01/app/11.2.0/grid/crs/install/crsconfig_params
```

3. After configuring the `crsconfig_params` file, log in as root, and run the script `Grid_home/crs/install/rootcrs.pl` on each node, using the following syntax:.

Grid_home/perl/lib/perl -IGRID_HOME/perl/lib -I*Grid_home*/crs/install *Grid_home*/crs/install/rootcrs.pl

For example:

```
# /u01/app/11.2.0/grid/perl/lib/perl -I/u01/app/11.2.0/grid/perl/lib \
-I/u01/app/11.2.0/grid/crs/install /u01/app/11.2.0/grid/crs/install/rootcrs.pl
```

4. Using the information you noted from the `root.sh` script output in Section 4.3.1, "Installing the Software Binaries," follow the output of the `root.sh` script, and run the command *Grid_home*/`crs/install/roothas.pl` or *Grid_home*/`crs/install/rootcrs.pl` as required. For example:

```
$ cd /u01/app/11.2.0/grid/crs/install
$ perl rootcrs.pl
```

Use *Grid_home*/`crs/install/roothas.pl` to configure Oracle Grid Infrastructure for a standalone server. Use *Grid_home*/`crs/install/rootcrs.pl` to configure Oracle Grid Infrastructure for a cluster.

> **Note:** Oracle grid infrastructure can be used for standalone servers and for clusters. However, if you first configure Oracle grid infrastructure for a standalone server, and then decide you want to configure Oracle grid infrastructure for a cluster, then you must re-link the Oracle software before you run `rootcrs.pl` to configure Oracle grid infrastructure for a clusters. The **Install Grid Infrastructure Software Only** installation option does not assume a cluster configuration, and therefore does not automatically link the Oracle RAC option.

5. Change directory to `Grid_home`/oui/bin, where `Grid_home` is the path of the Grid Infrastructure home on each cluster member node.

6. Enter the following command syntax, where `Grid_home` is the path of the Grid Infrastructure home on each cluster member node, and `node_list` is a comma-delimited list of nodes on which you want the software enabled:

runInstaller -updateNodeList ORACLE_HOME=*Grid_home* -defaultHomeName

For example

```
$ ./runInstaller -updateNodeList ORACLE_HOME=/u01/app/11.2.0/grid
-defaultHomeName
"CLUSTER_NODES={node_list}" CRS=TRUE
```

To enable the Oracle Clusterware installation on the local node only, enter the following command, where `Grid_home` is the Grid home on the local node, and `node_list` is a comma-delimited list of nodes on which you want the software enabled:

runInstaller -updateNodeList ORACLE_HOME=*Grid_home* -defaultHomeName "CLUSTER_NODES={*node_list*}" CRS=TRUE -local

For example:

```
$ ./runInstaller -updateNodeList ORACLE_HOME=/u01/app/11.2.0/grid
-defaultHomeName
"CLUSTER_NODES={node_list}" CRS=TRUE -local
```

4.4 Confirming Oracle Clusterware Function

After installation, log in as `root`, and use the following command syntax on each node to confirm that your Oracle Clusterware installation is installed and running correctly:

crsctl check crs

For example:

```
$ crsctl check crs

CRS-4638: Oracle High Availability Services is online
CRS-4537: Cluster Ready Services is online
CRS-4529: Cluster Synchronization Services is online
CRS-4533: Event Manager is online
```

> **Caution:** After installation is complete, do not remove manually or run cron jobs that remove /tmp/.oracle or /var/tmp/.oracle or its files while Oracle Clusterware is up. If you remove these files, then Oracle Clusterware could encounter intermittent hangs, and you will encounter error CRS-0184: Cannot communicate with the CRS daemon.

4.5 Confirming Oracle ASM Function for Oracle Clusterware Files

If you installed the OCR and voting disk files on Oracle ASM, then use the following command syntax as the Grid Infrastructure installation owner to confirm that your Oracle ASM installation is running:

srvctl status asm

For example:

```
$ srvctl status asm
ASM is running on node1,node2
```

Oracle ASM is running only if it is needed for Oracle Clusterware files. If you have not installed OCR and voting disks files on Oracle ASM, then the Oracle ASM instance should be down.

> **Note:** To manage Oracle ASM or Oracle Net 11*g* release 2 (11.2) or later installations, use the `srvctl` binary in the Oracle grid infrastructure home for a cluster (Grid home). If you have Oracle Real Application Clusters or Oracle Database installed, then you cannot use the `srvctl` binary in the database home to manage Oracle ASM or Oracle Net.

5

Oracle Grid Infrastructure Postinstallation Procedures

This chapter describes how to complete the postinstallation tasks after you have installed the Oracle grid infrastructure software.

This chapter contains the following topics:

- Required Postinstallation Tasks
- Recommended Postinstallation Tasks
- Using Older Oracle Database Versions with Grid Infrastructure
- Modifying Oracle Clusterware Binaries After Installation

5.1 Required Postinstallation Tasks

You must perform the following tasks after completing your installation:

- Download and Install Patch Updates

Note: In prior releases, backing up the voting disks using a `dd` command was a required postinstallation task. With Oracle Clusterware release 11.2 and later, backing up and restoring a voting disk using the `dd` command may result in the loss of the voting disk, so this procedure is not supported.

5.1.1 Download and Install Patch Updates

Refer to the My Oracle Support Web site for required patch updates for your installation.

Note: Browsers require an Adobe Flash plug-in, version 9.0.115 or higher to use My Oracle Support. Check your browser for the correct version of Flash plug-in by going to the Adobe Flash checker page, and installing the latest version of Adobe Flash.

If you do not have Flash installed, then download the latest version of the Flash Player from the Adobe Web site:

`http://www.adobe.com/go/getflashplayer`

To download required patch updates:

1. Use a Web browser to view the My Oracle Support Web site:

   https://metalink.oracle.com

2. Log in to My Oracle Support Web site.

   > **Note:** If you are not a My Oracle Support registered user, then click **Register for My Oracle Support** and register.

3. On the main My Oracle Support page, click **Patches & Updates**.

4. On the Patches & Update page, in the Patch Search frame, type **Oracle Database**. and select the release and your platform from the list selections, and click **Search**.

5. Any available patch updates appear under the Patch Results heading.

6. Click the patch number to download the patch.

7. On the Patch Set page, click **View README** and read the page that appears. The README page contains information about the patch set and how to apply the patches to your installation.

8. Return to the Patch Set page, click **Download**, and save the file on your system.

9. Use the unzip utility provided with Oracle Database 11*g* release 2 (11.2) to uncompress the Oracle patch updates that you downloaded from My Oracle Support. The unzip utility is located in the `$ORACLE_HOME/bin` directory.

10. Refer to Appendix E on page E-1 for information about how to stop database processes in preparation for installing patches.

5.2 Recommended Postinstallation Tasks

Oracle recommends that you complete the following tasks as needed after installing Oracle grid infrastructure:

- Back Up the root.sh Script
- Install Cluster Health Management
- Tune Semaphore Parameters
- Create a Fast Recovery Area Disk Group

5.2.1 Back Up 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 the 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 `root.sh` file copy.

5.2.2 Install Cluster Health Management

To address troubleshooting issues, Oracle recommends that you install OS Watcher and RACDDT

5.2.2.1 Installing OS Watcher and RACDDT

Install OS Watcher to help resolve operating system issues with your cluster. If you intend to install an Oracle RAC database, then also install RACDDT. You must have access to My Oracle Support to download OS Watcher and RACDDT.

OS Watcher (OSW) is a collection of UNIX/Linux shell scripts that collect and archive operating system and network metrics to aid Oracle Support in diagnosing various issues related to system and performance. OSW operates as a set of background processes on the server and gathers operating system data on a regular basis. The scripts use common utilities such as `vmstat`, `netstat` and `iostat`.

RACDDT is a data collection tool designed and configured specifically for gathering diagnostic data related to Oracle RAC technology. RACDDT is a set of scripts and configuration files that is run on one or more nodes of an Oracle RAC cluster. The main script is written in Perl, while a number of proxy scripts are written using Korn shell. RACDDT will run on all supported UNIX and Linux platforms, but is not supported on any Windows platforms.

OSW is also included in the RACDDT script file, but is not installed by RACDDT. OSW must be installed on each node where data is to be collected.

To download binaries for OS Watcher and RACDDT, go to the following URL:

https://metalink.oracle.com

Download OSW by searching for OS Watcher, and downloading the binaries from the User Guide bulletin. Installation instructions for OSW are provided in the user guide. Download RACDDT by searching for RACDDT, and downloading the binaries from the RACDDT User Guide bulletin.

5.2.3 Tune 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:

    2 * sum (process parameters of all database instances on the system) + overhead for background processes + system and other application requirements

2. Set `semmns` (total semaphores systemwide) to this total.

3. Set `semmsl` (semaphores for each set) to 256.

4. Set `semmni` (total semaphores sets) to `semmns` divided by `semmsl`, rounded up to the nearest multiple of 1024.

5.2.4 Create a Fast Recovery Area Disk Group

During installation, by default you can create one disk group. If you plan to add an Oracle Database for a standalone server or an Oracle RAC database, then you should create the Fast Recovery Area for database files.

5.2.4.1 About the Fast Recovery Area and the Fast Recovery Area Disk Group

The Fast Recovery Area is a unified storage location for all Oracle Database 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 Flash 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 Database files can be placed on the same disk group, and you can also place flash recovery files in the same disk group. However, Oracle recommends that you create a separate Flash 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_SIZE. 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 data files and control files, the online redo logs, and the archived redo log files needed to recover your database using the data file 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 Area for each database depending on the importance of each database. For example, if database1 is your least important database, database 2 is of greater importance and database 3 is of greatest importance, then you can set different DB_RECOVERY_FILE_DEST_SIZE settings for each database to meet your retention target for each database: 30 GB for database 1, 50 GB for database 2, and 70 GB for database 3.

> **See Also:** *Oracle Database Storage Administrator's Guide*

5.2.4.2 Creating the Fast Recovery Area Disk Group

To create a flash recovery file disk group:

1. Navigate to the Grid home bin directory, and start ASM Configuration Assistant (`asmca`). For example:

   ```
   $ cd /u01/app/11.2.0/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**.

5.3 Using Older Oracle Database Versions with Grid Infrastructure

Review the following sections for information about using older Oracle Database releases with 11*g* release 2 (11.2) grid infrastructure installations:

- General Restrictions for Using Older Oracle Database Versions
- Pinning Cluster Nodes for Oracle Database Release 10.x or 11.x
- Enabling The Global Services Daemon (GSD) for Oracle Database Release 9.2
- Using the Correct LSNRCTL Commands

5.3.1 General Restrictions for Using Older Oracle Database Versions

You can use Oracle Database release 9.2, release 10.x and release 11.1 with Oracle Clusterware 11*g* release 2 (11.2).

To use Oracle Real Application Clusters release 9.2 with Oracle Clusterware 11*g* release 2 (11.2), install and run Oracle9*i* Cluster Manager for the release 9.2 database. Oracle9*i* Cluster Manager can coexist with Oracle Clusterware.

If you upgrade an existing version of Oracle Clusterware and Oracle ASM to Oracle grid infrastructure release 11.2 (which includes Oracle Clusterware and Oracle ASM), and you also plan to upgrade your Oracle RAC database to 11.2, then the required configuration of existing databases is completed automatically when you complete the Oracle RAC upgrade, and this section does not concern you.

However, if you upgrade to release 11.2 Oracle grid infrastructure, and you have existing Oracle RAC installations you do not plan to upgrade, or if you install older versions of Oracle RAC (9.2, 10.2 or 11.1) on a release 11.2 Oracle grid infrastructure cluster, then you must complete additional configuration tasks or apply patches, or both, before the older databases will work correctly with Oracle grid infrastructure.

> **Note:** Before you start an Oracle RAC or Oracle Database installation on an Oracle Clusterware release 11.2 installation, if you are upgrading from releases 11.1.0.7, 11.1.0.6, and 10.2.0.4, then Oracle recommends that you check for the latest recommended patches for the release you are upgrading from, and install those patches as needed on your existing database installations before upgrading.
>
> For more information on recommended patches, refer to "Oracle Upgrade Companion," which is available through Note 785351.1 on My Oracle Support:
>
> https://metalink.oracle.com
>
> You may also refer to Notes 756388.1 and 756671.1 for the current list of recommended patches for each release

5.3.2 Pinning Cluster Nodes for Oracle Database Release 10.x or 11.x

When Oracle Database version 10.x or 11x is installed on a new Oracle grid infrastructure for a cluster configuration, it is configured for dynamic cluster configuration, in which some or all IP addresses are provisionally assigned, and other

cluster identification information is dynamic. This configuration is incompatible with older database releases, which require fixed addresses and configuration.

You can change the nodes where you want to run the older database to create a persistent configuration. Creating a persistent configuration for a node is called pinning a node.

To pin a node in preparation for installing an older Oracle Database version, use *Grid_home*/bin/crsctl with the following command syntax, where *nodes* is a space-delimited list of one or more nodes in the cluster whose configuration you want to pin:

```
crsctl pin css -n nodes
```

For example, to pin nodes node3 and node4, log in as root and enter the following command:

```
$ crsctl pin css -n node3 node4
```

To determine if a node is in a pinned or unpinned state, use *Grid_home*/bin/olsnodes with the following command syntax:

To list all pinned nodes:

```
olsnodes -t -n
```

For example:

```
# /u01/app/11.2.0/grid/bin/olsnodes -t -n
node1 1      Pinned
node2 2      Pinned
node3 3      Pinned
node4 4      Pinned
```

To list the state of a particular node:

```
olsnodes -t -n node3
```

For example:

```
# /u01/app/11.2.0/grid/bin/olsnodes -t -n node3
node3 3      Pinned
```

> **See Also:** *Oracle Clusterware Administration and Deployment Guide* for more information about pinning and unpinning nodes

5.3.3 Enabling The Global Services Daemon (GSD) for Oracle Database Release 9.2

When Oracle Database 9*i* release 2 (9.2) is installed on an 11*g* release 2 (11.2) Oracle grid infrastructure for a cluster configuration, the Global Services daemon (GSD) is disabled by default. Use the following commands to enable the GSD before you install a release 9.2 Oracle Database:

```
srvctl enable nodeapps -g
srvctl start nodeapps
```

5.3.4 Using the Correct LSNRCTL Commands

To administer 11*g* release 2 local and scan listeners using the lsnrctl command, set your $ORACLE_HOME environment variable to the path for the grid infrastructure

home (Grid home). Do not attempt to use the `lsnrctl` commands from Oracle home locations for previous releases, as they cannot be used with the new release.

5.4 Modifying Oracle Clusterware Binaries After Installation

After installation, if you need to modify the Oracle Clusterware configuration, then you must unlock the Grid home.

For example, if you want to apply a one-off patch, or if you want to modify an Oracle Exadata configuration to run IPC traffic over RDS on the interconnect instead of using the default UDP, then you must unlock the Grid home.

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.

Unlock the home using the following procedure:

1. Change directory to the path *Grid_home*/crs/install, where *Grid_home* is the path to the Grid home, and unlock the Grid home using the command `rootcrs.pl -unlock -crshome Grid_home`, where Grid_home is the path to your Grid infrastructure home. For example, with the grid home `/u01/app/11.2.0/grid`, enter the following command:

   ```
   # cd /u01/app/11.2.0/grid/crs/install
   # perl rootcrs.pl -unlock -crshome /u01/app/11.2.0/grid
   ```

2. Change user to the grid infrastructure software owner, and relink binaries using the command syntax make -f *Grid_home*/lib/ins_rdbms.mk *target*, where *Grid_home* is the Grid home, and *target* is the binaries that you want to relink. For example, where the grid user is `grid`, $ORACLE_HOME is set to the Grid home, and where you are updating the interconnect protocol from UDP to IPC, enter the following command:

   ```
   # su grid
   $ make -f $ORACLE_HOME/rdbms/lib/ins_rdbms.mk ipc_rds ioracle
   ```

   Note: To relink binaries, you can also change to the grid installation owner and run the command `Grid_home/bin/relink`.

   ---

3. Relock the Grid home and restart the cluster using the following command:

   ```
   # perl rootcrs.pl -patch
   ```

4. Repeat steps 1 through 3 on each cluster member node.

6

How to Modify or Deinstall Oracle Grid Infrastructure

This chapter describes how to remove Oracle Clusterware and Oracle ASM.

This chapter contains the following topics:

- Deciding When to Deinstall Oracle Clusterware
- Migrating Standalone Grid Infrastructure Servers to a Cluster
- Relinking Oracle Grid Infrastructure for a Cluster Binaries
- Deconfiguring Oracle Clusterware Without Removing Binaries
- Removing Oracle Clusterware and ASM

> **See Also:** Product-specific documentation for requirements and restrictions to remove an individual product

6.1 Deciding When to Deinstall Oracle Clusterware

Remove installed components in the following situations:

- You have successfully installed Oracle Clusterware, and you want to remove the Clusterware installation, either in an educational environment, or a test environment.
- You have encountered errors during or after installing or upgrading Oracle Clusterware, and you want to reattempt an installation.
- Your installation or upgrade stopped because of a hardware or operating system failure.
- You are advised by Oracle Support to reinstall Oracle Clusterware.

6.2 Migrating Standalone Grid Infrastructure Servers to a Cluster

If you have an Oracle Database installation using Oracle Restart (that is, an Oracle grid infrastructure installation for a standalone server), and you want to configure that server as a cluster member node, then complete the following tasks:

1. Inspect the Oracle configuration with `srvctl` using the following syntax, where *db_unique_name* is the unique name for the database, and *lsnrname* is the name of the listeners:

   srvctl config database -d *db_unique_name*

   srvctl config service -d *db_unique_name*

srvctl config listener -l *lsnrname*

Write down the configuration information for the server.

2. Change directory to *Grid home*/crs/install. For example:

   ```
   # cd /u01/app/11.2.0/grid/crs/install
   ```

3. Stop all of the databases, services, and listeners that you discovered in step 1.

4. Deconfigure and deinstall the Oracle grid infrastructure installation for a standalone server, using the following command:

   ```
   # roothas.pl -deinstall
   ```

5. Prepare the server for Oracle Clusterware configuration, as described in this document.

6. Clone the Oracle grid infrastructure for a cluster software from an existing node, or install and configure Oracle grid infrastructure for a cluster.

7. Add the Oracle Database for support by Oracle grid infrastructure for a cluster, using the configuration information you recorded in step 1. Use the following command syntax, where *db_unique_name* is the unique name of the database on the node, and nodename is the name of the node:

   srvctl add database -d db_unique_name -o $ORACLE_HOME -x nodename

   For example, with the database name mydb_node1, and the nodename node1, enter the following command:

   ```
   srvctl add database -d mydb_node1 -o $ORACLE_HOME -x node1
   ```

8. Add each service to the database, using the command `srvctl add service`.

6.3 Relinking Oracle Grid Infrastructure for a Cluster Binaries

After installing Oracle grid infrastructure for a cluster (Oracle Clusterware and Oracle ASM configured for a cluster), if you need to modify the binaries, then use the following procedure, where `Grid_home` is the grid infrastructure for a cluster home:

> **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.

As root:

```
# cd Grid_home/crs/install
# perl rootcrs.pl -unlock
```

As the grid infrastructure for a cluster owner:

```
$ export ORACLE_HOME=Grid_home
$ Grid_home/bin/relink
```

As root again:

```
# cd Grid_home/crs/install
# perl rootcrs.pl -patch
```

You must relink the Oracle Clusterware and Oracle ASM binaries every time you apply an operating system patch or after an operating system upgrade.

6.4 Deconfiguring Oracle Clusterware Without Removing Binaries

Running the `rootcrs.pl` command flags `-deconfig -force` enables you to deconfigure Oracle Clusterware on one or more nodes without removing installed binaries. This feature is useful if you encounter an error on one or more cluster nodes during installation when running the `root.sh` command, such as a missing operating system package on one node. By running `rootcrs.pl -deconfig -force` on nodes where you encounter an installation error, you can deconfigure Oracle Clusterware on those nodes, correct the cause of the error, and then run `root.sh` again.

> **Note:** Stop any databases, services, and listeners that may be installed and running before deconfiguring Oracle Clusterware.

To deconfigure Oracle Clusterware:

1. Log in as the `root` user on a node where you encountered an error.

2. Change directory to Grid_home/crs/install. For example:

    ```
    # cd /u01/app/11.2.0/grid/crs/install
    ```

3. Run rootcrs.pl with the -deconfig -force flags. For example:

    ```
    # perl rootcrs.pl -deconfig -force
    ```

    Repeat on other nodes as required.

4. If you are deconfiguring Oracle Clusterware on all nodes in the cluster, then on the last node, enter the following command:

    ```
    # perl rootcrs.pl -deconfig -force -lastnode
    ```

    The `-lastnode` flag completes deconfiguration of the cluster, including the OCR and voting disks.

6.5 Removing Oracle Clusterware and ASM

The `deinstall` command removes Oracle Clusterware and ASM from your server. 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 for Oracle Clusterware and ASM

- Example of a Deinstallation Parameter File for Grid Infrastructure for a Cluster

6.5.1 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 `deinstall` command stops Oracle software, and removes Oracle software and configuration files on the operating system.

The command uses the following syntax, where variable content is indicated by 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 grid home. For example:

```
$ cd /u01/app/11.2.0/grid/deinstall
$ ./deinstall
```

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 noninteractive mode. This option requires a properties file that contains the configuration values for the Oracle home that is being deinstalled or deconfigured.

  To create a properties file and provide the required parameters, refer to the template file `deinstall.rsp.tmpl`, located in the `response` folder. If you prefer, instead of using the template file, you can generate a properties file by using the `-checkonly` option to have `deinstall` discover 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.

- ■ `-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.

- ■ `-local`

  Use this flag on a multinode environment to deconfigure 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. If you are running the deinstall command from the Oracle home that you plan to deinstall, then you do not need to use the `-paramfile` flag.

  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 name2=value name3=value* ...]

  Use this flag with a parameter file to override one or more values 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.

6.5.2 Example of Running the Deinstall Command for Oracle Clusterware and ASM

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.

To run the deinstall command from an Oracle grid infrastructure for a cluster home, enter the following command:

```
$ cd /u01/app/11.2.0/grid/deinstall/
$ ./deinstall
```

You can run generate a deinstall parameter file by running the deinstall command using the -checkonly flag before you run the command to deinstall the home, or you can use the response file template and manually edit it to create the parameter file to use with the deinstall command.

6.5.3 Example of a Deinstallation Parameter File for Grid Infrastructure for a Cluster

You can run the deinstall command with the -paramfile option to use the values you specify in the parameter file. The following is an example of a parameter file for a cluster on nodes node1 and node2, in which the Oracle grid infrastructure for a cluster software binary owner is grid, the Oracle grid infrastructure home (Grid home) is in the path /u01/app/11.2.0/grid, the Oracle base (the Oracle base for grid infrastructure, containing Oracle ASM log files, Oracle Clusterware logs, and other administrative files) is /u01/app/11.2.0/grid/, the central Oracle Inventory home (oraInventory) is /u01/app/oraInventory, the virtual IP addresses (VIP) are 192.0.2.2 and 192.0.2.4, the local node (the node where you are running the deinstallation session from) is node1:

```
#Copyright (c) 2005, 2006 Oracle Corporation.  All rights reserved.
#Fri Feb 06 00:08:58 PST 2009
LOCAL_NODE=node1
HOME_TYPE=CRS
ASM_REDUNDANCY=\
ORACLE_BASE=/u01/app/11.2.0/grid/
VIP1_MASK=255.255.252.0
NEW_NODEVIPS='node1-vip/255.255.252.0/lan0,node2-vip/255.255.252.0/lan0'
VOTING_DISKS=/u02/storage/grid/vdsk
SCAN_PORT=1522
silent=true
ASM_UPGRADE=false
ORA_CRS_HOME=/u01/app/11.2.0/grid
GPNPCONFIGDIR=$ORACLE_HOME
LOGDIR=/home/grid/SH/deinstall/logs/
GPNPGCONFIGDIR=$ORACLE_HOME
ORACLE_OWNER=grid
NODELIST=node1,node2
CRS_STORAGE_OPTION=2
NETWORKS="lan0"/192.0.2.1\:public,"lan1"/10.0.0.1\:cluster_interconnect
VIP1_IP=192.0.2.2
NETCFGJAR_NAME=netcfg.jar
ORA_DBA_GROUP=dba
CLUSTER_NODES=node1,node2
JREDIR=/u01/app/11.2.0/grid/jdk/jre
VIP1_IF=lan0
REMOTE_NODES=node2
VIP2_MASK=255.255.252.0
ORA_ASM_GROUP=asm
LANGUAGE_ID='AMERICAN_AMERICA.WE8ISO8859P1'
CSS_LEASEDURATION=400
NODE_NAME_LIST=node1,node2
SCAN_NAME=node1scn
SHAREJAR_NAME=share.jar
HELPJAR_NAME=help4.jar
SILENT=false
local=false
INVENTORY_LOCATION=/u01/app/oraInventory
GNS_CONF=false
JEWTJAR_NAME=jewt4.jar
OCR_LOCATIONS=/u02/storage/grid/ocr
EMBASEJAR_NAME=oemlt.jar
ORACLE_HOME=/u01/app/11.2.0/grid
CRS_HOME=true
VIP2_IP=192.0.2.4
ASM_IN_HOME=n
EWTJAR_NAME=ewt3.jar
HOST_NAME_LIST=node1,node2
JLIBDIR=/u01/app/11.2.0/grid/jlib
VIP2_IF=lan0
VNDR_CLUSTER=false
CRS_NODEVIPS='node1-vip/255.255.252.0/lan0,node2-vip/255.255.252.0/lan0'
CLUSTER_NAME=node1-cluster
```

A

Troubleshooting the Oracle Clusterware Installation Process

This appendix provides troubleshooting information for installing Oracle Clusterware.

> **See Also:** The Oracle Database 11*g* Oracle RAC documentation set included with the installation media in the Documentation directory:
>
> - *Oracle Clusterware Administration and Deployment Guide*
> - *Oracle Real Application Clusters Administration and Deployment Guide*

This appendix contains the following topics:

- Install OS Watcher and RACDDT
- General Installation Issues
- Performing Cluster Diagnostics During Oracle Clusterware Installations
- Interconnect Errors

A.1 Install OS Watcher and RACDDT

To address troubleshooting issues, Oracle recommends that you install OS Watcher, and if you intend to install an Oracle RAC database, RACDDT. You must have access to Oracle*MetaLink* to download OS Watcher and RACDDT.

OS Watcher (OSW) is a collection of UNIX/Linux shell scripts that collect and archive operating system and network metrics to aid Oracle Support in diagnosing various issues related to system and performance. OSW operates as a set of background processes on the server and gathers operating system data on a regular basis. The scripts use common utilities such as `vmstat`, `netstat` and `iostat`.

RACDDT is a data collection tool designed and configured specifically for gathering diagnostic data related to Oracle RAC technology. RACDDT is a set of scripts and configuration files that is run on one or more nodes of an Oracle RAC cluster. The main script is written in Perl, while a number of proxy scripts are written using Korn shell. RACDDT will run on all supported UNIX and Linux platforms, but is not supported on any Windows platforms.

OSW is also included in the RACDDT script file, but is not installed by RACDDT. OSW must be installed on each node where data is to be collected.

To download binaries for OS Watcher and RACDDT, go to the following URL:

https://metalink.oracle.com

Download OSW by searching for OS Watcher, and downloading the binaries from the User Guide bulletin. Installation instructions for OSW are provided in the user guide. Download RACDDT by searching for RACDDT, and downloading the binaries from the RACDDT User Guide bulletin.

A.2 General Installation Issues

The following is a list of examples of types of errors that can occur during installation. It contains the following issues:

- An error occurred while trying to get the disks

- Failed to connect to server, Connection refused by server, or Can't open display

- Nodes unavailable for selection from the OUI Node Selection screen

- Node nodename is unreachable

- PROT-8: Failed to import data from specified file to the cluster registry

- Time stamp is in the future

- Timed out waiting for the CRS stack to start

An error occurred while trying to get the disks

Cause: There is an entry in /etc/oratab pointing to a non-existent Oracle home. The OUI error file should show the following error: "java.io.IOException: /home/oracle/OraHome//bin/kfod: not found" (Oracle*Metalink* bulletin 276454.1)

Action: Remove the entry in /etc/oratab pointing to a non-existing Oracle home.

Failed to connect to server, Connection refused by server, or Can't open display

Cause: These are typical of X Window display errors on Windows or UNIX systems, where xhost is not properly configured.

Action: In a local terminal window, log in as the user that started the X Window session, and enter the following command:

$ xhost *fully_qualified_remote_host_name*

For example:

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

Then, enter the following commands, where `workstation_name` is the host name or IP address of your workstation.

Bourne, Bash, or Korn shell:

```
$ DISPLAY=workstation_name:0.0
$ export DISPLAY
```

To determine whether X Window applications display correctly on the local system, enter the following command:

```
$ xclock
```

The X clock should appear on your monitor.

If the X clock appears, then close the X clock and start Oracle Universal Installer again.

Nodes unavailable for selection from the OUI Node Selection screen

Cause: Oracle Clusterware is either not installed, or the Oracle Clusterware services are not up and running.

Action: Install Oracle Clusterware, or review the status of your Oracle Clusterware. Consider restarting the nodes, as doing so may resolve the problem.

Node *nodename* is unreachable

Cause: Unavailable IP host

Action: Attempt the following:

1. Run the shell command `netstat -in`. Compare the output of this command with the contents of the `/etc/hosts` file to ensure that the node IP is listed.

2. Run the shell command `nslookup` to see if the host is reachable.

3. As the `oracle` user, attempt to connect to the node with `ssh` or `rsh`. If you are prompted for a password, then user equivalence is not set up properly. The installer should configure SSH for you. If you are unable to use automatic SSH configuration, then review the section Appendix D.1, "Configuring SSH Manually on All Cluster Nodes."

PROT-8: Failed to import data from specified file to the cluster registry

Cause: Insufficient space in an existing Oracle Cluster Registry device partition, which causes a migration failure while running `rootupgrade`. To confirm, look for the error "utopen:12:Not enough space in the backing store" in the log file `$ORA_CRS_HOME/log/`*hostname*`/client/ocrconfig_`*pid*`.log`.

Action: Identify a storage device that has 280 MB or more available space. Locate the existing raw device name from `/var/opt/oracle/srvConfig.loc`, and copy the contents of this raw device to the new device using the command `dd`.

Time stamp is in the future

Cause: One or more nodes has a different clock time than the local node. If this is the case, then you may see output similar to the following:

```
time stamp 2005-04-04 14:49:49 is 106 s in the future
```

Action: Ensure that all member nodes of the cluster have the same clock time.

Timed out waiting for the CRS stack to start

Cause: If a configuration issue prevents the Oracle grid infrastructure software from installing successfully on all nodes, then you may see error messages such as "Timed out waiting for the CRS stack to start," or you may notice that Oracle Clusterware-managed resources were not create on some nodes after you exit the installer. You also may notice that resources have a status other than ONLINE.

Action: Deconfigure the grid infrastructure installation without removing binaries, and review log files to determine the cause of the configuration issue. After you have fixed the configuration issue, rerun the scripts used during installation to configure Oracle Clusterware.

> **See Also:** Section 6.4, "Deconfiguring Oracle Clusterware Without Removing Binaries"

A.3 Performing Cluster Diagnostics During Oracle Clusterware Installations

If Oracle Universal Installer (OUI) does not display the Node Selection page, then perform clusterware diagnostics by running the `olsnodes -v` command from the binary directory in your Oracle Clusterware home *(CRS_home*/bin on Linux and UNIX-based systems, and *CRS_home*\BIN on Windows-based systems) and analyzing its output. Refer to your clusterware documentation if the detailed output indicates that your clusterware is not running.

In addition, use the following command syntax to check the integrity of the Cluster Manager:

```
cluvfy comp clumgr -n node_list -verbose
```

In the preceding syntax example, the variable *node_list* is the list of nodes in your cluster, separated by commas.

A.4 Interconnect Errors

If you use more than one NIC for the interconnect, then you must use NIC bonding, or the interconnect will fail.

If you install Oracle Clusterware and Oracle RAC, then they must use the same NIC or bonded NIC cards for the interconnect.

If you use bonded NIC cards, then they must be on the same subnet.

B

Installing and Configuring Oracle Database 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 the Installer Using a Response File
- Running Net Configuration Assistant Using a Response File
- Running Database Configuration Assistants Using Response Files
- Postinstallation Configuration Using a Response File

How Response Files Work

When you start the installer, you can use a response file to automate the installation and configuration of Oracle software, either fully or partially. The installer uses the values contained in the response file to provide answers to some or all installation prompts.

Typically, the 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 the installer from 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 the installer, then it runs in silent mode. During a silent mode installation, the 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 the installer runs in response file mode. During a response file mode installation, the 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.

You define the settings for a silent or response file installation by entering values for the variables listed in the response file. For example, to specify the Oracle home name, supply the appropriate value for the ORACLE_HOME variable:

```
ORACLE_HOME="OraDBHome1"
```

Another way of specifying the response file variable settings is to pass them as command line arguments when you run the installer. For example:

```
-silent "ORACLE_HOME=OraDBHome1" ...
```

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=binks342" ...
```

Ensure that you enclose the variable and its setting in quotes.

> **See Also:** *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX* for more information about response files

Reasons for Using Silent Mode or Response File Mode

The following table provides use cases for running the installer in silent mode or response file mode.

Mode	Uses
Silent	Use silent mode to do the following installations: ■ Complete an unattended installation, which you schedule using operating system utilities such as at. ■ 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. The installer displays progress information on the terminal that you used to start it, but it does not display any of the installer screens.
Response file	Use response file mode to complete similar Oracle software installations on multiple systems, providing default answers to some, but not all of the 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.

General Procedure for Using Response Files

The following are the general steps to install and configure Oracle products using the installer in silent or response file mode:

> **Note:** You must complete all required preinstallation tasks on a system before running the installer in silent or response file mode.

1. Create the oraInst.loc file if it is not present on the server.

2. Prepare a response file.

3. Run the installer in silent or response file mode.

4. If you completed a software-only installation, then run Net Configuration Assistant and Database Configuration Assistant in silent or response file mode.

These steps are described in the following sections.

Creating the oraInst.loc File

If you plan to install Oracle products using the installer in silent or response file mode, and an `oraInst.loc` file does not already exist, then you must manually create the `oraInst.loc` file. This file specifies the location of the Oracle Inventory directory, which is where the installer creates the central inventory of Oracle products installed on the system.

> **Note:** If Oracle software has been installed previously on the system, then the `oraInst.loc` file should already exist. If the file does exist, then you do not need to create this file.

To create the `oraInst.loc` file, follow these steps:

1. Switch user to `root`:

   ```
   $ su - root
   ```

2. Change directory:

   ```
   # cd /var/opt/oracle
   ```

3. Use a text editor to create the `oraInst.loc` file, containing the following lines:

   ```
   inventory_loc=$ORACLE_BASE/oraInventory
   inst_group=oinstall
   ```

   This example assumes that the `$ORACLE_BASE` environment variable for the Oracle software installation owner is set to the path of the Oracle base directory, such as `/u01/app/oracle`.

4. Set the ownership of the `oraInst.loc` file to an Oracle software installation owner, and to members of the oraInventory group, and change permissions to 664. For example, if the installation owner is `oracle`, and the oraInventory group is `oinstall`, then enter the following commands:

   ```
   # chown oracle:oinstall oraInst.loc
   # chmod 664 oraInst.loc
   ```

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
- Recording a Response File

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 at `database/response` directory on the installation media.

> **Note:** If you copied the software to a hard disk, then the response files are located in the directory /response.

Table B–1 lists the response files provided with this software:

Table B–1   Response Files for Oracle Database

Response File	Description
db_install.rsp	Silent installation of Oracle Database 11*g*
dbca.rsp	Silent installation of Database Configuration Assistant
netca.rsp	Silent installation of Oracle Net Configuration Assistant

Table B–2   Response files for Oracle Grid Infrastructure

Response File	Description
crs_install.rsp	Silent installation of Oracle grid infrastructure installations

> **Caution:** When you modify a response file template and save a file for use, the response file may contain plain text passwords. Ownership of the response file should be given to the Oracle software installation owner only, and permissions on the response file should be changed to 600. Oracle strongly recommends that database administrators or other administrators delete or secure response files when they are not in use.

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 database 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. "How Response Files Work" on page B-1 explains this method.

   > **See Also:** *Oracle Universal Installer and OPatch User's Guide for Windows and UNIX* for detailed information on creating response files

3. Follow the instructions in the file to edit it.

   > **Note:** The installer or configuration assistant fails if you do not correctly configure the response file.

4. Change the permissions on the file to 600:

```
$ chmod 600 /local_dir/response_file.rsp
```

> **Note:** A fully specified response file for an Oracle Database 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.

Recording a Response File

You can use the installer in interactive mode to record 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.

Starting with Oracle Database 11*g* Release 2 (11.2), you can save all the installation steps into a response file during installation by clicking **Save Response File** on the Summary page. You can use the generated response file for a silent installation later.

When you record the response file, you can either complete the installation, or you can exit from the installer on the Summary page, before it starts to copy the software to the system.

If you use record mode during a response file mode installation, then the installer records the variable values that were specified in the original source response file into the new response file.

> **Note:** Oracle Universal Installer does not record passwords in the response file.

To record a response file:

1. Complete preinstallation tasks as for a normal installation.

2. If you have not installed Oracle software on this system previously, then create the `oraInst.loc` file as described in Creating the oraInst.loc File.

3. Ensure that the Oracle software owner user (typically `oracle`) has permissions to create or write to the Oracle home path that you will specify when you run the installer.

4. On each installation screen, specify the required information.

5. When the installer displays the Summary screen, perform the following steps:

   a. Click **Save Response File** and specify a file name and location to save the values for the response file, and click **Save**.

   b. Click **Finish** to create the response file and continue with the installation.

   Click **Save Response File** and click **Cancel** if you only want to create the response file but not continue with the installation. The installation will stop, but the settings you have entered will be recorded in the response file.

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.

Running the Installer Using a Response File

Run Oracle Universal Installer at the command line, specifying the response file you created. The Oracle Universal Installer executable, runInstaller, provides several options. For help information on 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 the installer using a response file:

1. Complete the preinstallation tasks as for a normal installation

2. Log in as the software installation owner user.

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 the 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 the installer fails.

In this example:

- *directory_path* is the path of the DVD or the path of the directory on the hard drive where you have copied the installation binaries.

- -silent runs the 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. For example

```
$ su root
password:
# /oracle_home_path/root.sh
```

Running Net Configuration Assistant Using a Response File

You can run Net Configuration Assistant in silent mode to configure and start an Oracle Net listener on the system, configure naming methods, and configure Oracle Net service names. To run Net Configuration Assistant in silent mode, you must copy and edit a response file template. Oracle provides a response file template named

netca.rsp in the response directory in the database/response directory on the DVD.

> **Note:** If you copied the software to a hard disk, then the response file template is located in the database/response directory.

To run Net Configuration Assistant using a response file:

1. Copy the netca.rsp response file template from the response file directory to a directory on your system:

    ```
    $ cp /directory_path/response/netca.rsp local_directory
    ```

    In this example, *directory_path* is the path of the database directory on the DVD. If you have copied the software to a hard drive, you can edit the file in the response directory if you prefer.

2. Open the response file in a text editor:

    ```
    $ vi /local_dir/netca.rsp
    ```

3. Follow the instructions in the file to edit it.

    > **Note:** Net Configuration Assistant fails if you do not correctly configure the response file.

4. Log in as the Oracle software owner user, and set the ORACLE_HOME environment variable to specify the correct Oracle home directory.

5. Enter a command similar to the following to run Net Configuration Assistant in silent mode:

    ```
    $ $ORACLE_HOME/bin/netca /silent /responsefile /local_dir/netca.rsp
    ```

    In this command:

    -   The /silent option indicates runs Net Configuration Assistant in silent mode.

    -   *local_dir* is the full path of the directory where you copied the netca.rsp response file template.

Running Database Configuration Assistants Using Response Files

You can run configuration assistants in response file or silent mode to configure and start Oracle software after it is installed on the system. To run configuration assistants in response file or silent mode, you must copy and edit a response file template.

> **Note:** If you copied the software to a hard disk, then the response file template is located in the /response directory.

This section contains the following topics:

-   About the Database Configuration Assistant in Response File Mode

-   Running Database Configuration Assistant in Response File or Silent Mode

About the Database Configuration Assistant in Response File Mode

In the response file mode, Database Configuration Assistant uses values that you specify, in the response file or as command line options, to create a database. As it configures and starts the database, it displays a window that contains status messages and a progress bar. The window that it displays is the same window that is displayed when you choose to create a preconfigured database during an Enterprise Edition or Standard Edition installation.

To run Database Configuration Assistant in response file mode, you must use a graphical display and set the DISPLAY environment variable. Use -progressOnly flag to set the run mode to response file.

Oracle provides a response file template named dbca.rsp in the /response directory on the installation media.

Running Database Configuration Assistant in Response File or Silent Mode

To run Database Configuration Assistant in response file or silent mode:

1. Copy the dbca.rsp response file template from the response file directory to a directory on your system:

    ```
    $ cp /directory_path/response/dbca.rsp local_directory
    ```

    In this example, *directory_path* is the path of the database directory on the DVD. If you have copied the software to a hard drive, you can edit the file in the response directory if you prefer.

    > **Note:** As an alternative to editing the response file template, you can also create a database by specifying all required information as command line options when you run Database Configuration Assistant. For information about the list of options supported, enter the following command:
    >
    > ```
    > $ $ORACLE_HOME/bin/dbca -help
    > ```

2. Open the response file in a text editor:

    ```
    $ vi /local_dir/dbca.rsp
    ```

3. Edit the file, following the instructions in the file.

    > **Note:** Database Configuration Assistant fails if you do not correctly configure the response file.

4. Log in as the Oracle software owner user, and set the ORACLE_HOME environment variable to specify the correct Oracle home directory.

5. If you intend running Database Configuration Assistant in response file mode, set the DISPLAY environment variable.

6. Use the following command syntax to run Database Configuration Assistant in silent or response file mode using a response file:

    ```
    $ORACLE_HOME/bin/dbca {-progressOnly | -silent} -responseFile \
    /local_dir/dbca.rsp
    ```

In this example:

- The -silent option runs Database Configuration Assistant in silent mode.

- The -progressOnly option runs Database Configuration Assistant in response file mode.

- *local_dir* is the full path of the directory where you copied the dbca.rsp response file template.

Postinstallation Configuration Using a Response File

Use the following sections to create and run a response file configuration after installing Oracle software.

About the Postinstallation Configuration File

When you run a silent or response file installation, you provide information about your servers in a response file that you otherwise provide manually during a graphical user interface installation. However, the response file does not contain passwords for user accounts that configuration assistants require after software installation is complete. The configuration assistants are started with a script called configToolAllCommands. You can run this script in response file mode by creating and using a password response file. The script uses the passwords to run the configuration tools in succession to complete configuration.

If you keep the password file to use for clone installations, then Oracle strongly recommends that you store it in a secure location. In addition, if you have to stop an installation to fix an error, you can run the configuration assistants using configToolAllCommands and a password response file.

The configToolAllCommands password response file consists of the following syntax options:

- *internal_component_name* is the name of the component that the configuration assistant configures

- *variable_name* is the name of the configuration file variable

- *value* is the desired value to use for configuration.

The command syntax is as follows:

internal_component_name|variable_name=value

For example:

oracle.assistants.asm|S_ASMPASSWORD=welcome

Oracle strongly recommends that you maintain security with a password response file:

- Permissions on the response file should be set to 600.

- The owner of the response file should be the installation owner user, with the group set to the central inventory (oraInventory) group.

Running Postinstallation Configuration Using a Response File

To run configuration assistants with the configToolAllCommands script:

1. Create a response file using the syntax *filename*.properties. For example:

   ```
   $ touch cfgrsp.properties
   ```

2. Open the file with a text editor, and cut and paste the password template, modifying as needed.

Example B–1   Password response file for Oracle grid infrastructure installation for a cluster

Oracle grid infrastructure requires passwords for Automatic Storage Management Configuration Assistant (ASMCA), and for Intelligent Platform Management Interface Configuration Assistant (IPMICA) if you have a BMC card and you want to enable this feature. Provide the following response file:

```
oracle.assistants.asm|S_ASMPASSWORD=password
oracle.assistants.asm|S_ASMMONITORPASSWORD=password
oracle.crs|S_BMCPASSWORD=password
```

If you do not have a BMC card, or you do not want to enable IPMI, then leave the S_BMCPASSWORD input field blank.

Example B–2   Password response file for Oracle Real Application Clusters

Oracle Database configuration requires configuring a password for the SYS, SYSTEM, SYSMAN, and DBSNMP passwords for use with Database Configuration Assistant (DBCA). In addition, if you use Oracle ASM storage, then configure the ASMSNMP password. Also, if you selected to configure Oracle Enterprise Manager, then you must provide the password for the Oracle software installation owner for the S_HOSTUSERPASSWORD response.

```
oracle.assistants.server|S_SYSPASSWORD=password
oracle.assistants.server|S_SYSTEMPASSWORD=password
oracle.assistants.server|S_SYSMANPASSWORD=password
oracle.assistants.server|S_DBSNMPPASSWORD=password
oracle.assistants.server|S_HOSTUSERPASSWORD=password
oracle.assistants.server|S_ASMSNMPPASSWORD=password
```

If you do not want to enable Oracle Enterprise Manager or Oracle ASM, then leave those password fields blank.

3. Change permissions to secure the file. For example:

```
$ ls -al cfgrsp.properties
-rw------- 1 oracle oinstall 0 Apr 30 17:30 cfgrsp
```

4. Change directory to `$ORACLE_HOME/cfgtoollogs`, and run the configuration script using the following syntax:

configToolAllCommands RESPONSE_FILE=/*path*/*name*.properties

for example:

```
$ ./configToolAllCommands RESPONSE_FILE=/home/oracle/cfgrsp.properties
```

C

Oracle Grid Infrastructure for a Cluster Installation Concepts

This appendix explains the reasons for preinstallation tasks that you are asked to perform, and other installation concepts.

This appendix contains the following sections:

- Understanding Preinstallation Configuration
- Understanding Storage Configuration
- Understanding Out-of-Place Upgrade

C.1 Understanding Preinstallation Configuration

This section reviews concepts about grid infrastructure for a cluster preinstallation tasks. It contains the following sections:

- Understanding Oracle Groups and Users
- Understanding the Oracle Base Directory Path
- Understanding Network Addresses
- Understanding Network Time Requirements

C.1.1 Understanding Oracle Groups and Users

This section contains the following topics:

- Understanding the Oracle Inventory Group
- Understanding the Oracle Inventory Directory

C.1.1.1 Understanding the Oracle Inventory Group

You must have a group whose members are given access to write to the Oracle Inventory (`oraInventory`) directory, which is the central inventory record of all Oracle software installations on a server. Members of this group have write privileges to the Oracle central inventory (`oraInventory`) directory, and are also granted permissions for various Oracle Clusterware resources, OCR keys, directories in the Oracle Clusterware home to which DBAs need write access, and other necessary privileges. By default, this group is called `oinstall`. The Oracle Inventory group must be the primary group for Oracle software installation owners.

The `oraInventory` directory contains the following:

- A registry of the Oracle home directories (Oracle grid infrastructure and Oracle Database) on the system

- Installation logs and trace files from installations of Oracle software. These files are also copied to the respective Oracle homes for future reference.

- Other metadata inventory information regarding Oracle installations are stored in the individual Oracle home inventory directories, and are separate from the central inventory.

You can configure one group to be the access control group for the 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.

> **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 (`oracle` or `grid`) that you use to install Oracle grid infrastructure. Refer to "Determining If the Oracle Inventory and Oracle Inventory Group Exists" to identify an existing Oracle Inventory group.

C.1.1.2 Understanding the Oracle Inventory Directory

The Oracle Inventory directory (`oraInventory`) is the central inventory location for all Oracle software installed on a server.

The first time you install Oracle software on a system, the installer checks to see if you have created an Optimal Flexible Architecture (OFA) compliant path in the format u[01-09]/app, such as `/u01/app`, and that the user running the installation has permissions to write to that path. If this is true, then the installer creates the Oracle Inventory directory in the path /u[01-09]/app/oraInventory. For example:

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

When you provide an Oracle base path when prompted during installation, or you have set the environment variable `$ORACLE_BASE` for the user performing the Oracle grid infrastructure installation, then OUI creates the Oracle Inventory directory in the path `$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`, one directory level above Oracle base.

If you have created neither 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
```

As this placement can cause permission errors during subsequent installations with multiple Oracle software owners, Oracle recommends that you either create an OFA-compliant installation path, or set an `$ORACLE_BASE` environment path.

For new installations, Oracle recommends that you allow OUI to create the Oracle Inventory directory (`oraInventory`). By default, if you create an Oracle path in compliance with OFA structure, such as `/u01/app`, that is owned by an Oracle software owner, then the Oracle Inventory is created in the path `u01/app/oraInventory` using correct permissions to allow all Oracle installation owners to write to this central inventory directory.

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.

C.1.2 Understanding the Oracle Base Directory Path

This section contains information about preparing an Oracle base directory.

C.1.2.1 Overview of the Oracle Base directory

During installation, you are prompted to specify an Oracle base location, which is owned by the user performing the installation. You can choose a location with an existing Oracle home, or choose another directory location that does not have the structure for an Oracle base directory.

Using the Oracle base directory path helps to facilitate the organization of Oracle installations, and helps to ensure that installations of multiple databases maintain an Optimal Flexible Architecture (OFA) configuration.

C.1.2.2 Understanding Oracle Base and Grid Infrastructure Directories

Even if you do not use the same software owner to install Grid Infrastructure (Oracle Clusterware and Oracle ASM) and Oracle Database, be aware that running the `root.sh` script during the Oracle grid infrastructure installation changes ownership of the home directory where clusterware binaries are placed to `root`, and all ancestor directories to the root level (`/`) are also changed to `root`. For this reason, the Oracle grid infrastructure for a cluster home cannot be in the same location as other Oracle software.

However, Oracle grid infrastructure for a standalone database--Oracle Restart--can be in the same location as other Oracle software.

> **See Also:** *Oracle Database Installation Guide* for your platform for more information about Oracle Restart

C.1.3 Understanding Network Addresses

During installation, you are asked to identify the planned use for each network interface that OUI detects on your cluster node. Identify each interface as a public or private interface, or as an interface that you do not want Oracle Clusterware to use. Public and virtual IP addresses are configured on public interfaces. Private addresses are configured on private interfaces.

Refer to the following sections for detailed information about each address type:

- About the Public IP Address
- About the Private IP Address
- About the Virtual IP Address
- About the Grid Naming Service (GNS) Virtual IP Address
- About the SCAN

C.1.3.1 About the Public IP Address

The public IP address is assigned dynamically using DHCP, or defined statically in a DNS or in a hosts file. It uses the public interface (the interface with access available to clients).

C.1.3.2 About the Private IP Address

Oracle Clusterware uses interfaces marked as private for internode communication. Each cluster node needs to have an interface that you identify during installation as a private interface. Private interfaces need to have addresses configured for the interface itself, but no additional configuration is required. Oracle Clusterware uses interfaces marked as private as the cluster interconnects. Any interface that you identify as private must be on a subnet that connects to every node of the cluster. Oracle Clusterware uses all the interfaces you identify for use as private interfaces.

For the private interconnects, because of Cache Fusion and other traffic between nodes, Oracle strongly recommends using a physically separate, private network. If you configure addresses using a DNS, then you should ensure that the private IP addresses are reachable only by the cluster nodes.

After installation, if you modify interconnects on Oracle RAC with the `CLUSTER_INTERCONNECTS` initialization parameter, then you must change it to a private IP address, on a subnet that is not used with a public IP address, nor marked as a public subnet by `oifcfg`. Oracle does not support changing the interconnect to an interface using a subnet that you have designated as a public subnet.

> **See Also:** *Oracle Clusterware Administration and Deployment Guide* for further information about setting up and using bonded multiple interfaces

You should not use a firewall on the network with the private network IP addresses, as this can block interconnect traffic.

C.1.3.3 About the Virtual IP Address

The virtual IP (VIP) address is registered in the GNS, or the DNS. Select an address for your VIP that meets the following requirements:

- The IP address and host name are currently unused (it can be registered in a DNS, but should not be accessible by a `ping` command)

- The VIP is on the same subnet as your public interface

C.1.3.4 About the Grid Naming Service (GNS) Virtual IP Address

The GNS virtual IP address is a static IP address configured in the DNS. The DNS delegates queries to the GNS virtual IP address, and the GNS daemon responds to incoming name resolution requests at that address.

Within the subdomain, the GNS uses multicast Domain Name Service (mDNS), included with Oracle Clusterware, to enable the cluster to map hostnames and IP addresses dynamically as nodes are added and removed from the cluster, without requiring additional host configuration in the DNS.

To enable GNS, you must have your network administrator provide a set of IP addresses for a subdomain assigned to the cluster (for example, `grid.example.com`), and delegate DNS requests for that subdomain to the GNS virtual IP address for the cluster, which GNS will serve. The set of IP addresses is provided to the cluster through DHCP, which must be available on the public network for the cluster.

> **See Also:** *Oracle Clusterware Administration and Deployment Guide* for more information about Grid Naming Service

C.1.3.5 About the SCAN

Oracle Database 11*g* release 2 clients connect to the database using SCANs. The SCAN and its associated IP addresses provide a stable name for clients to use for connections, independent of the nodes that make up the cluster. SCAN addresses, virtual IP addresses, and public IP addresses must all be on the same subnet.

> **Note:**   You can only create the SCAN on the default public network (Net1). If you install with multiple public networks, you cannot create a SCAN for each network, but rather only Net1.

The SCAN resolves to multiple IP addresses in the cluster handling public client connections. When a client submits a request, the SCAN listener listening on a SCAN IP address and the SCAN port is made available to a client. Because all services on the cluster are registered with the SCAN listener, the SCAN listener replies with the address of the local listener on the least-loaded node where the service is currently being offered. Finally, the client establishes connection to the service through the listener on the node where service is offered. All of these actions take place transparently to the client without any explicit configuration required in the client.

During installation listeners are created. They listen on the SCAN IP addresses provided on nodes for the SCAN IP addresses. Oracle Net Services routes application requests to the least loaded instance providing the service. Because the SCAN addresses resolve to the cluster, rather than to a node address in the cluster, nodes can be added to or removed from the cluster without affecting the SCAN address configuration.

The SCAN should be configured so that it is resolvable either by using Grid Naming Service (GNS) within the cluster, or by using Domain Name Service (DNS) resolution. For high availability and scalability, Oracle recommends that you configure the SCAN name so that it resolves to three IP addresses. At a minimum, the SCAN must resolve to at least one address.

If you specify a GNS domain, then the SCAN name defaults to *clustername*-scan.*GNS_domain*. Otherwise, it defaults to *clustername*-scan.*current_domain*. For example, if you start Oracle grid infrastructure installation from the server `node1`, the cluster name is `mycluster`, and the GNS domain is `grid.example.com`, then the SCAN Name is `mycluster-scan.grid.example.com`.

Clients configured to use IP addresses for Oracle Database releases prior to Oracle Database 11*g* release 2 can continue to use their existing connection addresses; using SCANs is not required. When you upgrade to Oracle Clusterware 11*g* release 2 (11.2), the SCAN becomes available, and you should use the SCAN for connections to Oracle Database 11*g* release 2 or later databases. When an earlier version of Oracle Database is upgraded, it registers with the SCAN listeners, and clients can start using the SCAN to connect to that database. The database registers with the SCAN listener through the remote listener parameter in the init.ora file. The REMOTE_LISTENER parameter must be set to SCAN:PORT. Do not set it to a TNSNAMES alias with a single address with the SCAN as HOST=SCAN.

The SCAN is optional for most deployments. However, clients using Oracle Database release 11*g* release 2 and later policy-managed databases using server pools should access the database using the SCAN. This is because policy-managed databases can run on different servers at different times, so connecting to a particular node virtual IP address for a policy-managed database is not possible.

C.1.4 Understanding Network Time Requirements

Oracle Clusterware 11*g* release 2 (11.2) is automatically configured with Cluster Time Synchronization Service (CTSS). This service provides automatic synchronization of all cluster nodes using the optimal synchronization strategy for the type of cluster you deploy. If you have an existing cluster synchronization service, such as NTP, then it will start in an observer mode. Otherwise, it will start in an active mode to ensure that time is synchronized between cluster nodes. CTSS will not cause compatibility issues.

The CTSS module is installed as a part of Oracle grid infrastructure installation. CTSS daemons are started up by the OHAS daemon (`ohasd`), and do not require a command-line interface.

C.2 Understanding Storage Configuration

This section contains the following information:

- About Migrating Existing Oracle ASM Instances
- About Converting Standalone Oracle ASM Installations to Clustered Installations

C.2.1 About Migrating Existing Oracle ASM Instances

If you have an Oracle ASM installation from a prior release installed on your server, or in an existing Oracle Clusterware installation, then you can use Automatic Storage Management Configuration Assistant (ASMCA, located in the path *Grid_home*/bin) to upgrade the existing Oracle ASM instance to Oracle ASM 11*g* release 2 (11.2), and subsequently configure failure groups, and ASM volumes.

> **Note:** You must first shut down all database instances and applications on the node with the existing Oracle ASM instance before upgrading it.

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

On an existing Oracle Clusterware or Oracle RAC installation, if the prior version of Oracle ASM instances on all nodes is Oracle ASM 11*g* release 1, then you are provided with the option to perform a rolling upgrade of Oracle ASM instances. If the prior version of Oracle ASM instances on an Oracle RAC installation are from an Oracle ASM release prior to Oracle ASM 11*g* release 1, then rolling upgrades cannot be performed. Oracle ASM is then upgraded on all nodes to 11*g* release 2 (11.2).

C.2.2 About Converting Standalone Oracle ASM Installations to Clustered Installations

If you have an existing standalone Oracle ASM installations on one or more nodes that are member nodes of the cluster, then OUI proceeds to install Oracle grid infrastructure for a cluster.

If you place Oracle Clusterware files (OCR and voting disks) on Oracle ASM, then ASMCA is started at the end of the clusterware installation, and provides prompts for you to migrate and upgrade the Oracle ASM instance on the local node, so that you have an Oracle ASM 11*g* release 2 (11.2) installation.

On remote nodes, ASMCA identifies any standalone Oracle ASM instances that are running, and prompts you to shut down those Oracle ASM instances, and any database instances that use them. ASMCA then extends clustered Oracle ASM

instances to all nodes in the cluster. However, diskgroup names on the cluster-enabled Oracle ASM instances must be different from existing standalone diskgroup names.

> **See Also:** *Oracle Database Storage Administrator's Guide*

C.3 Understanding Out-of-Place Upgrade

With an out-of-place upgrade, the installer installs the newer version in a separate Oracle Clusterware home. Both versions of Oracle Clusterware are on each cluster member node, but only one version is active.

Rolling upgrade avoids downtime and ensure continuous availability while the software is upgraded to a new version.

If you have separate Oracle Clusterware homes on each node, then you can perform an out-of-place upgrade on all nodes, or perform an out-of-place rolling upgrade, so that some nodes are running Oracle Clusterware from the earlier version Oracle Clusterware home, and other nodes are running Oracle Clusterware from the new Oracle Clusterware home.

An in-place upgrade of Oracle Clusterware 11*g* release 2 is not supported.

> **See Also:** Appendix E, "How to Upgrade to Oracle Grid Infrastructure 11g Release 2" for instructions on completing rolling upgrades

D

How to Complete Installation Prerequisite Tasks Manually

This appendix provides instructions for how to complete configuration tasks manually that Cluster Verification Utility (CVU) and the installer (OUI) normally complete during installation. Use this appendix as a guide if you cannot use the fixup script.

This appendix contains the following information:

- Configuring SSH Manually on All Cluster Nodes
- Configuring Kernel Parameters Manually

D.1 Configuring SSH Manually on All Cluster Nodes

Passwordless SSH configuration is a mandatory installation requirement. SSH is used during installation to configure cluster member nodes, and SSH is used after installation by configuration assistants, Oracle Enterprise Manager, Opatch, and other features.

Automatic Passwordless SSH configuration using OUI creates RSA encryption keys on all nodes of the cluster. If you have system restrictions that require you to set up SSH manually, such as using DSA keys, then use this procedure as a guide to set up passwordless SSH.

In the examples that follow, the Oracle software owner listed is the `grid` user.

If SSH is not available, then OUI attempts to use `rsh` and `rcp` instead. However, these services often are disabled for security.

This section contains the following:

- Checking Existing SSH Configuration on the System
- Configuring SSH on Cluster Nodes
- Enabling SSH User Equivalency on Cluster Nodes

D.1.1 Checking Existing SSH Configuration on the System

To determine if SSH is running, enter the following command:

```
$ pgrep sshd
```

If SSH is running, then the response to this command is one or more process ID numbers. In the home directory of the installation software owner (`grid`, `oracle`), use the command `ls -al` to ensure that the `.ssh` directory is owned and writable only by the user.

You need either an RSA or a DSA key for the SSH protocol. RSA is used with the SSH 1.5 protocol, while DSA is the default for the SSH 2.0 protocol. With OpenSSH, you can use either RSA or DSA. The instructions that follow are for SSH1. If you have an SSH2 installation, and you cannot use SSH1, then refer to your SSH distribution documentation to configure SSH1 compatibility or to configure SSH2 with DSA.

D.1.2 Configuring SSH on Cluster Nodes

To configure SSH, you must first create RSA or DSA keys on each cluster node, and then copy all the keys generated on all cluster node members into an authorized keys file that is identical on each node. Note that the SSH files must be readable only by root and by the software installation user (oracle, grid), as SSH ignores a private key file if it is accessible by others. In the examples that follow, the DSA key is used.

You must configure SSH separately for each Oracle software installation owner that you intend to use for installation.

To configure SSH, complete the following:

D.1.2.1 Create SSH Directory, and Create SSH Keys On Each Node

Complete the following steps on each node:

1. Log in as the software owner (in this example, the grid user).

2. To ensure that you are logged in as grid, and to verify that the user ID matches the expected user ID you have assigned to the grid user, enter the commands id and id grid. Ensure that Oracle user group and user and the user terminal window process you are using have group and user IDs are identical. For example:

```
$ id
uid=502(grid) gid=501(oinstall) groups=501(oinstall),502(grid,asmadmin,asmdba)
$ id grid
uid=502(grid) gid=501(oinstall) groups=501(oinstall),502(grid,asmadmin,asmdba)
```

3. If necessary, create the .ssh directory in the grid user's home directory, and set permissions on it to ensure that only the oracle user has read and write permissions:

```
$ mkdir ~/.ssh
$ chmod 700 ~/.ssh
```

> **Note:** SSH configuration will fail if the permissions are not set to 700.

4. Enter the following command:

```
$ /usr/bin/ssh-keygen -t dsa
```

At the prompts, accept the default location for the key file (press **Enter**).

> **Note:** SSH with passphrase is not supported for Oracle Clusterware 11*g* release 2 and later releases.

This command writes the DSA public key to the ~/.ssh/id_dsa.pub file and the private key to the ~/.ssh/id_dsa file.

Never distribute the private key to anyone not authorized to perform Oracle software installations.

5. Repeat steps 1 through 4 on each node that you intend to make a member of the cluster, using the DSA key.

D.1.2.2 Add All Keys to a Common authorized_keys File

Complete the following steps:

1. On the local node, change directories to the `.ssh` directory in the Oracle grid infrastructure owner's home directory (typically, either `grid` or `oracle`).

Then, add the DSA key to the `authorized_keys` file using the following commands:

```
$ cat id_dsa.pub >> authorized_keys
$ ls
```

In the .ssh directory, you should see the `id_rsa.pub` keys that you have created, and the file `authorized_keys`.

2. On the local node, use SCP (Secure Copy) or SFTP (Secure FTP) to copy the `authorized_keys` file to the `oracle` user `.ssh` directory on a remote node. The following example is with SCP, on a node called node2, with the Oracle grid infrastructure owner `grid`, where the `grid` user path is `/home/grid`:

```
[grid@node1 .ssh]$ scp authorized_keys node2:/home/grid/.ssh/
```

You are prompted to accept a DSA key. Enter Yes, and you see that the node you are copying to is added to the `known_hosts` file.

When prompted, provide the password for the grid user, which should be the same on all nodes in the cluster. The `authorized_keys` file is copied to the remote node.

Your output should be similar to the following, where xxx represents parts of a valid IP address:

```
[grid@node1 .ssh]$ scp authorized_keys node2:/home/grid/.ssh/
The authenticity of host 'node2 (xxx.xxx.173.152) can't be established.
DSA key fingerprint is 7e:60:60:ae:40:40:d1:a6:f7:4e:zz:me:a7:48:ae:f6:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'node1,xxx.xxx.173.152' (dsa) to the list
of known hosts
grid@node2's password:
authorized_keys     100%     828     7.5MB/s     00:00
```

3. Using SSH, log in to the node where you copied the `authorized_keys` file. Then change to the `.ssh` directory, and using the `cat` command, add the DSA keys for the second node to the `authorized_keys` file, clicking **Enter** when you are prompted for a password, so that passwordless SSH is set up:

```
[grid@node1 .ssh]$ ssh node2
[grid@node2 grid]$ cd .ssh
[grid@node2 ssh]$ cat id_dsa.pub  >> authorized_keys
```

Repeat steps 2 and 3 from each node to each other member node in the cluster.

When you have added keys from each cluster node member to the `authorized_keys` file on the last node you want to have as a cluster node member, then use `scp` to copy the `authorized_keys` file with the keys from all nodes back to each cluster node member, overwriting the existing version on the other nodes.

To confirm that you have all nodes in the `authorized_keys` file, enter the command `more authorized_keys`, and determine if there is a DSA key for each member node. The file lists the type of key (`ssh-dsa`), followed by the key, and then followed by the user and server. For example:

```
ssh-dsa AAAABBBB . . . = grid@node1
```

Note: The `grid` user's `/.ssh/authorized_keys` file on every node must contain the contents from all of the `/.ssh/id_dsa.pub` files that you generated on all cluster nodes.

D.1.3 Enabling SSH User Equivalency on Cluster Nodes

After you have copied the `authorized_keys` file that contains all keys to each node in the cluster, complete the following procedure, in the order listed. In this example, the Oracle grid infrastructure software owner is named `grid`:

1. On the system where you want to run OUI, log in as the `grid` user.

2. Use the following command syntax, where *hostname1*, *hostname2*, and so on, are the public hostnames (alias and fully qualified domain name) of nodes in the cluster to run SSH from the local node to each node, including from the local node to itself, and from each node to each other node:

```
[grid@nodename]$ ssh hostname1 date
[grid@nodename]$ ssh hostname2 date
   .
   .
   .
```

For example:

```
[grid@node1 grid]$ ssh node1 date
The authenticity of host 'node1 (xxx.xxx.100.101)' can't be established.
DSA key fingerprint is 7z:60:60:zz:48:48:z1:a0:f7:4e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'node1,xxx.xxx.100.101' (DSA) to the list of
known hosts.
Mon Dec 4 11:08:13 PST 2006
[grid@node1 grid]$ ssh node1.example.com date
The authenticity of host 'node1.example.com (xxx.xxx.100.101)' can't be
established.
DSA key fingerprint is 7z:60:60:zz:48:48:z1:a0:f7:4e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'node1.example.com,xxx.xxx.100.101' (DSA) to the
list of known hosts.
Mon Dec 4 11:08:13 PST 2006
[grid@node1 grid]$ ssh node2 date
Mon Dec 4 11:08:35 PST 2006
.
.
.
```

At the end of this process, the public hostname for each member node should be registered in the `known_hosts` file for all other cluster nodes.

If you are using a remote client to connect to the local node, and you see a message similar to "Warning: No xauth data; using fake authentication data for X11 forwarding," then this means that your authorized keys file is configured correctly,

but your SSH configuration has X11 forwarding enabled. To correct this issue, proceed to Section 2.11.4, "Setting Display and X11 Forwarding Configuration."

3. Repeat step 2 on each cluster node member.

If you have configured SSH correctly, then you can now use the `ssh` or `scp` commands without being prompted for a password. For example:

```
[grid@node1 ~]$ ssh node2 date
Mon Feb 26 23:34:42 UTC 2009
[grid@node1 ~]$ ssh node1 date
Mon Feb 26 23:34:48 UTC 2009
```

If any node prompts for a password, then verify that the `~/.ssh/authorized_keys` file on that node contains the correct public keys, and that you have created an Oracle software owner with identical group membership and IDs.

D.2 Configuring Kernel Parameters Manually

> **Note:** The kernel parameter values shown in this section are recommended values only. For production database systems, Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.
>
> On HP-UX 11.31 (version 3), the following parameters are not valid:
>
> - msgmap
> - msgseg
> - ncallout

D.2.1 Minimal Kernel Parameter Values

On all cluster nodes, verify that the kernel parameters shown in Table D–1 are set either to the formula shown, or to values greater than or equal to the recommended value shown. The procedure following the table describes how to verify and set the values.

Table D–1   Minimal HP-UX Kernel Parameter Values

Parameter	Minimum Required Value
ksi_alloc_max	32768
executable_stack	0
maxfiles	1024
maxfiles_lim	63488
max_thread_proc	1024
maxdsiz	1073741824 (1 GB)
maxdsiz_64bit	2147483648 (2 GB)
maxssiz	134217728 (128 MB)
maxssiz_64bit	1073741824 (1 GB)
maxuprc	3686

Table D–1   (Cont.) Minimal HP-UX Kernel Parameter Values

Parameter	Minimum Required Value
msgmap	4096
msgmni	4096
msgtql	4096
ncsize	35840
nflocks	4096
ninode	34816
nkthread	7184
nproc	4096
semmni	4096
semmns	8192
semmnu	4096
semvmx	32767
shmmax	1073741824
shmmni	4092
shmseg	512

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

D.2.2 Checking Kernel Parameters Manually

To view the current value or formula specified for these kernel parameters, and to change them if necessary, use `kctune`, HP System Management Homepage (HP SMH), or HP-UX Kernel Configuration (`kcweb`).

- Modifying Kernel Settings Using KCTUNE
- Modifying Kernel Settings Using SMH
- Modifying Kernel Settings Using KCWEB

D.2.2.1 Modifying Kernel Settings Using KCTUNE

Use `/usr/sbin/kctune` to view or change kernel parameters. For example, to view kernel parameters, enter kctune with the `-d` flag. For example:

```
# /usr/sbin/kctune -d
```

To modify a kernel parameter, enter kctune *variable=value*. For example:

```
# /usr/sbin/kctune aio_listio_max=512
```

Complete this procedure on all other cluster nodes.

D.2.2.2 Modifying Kernel Settings Using SMH

The following procedure describes how to modify kernel settings using HP System Management Homepage (SMH):

1. Optionally, set the DISPLAY environment variable to specify the display of the local system:

   – Bourne, Bash, or Korn shell:

   ```
   # DISPLAY=local_host:0.0 ; export DISPLAY
   ```

   – C shell:

   ```
   # setenv DISPLAY local_host:0.0
   ```

2. Start SMH:

   ```
   # /usr/sbin/smh
   ```

3. Choose the **Kernel Configuration** area, then choose the **Configurable Parameters** area.

4. Check the value or formula specified for each of these parameters and, if necessary, modify that value or formula.

   If necessary, refer to the SMH online Help for more information about completing this step.

   > **Note:** If you modify the value of a parameter that is not dynamic, then you must restart the system.

5. If necessary, when the system restarts, log in and switch user to `root`.

6. Complete this procedure on all other cluster nodes.

D.2.2.3 Modifying Kernel Settings Using KCWEB

The following procedure shows how to

1. Enter the following command to start the `kcweb` application:

   ```
   # /usr/sbin/kcweb -F
   ```

2. Check the value or formula specified for each of these parameters and, if necessary, modify that value or formula.

   If necessary, refer to the `kcweb` online Help for more information about completing this step.

   > **Note:** If you modify the value of a parameter that is not dynamic, then you must restart the system.

3. If necessary, when the system restarts, log in and switch user to `root`.

4. Complete this procedure on all other cluster nodes.

E

How to Upgrade to Oracle Grid Infrastructure 11*g* Release 2

This appendix describes how to perform Oracle Clusterware and Oracle Automatic Storage Management upgrades.

Oracle Clusterware upgrades can be rolling upgrades, in which a subset of nodes are brought down and upgraded while other nodes remain active. Oracle Automatic Storage Management 11*g* release 2 (11.2) upgrades can be rolling upgrades. If you upgrade a subset of nodes, then a software-only installation is performed on the existing cluster nodes that you do not select for upgrade.

This appendix contains the following topics:

- Back Up the Oracle Software Before Upgrades
- Unset Oracle Environment Variables
- Restrictions for Clusterware and ASM Upgrades to Grid Infrastructure
- Verify System Readiness for Upgrades
- Upgrading an Existing Oracle Clusterware Installation
- Performing Rolling Upgrades From an Earlier Release
- Updating DB Control and Grid Control Target Parameters
- Downgrading Oracle Clusterware After an Upgrade

E.1 Back Up the Oracle Software Before Upgrades

Before you make any changes to the Oracle software, Oracle recommends that you create a backup of the Oracle software and databases.

E.2 Unset Oracle Environment Variables

Unset Oracle environment variables.

If you have set ORA_CRS_HOME as an environment variable, following instructions from Oracle Support, then unset it before starting an installation or upgrade. You should never use ORA_CRS_HOME as an environment variable except under explicit direction from Oracle Support.

If you have had an existing installation on your system, and you are using the same user account to install this installation, then unset the following environment variables: ORA_CRS_HOME; ORACLE_HOME; ORA_NLS10; TNS_ADMIN; and any

other environment variable set for the Oracle installation user that is connected with Oracle software homes.

E.3 Restrictions for Clusterware and ASM Upgrades to Grid Infrastructure

Be aware of the following restrictions and changes for upgrades to Oracle grid infrastructure installations, which consists of Oracle Clusterware and Automatic Storage Management (Oracle ASM):

- To upgrade existing Oracle Clusterware installations to Oracle grid infrastructure 11*g*, your release must be greater than or equal to 10.1.0.3, 10.2.0.3, or 11.1.0.6.

- To upgrade existing Oracle ASM installations to Oracle grid infrastructure 11*g* release 2 (11.2) in a rolling fashion, your release must be at least 11.1.0.6.

  > **See Also:** Oracle Upgrade Companion" Note 785351.1 on My Oracle Support:
  >
  > https://metalink.oracle.com

- Oracle Clusterware and Oracle ASM upgrades are always out-of-place upgrades. With 11*g* release 2 (11.2), you cannot perform an in-place upgrade of Oracle Clusterware and Oracle ASM to existing homes.

- If the existing Oracle Clusterware home is a shared home, note that you can use a non-shared home for the grid infrastructure for a cluster home for Oracle Clusterware and Oracle ASM 11*g* release 2 (11.2).

- With Oracle Clusterware 11*g* release 1 and later releases, the same user that owned the Oracle Clusterware 10*g* software must perform the Oracle Clusterware 11*g* upgrade. Before Oracle Database 11*g*, either all Oracle software installations were owned by the Oracle user, typically `oracle`, or Oracle Database software was owned by `oracle`, and Oracle Clusterware software was owned by a separate user, typically `crs`.

- Oracle ASM and Oracle Clusterware both run in the Oracle grid infrastructure home.

- During a major version upgrade to 11*g* release 2 (11.2), the software in the 11*g* release 2 (11.2) grid infrastructure home is not fully functional until the upgrade is completed. Running `srvctl`, `crsctl`, and other commands from the 11*g* release 2 (11.2) home is not supported until the final `rootupgrade.sh` script is run and the upgrade is complete across all nodes.

  To manage databases in the existing earlier version (release 10.x or 11.1) database homes during the grid infrastructure upgrade, use the `srvctl` from the existing database homes.

- During Oracle Clusterware installation, if there is a standalone Oracle ASM version on the local node, then it is converted to a clustered Oracle ASM 11*g* release 2 (11.2) installation, and Oracle ASM runs in the Oracle grid infrastructure home on all nodes.

- If a standalone (non-clustered) Oracle ASM installation is on a remote node, which is a node other than the local node (the node on which the Oracle grid infrastructure installation is being performed), then it will remain a standalone Oracle ASM installation. However, during installation, if you select to place the Oracle Cluster Registry (OCR) and voting disk files on Oracle ASM, then a

clustered Oracle ASM installation is created on all nodes in the cluster, and the standalone Oracle ASM installation on the remote node will become nonfunctional.

> **See Also:** *Oracle Database Upgrade Guide*

E.4 Verify System Readiness for Upgrades

Use the Cluster Verification Utility to assist you with system checks in preparation for starting a database upgrade.

> **See Also:** *Oracle Database Upgrade Guide*

E.5 Upgrading an Existing Oracle Clusterware Installation

If you have an existing Oracle Clusterware installation, then you upgrade your existing cluster by performing an out-of-place upgrade. You cannot perform an in-place upgrade.

E.5.1 Preparing to Upgrade an Existing Oracle Clusterware Installation

Complete the following tasks before starting an upgrade:

1. For each node, use Cluster Verification Utility to ensure that you have completed preinstallation steps. It can generate Fixup scripts to help you to prepare servers. In addition, the installer will help you to ensure all required prerequisites are met.

   Ensure that you have information you will need during installation, including the following:

   - An Oracle base location for Oracle Clusterware.

   - An Oracle grid infrastructure home location that is different from your existing Oracle Clusterware location

   - A SCAN address

   - Privileged user operating system groups to grant access to Oracle ASM data files (the OSDBA for ASM group), to grant administrative privileges to the Oracle ASM instance (OSASM group), and to grant a subset of administrative privileges to the Oracle ASM instance (OSOPER for ASM group)

   - `root` user access, to run scripts as `root` during installation

2. For the installation owner running the installation, if you have environment variables set for the existing installation, then unset the environment variables $ORACLE_HOME and $ORACLE_SID, as these environment variables are used during upgrade. For example:

   ```
   $ unset ORACLE_BASE
   $ unset ORACLE_HOME
   $ unset ORACLE_SID
   ```

   > **See Also:** Section E.2, "Unset Oracle Environment Variables"

E.6 Performing Rolling Upgrades From an Earlier Release

Use the following procedures to upgrade Oracle Clusterware or Automatic Storage Management:

- Verify System Readiness for Upgrades

- Performing a Rolling Upgrade of Oracle Clusterware

- Performing a Rolling Upgrade of Automatic Storage Management

> **Note:** When you upgrade to Oracle Clusterware 11*g* release 2 (11.2), Automatic Storage Management (Oracle ASM) is installed in the same home as Oracle Clusterware. In Oracle documentation, this home is called the "grid infrastructure home," or Grid home. Also note that Oracle does not support attempting to add additional nodes to a cluster during a rolling upgrade.

E.6.1 Verify System Readiness for Upgrades

Use Cluster Verification Utility to assist you with system checks in preparation for starting a database upgrade. The installer runs the appropriate CVU checks automatically, and either prompts you to fix problems, or provides a fixup script to be run on all nodes in the cluster before proceeding with the upgrade.

With Oracle Clusterware 11*g* release 2 (11.2), you can perform upgrades on a shared Oracle Clusterware home.

E.6.2 Performing a Rolling Upgrade of Oracle Clusterware

Use the following procedure to upgrade Oracle Clusterware from an earlier release to a later release:

> **Note:** Oracle recommends that you leave Oracle RAC instances running. When you start the root script on each node, that node's instances are shut down and then started up again by the `rootupgrade.sh` script.
>
> For standalone Oracle Databases on the cluster, only those that use Oracle ASM need to be shut down. Listeners do not need to be shut down.

1. Start the installer, and select the option to upgrade an existing Oracle Clusterware and Oracle ASM installation.

2. On the node selection page, select all nodes.

> **Note:** In contrast with releases prior to Oracle Clusterware 11*g* release 2, all upgrades are rolling upgrades, even if you select all nodes for the upgrade.
>
> Oracle recommends that you select all cluster member nodes for the upgrade, and then shut down database instances on each node before you run the upgrade `root` script, starting the database instance up again on each node after the upgrade is complete. You can also use this procedure to upgrade a subset of nodes in the cluster.

3. Select installation options as prompted.

   When prompted, run the `rootupgrade.sh` script on each node in the cluster that you want to upgrade. The script shuts down the earlier release installation,

replaces it with the new Oracle Clusterware release, and starts the new Oracle Clusterware installation.

After the `rootupgrade.sh` script is run on a node, the upgraded Oracle Clusterware stack and AUTOSTART resources are started on the node.

4. Run the `rootupgrade.sh` script on each node on which you are performing the rolling upgrade. Run the script on the local node first. After the script completes successfully, you can run the script in parallel on all nodes except for one, which you select as the last node. When the script is run successfully on all the nodes except the last node, run the script on the last node.

5. After running the `rootupgrade.sh` script on the last node in the cluster, if you left the check box with ASMCA marked, as is the default, then ASM Configuration Assistant runs automatically, and the Oracle Clusterware upgrade is complete. If you unclicked the box on the interview stage of the upgrade, then ASMCA is not run automatically.

If an earlier version of Automatic Storage Management is installed, then the installer starts ASM Configuration Assistant to upgrade Oracle ASM to 11*g* release 2 (11.2). You can choose to upgrade Oracle ASM at this time, or upgrade it later.

Oracle recommends that you upgrade Oracle ASM at the same time that you upgrade the Oracle Clusterware binaries. Until ASM is upgraded, Oracle databases that use ASM can't be created. Until ASM is upgraded, the 11*g* release 2 (11.2) ASM management tools in the Grid home (for example, `srvctl`) will not work.

> **Note:** At the end of the upgrade, if you set the OCR backup location manually to the older release Oracle Clusterware home (CRS home), then you must change the OCR backup location to the Oracle grid infrastructure home (Grid home). If you did not set the OCR backup location manually, then this issue does not concern you.
>
> Because upgrades of Oracle Clusterware are out-of-place upgrades, the previous release Oracle Clusterware home cannot be the location of the OCR backups. Backups in the old Oracle Clusterware home could be deleted.

E.6.3 Performing a Rolling Upgrade of Automatic Storage Management

After you have completed the Oracle Clusterware 11*g* release 2 (11.2) upgrade, if you did not choose to upgrade Oracle ASM when you upgraded Oracle Clusterware, then you can do it separately using the Automatic Storage Management Configuration Assistant (`asmca`) to perform rolling upgrades.

You can use asmca to complete the upgrade separately, but you should do it soon after you upgrade Oracle Clusterware, as Oracle ASM management tools such as `srvctl` will not work until Oracle ASM is upgraded.

> **Note:** ASMCA performs a rolling upgrade only if the earlier version of Oracle ASM is either 11.1.0.6 or 11.1.0.7. Otherwise, ASMCA performs a normal upgrade, in which ASMCA brings down all Oracle ASM instances on all nodes of the cluster, and then brings them all up in the new Grid home.

E.6.3.1 Preparing to Upgrade Oracle ASM

Note the following if you intend to perform rolling upgrades of Oracle ASM:

- The active version of Oracle Clusterware must be 11*g* release 2 (11.2). To determine the active version, enter the following command:

  ```
  $ crsctl query crs activeversion
  ```

- You can upgrade a standalone Oracle ASM installation to a clustered Oracle ASM installation. However, you can only upgrade an existing standalone Oracle ASM installation if you run the installation from the node on which the Oracle ASM installation is installed. You cannot upgrade a single instance Oracle ASM installation on a remote node.

- You must ensure that any rebalance operations on your existing Oracle ASM installation are completed before starting the upgrade process.

- During the upgrade process, you alter the Oracle ASM instances to an upgrade state. Because this upgrade state limits Oracle ASM operations, you should complete the upgrade process soon after you begin. The following are the operations allowed when an Oracle ASM instance is in the upgrade state:

  - Diskgroup mounts and dismounts

  - Opening, closing, resizing, or deleting database files

  - Recovering instances

  - Queries of fixed views and packages: Users are allowed to query fixed views and run anonymous PL/SQL blocks using fixed packages, such as dbms_diskgroup)

E.6.3.2 Upgrading Oracle ASM

Complete the following procedure to upgrade Oracle ASM:

1. On the node you plan to start the upgrade, set the environment variable ASMCA_ROLLING_UPGRADE as true. For example:

   ```
   $ export ASMCA_ROLLING_UPGRADE=true
   ```

2. From the Oracle grid infrastructure 11*g* release 2 (11.2) home, start ASMCA. For example:

   ```
   $ cd /u01/11.2/grid/bin
   $ ./asmca
   ```

3. Select **Upgrade**.

   ASM Configuration Assistant upgrades Oracle ASM in succession for all nodes in the cluster.

   > **See Also:**   *Oracle Database Upgrade Guide* and *Oracle Database Storage Administrator's Guide* for additional information about preparing an upgrade plan for Oracle ASM, and for starting, completing, and stopping Oracle ASM upgrades

E.7 Updating DB Control and Grid Control Target Parameters

Because Oracle Clusterware release 2 (11.2) is an out-of-place upgrade of the Oracle Clusterware home in a new location (the grid infrastructure for a cluster home, or Grid home), the path for the CRS_HOME parameter in some parameter files must be

changed. If you do not change the parameter, then you encounter errors such as "cluster target broken on dbcontrol or Grid control.

Use the following procedure to resolve this issue:

1. Log in to `dbconsole` or `gridconsole`.

2. Navigate to the **Cluster** tab.

3. Click **Monitoring Configuration**

4. Update the value for **Oracle Home** with the new Grid home path.

E.8 Downgrading Oracle Clusterware After an Upgrade

After a successful or a failed upgrade to Oracle Clusterware 11*g* release 2 (11.2), you can restore Oracle Clusterware to the previous version.

The restoration procedure in this section restores the Clusterware configuration to the state it was in before the Oracle Clusterware 11*g* release 2 (11.2) upgrade. Any configuration changes you performed during or after the 11*g* release 2 (11.2) upgrade are removed and cannot be recovered.

To restore Oracle Clusterware to the previous release:

1. On all remote nodes, use the command syntax *Grid_home*/crs/install/rootcrs.pl -downgrade [-force] to stop the 11*g* release 2 (11.2) resources, shut down the 11*g* release 2 (11.2) stack.

> **Note:** This command does not reset the OCR, or delete `ocr.loc`.

   For example:

   ```
   # /u01/app/11.2.0/grid/crs/install/rootcrs.pl -downgrade
   ```

   If you want to stop a partial or failed 11*g* release 2 (11.2) installation and restore the previous release Oracle Clusterware, then use the `-force` flag with this command.

2. After the `rootcrs.pl -downgrade` script has completed on all remote nodes, on the local node use the command syntax *Grid_home*/crs/install/rootcrs.pl -downgrade -lastnode -oldcrshome *pre11.2_crs_home* -version *pre11.2_crs_version* [-force], where *pre11.2_crs_home* is the home of the earlier Oracle Clusterware installation, and *pre11.2_crs_version* is the release number of the earlier Oracle Clusterware installation.

   For example:

   ```
   # /u01/app/11.2.0/grid/crs/install/rootcrs.pl -downgrade  -lastnode -oldcrshome
   /u01/app/crs -version 11.1.0.6.0
   ```

   This script downgrades the OCR, and removes binaries from the Grid home. If you want to stop a partial or failed 11*g* release 2 (11.2) installation and restore the previous release Oracle Clusterware, then use the `-force` flag with this command.

3. After the local node script completes, you are prompted to run `root.sh` from the earlier release Oracle Clusterware installation home in sequence on each member node of the cluster. After you complete this task, downgrade is completed.

Running `root.sh` from the earlier release Oracle Clusterware installation home restarts the Oracle Clusterware stack, starts up all the resources previously registered with Oracle Clusterware in the older version, and configures the old initialization scripts to run the earlier release Oracle Clusterware stack.

Index