Oracle® Collaboration Suite

High Availability Configuration

Release 2 (9.0.4) for UNIX and Linux

Part No. B15612-01

November 2004

ORACLE®

Oracle Collaboration Suite High Availability Configuration, Release 2 (9.0.4) for UNIX and Linux

Part No. B15612-01

Primary Authors: Raymond Dutcher, Ashish Prabhu

Contributor: Lyju Vadassery

Contents

List of Figures

List of Tables

Send Us Your Comments

Oracle Collaboration Suite High Availability Configuration, Release 2 (9.0.4) for UNIX and Linux

Part No. B15612-01

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: infodev_us@oracle.com
- FAX: (650) 506-7410. Attn: Oracle Collaboration Suite Documentation Manager
- Postal service:

  Oracle Corporation
  Server Technologies Documentation Manager
  500 Oracle Parkway, Mailstop 2op5
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This preface contains the following topics:

- Intended Audience
- Documentation Accessibility
- Structure
- Conventions

Intended Audience

Oracle Collaboration Suite High Availability Configuration is intended for administrators of Oracle Collaboration Suite. This document describes the procedure for installing and configuring a high-availability Oracle Collaboration Suite solution. However, all the possible ways of architecting the product are not covered in this document. Where applicable, alternative ways of architecting Oracle Collaboration Suite have been mentioned.

The instructions in this document were tested in a Sun Solaris 2.8 environment with SunCluster 3.1. Unless specified differently, these instructions are meant for the Solaris operating environment. There may be port-specific requirements for other UNIX platforms and Linux.

This document supplements the Oracle Collaboration Suite documentation, which you can access at

`http://www.oracle.com/technology/documentation/collab.html`

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. 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 additional information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation

JAWS, a Windows screen reader, 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, JAWS 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.

Structure

This document contains the following chapters and appendixes:

Chapter 1, "Overview of Oracle Collaboration Suite"

This chapter provides an overview of the components of Oracle Collaboration Suite.

Chapter 2, "Overview of High-Availability Architecture"

This chapter provides an overview of the high-availability architecture for deploying Oracle Collaboration Suite.

Chapter 3, "Installing and Configuring for High Availability"

This chapter provides instructions on installing and configuring Oracle Collaboration Suite for high availability.

Chapter 4, "Applying the 9.0.4.2 Patch Set"

This chapter supplements the instructions in the `readme` file for applying the 9.0.4.2 patch set.

Chapter 5, "Applying the 9.0.1.5 Patch Set"

This chapter supplements the instructions in the `readme` file for applying the 9.0.1.5 patch set.

Chapter 6, "Applying the 3620912 Patch"

This chapter provides instructions for applying the 3620912 patch.

Appendix A, "Acknowledgments"

This appendix lists the names of the Oracle partners who have contributed to the test environment used for developing this document.

Appendix B, "Component Startup and Shutdown Scripts"

This appendix provides scripts for starting up and shutting down Oracle Collaboration Suite components.

Appendix C, "Backing Up Information Storage and Software"

This appendix provides instructions for performing Information Storage and software backups.

Appendix D, "Creating Information Storage Tablespaces"

This appendix provides information and scripts for creating Information Storage tablespaces.

Appendix E, "Storage and Backup Planning Table"

This appendix provides information about the storage and backup requirements of Oracle Collaboration Suite tiers.

Appendix F, "Installation Checklist"

This appendix provides a checklist of the steps for installing and configuring Oracle Collaboration Suite for high availability.

Appendix G, "References"

This appendix provides references to documents and MetaLink notes that provide information about Oracle Collaboration Suite high availability.

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples
- Conventions for Microsoft Windows Operating Systems

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.
`UPPERCASE monospace (fixed-width) font`	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a `NUMBER` column. You can back up the database by using the `BACKUP` command. Query the `TABLE_NAME` column in the `USER_TABLES` data dictionary view. Use the `DBMS_STATS.GENERATE_STATS` procedure.

Convention	Meaning	Example
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter sqlplus to open SQL*Plus. The password is specified in the orapwd file. Back up the data files and control files in the /disk1/oracle/dbs directory. The department_id, department_name, and location_id columns are in the hr.departments table. Set the QUERY_REWRITE_ENABLED initialization parameter to true. Connect as oe user. The JRepUtil class implements these methods.
lowercase italic monospace (fixed-width) font	Lowercase italic monospace font represents placeholders or variables.	You can specify the *parallel_clause*. Run U*old_release*.SQL where *old_release* refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Brackets enclose one or more optional items. Do not enter the brackets.	DECIMAL (*digits* [, *precision*])
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	{ENABLE | DISABLE}
|	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
. . .	Horizontal ellipsis points indicate either:	
	■ That we have omitted parts of the code that are not directly related to the example	CREATE TABLE ... AS *subquery*;
	■ That you can repeat a portion of the code	SELECT *col1*, *col2*, ... , *coln* FROM employees;
. . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	

Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	acctbal NUMBER(11,2);
		acct CONSTANT NUMBER(4) := 3;

Convention	Meaning	Example

Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	`CONNECT SYSTEM/`*`system_password`*
		`DB_NAME = `*`database_name`*

`UPPERCASE`	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

`lowercase`	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files.
	Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

Conventions for Microsoft Windows Operating Systems

The following table describes conventions for Microsoft Windows operating systems and provides examples of their use.

Convention	Meaning	Example
Choose Start >	How to start a program.	To start the Database Configuration Assistant, choose Start > Programs > Oracle - *HOME_NAME* > Configuration and Migration Tools > Database Configuration Assistant.
File and directory names	File and directory names are not case sensitive. The following special characters are not allowed: left angle bracket (<), right angle bracket (>), colon (:), double quotation marks ("), slash (/), pipe (|), and dash (-). The special character backslash (\) is treated as an element separator, even when it appears in quotes. If the file name begins with \\, then Windows assumes it uses the Universal Naming Convention.	`c:\winnt"\"system32` is the same as `C:\WINNT\SYSTEM32`
`C:\>`	Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is the caret (^). Your prompt reflects the subdirectory in which you are working. Referred to as the *command prompt* in this manual.	`C:\oracle\oradata>`

Convention	Meaning	Example

	The backslash (\) special character is sometimes required as an escape character for the double quotation mark (") special character at the Windows command prompt. Parentheses and the single quotation mark (') do not require an escape character. Refer to your Windows operating system documentation for more information on escape and special characters.	C:\>exp scott/tiger TABLES=emp QUERY=\"WHERE job='SALESMAN' and sal<1600\"
		C:\>imp SYSTEM/*password* FROMUSER=scott TABLES=(emp, dept)

HOME_NAME	Represents the Oracle home name. The home name can be up to 16 alphanumeric characters. The only special character allowed in the home name is the underscore.	C:\> net start Oracle*HOME_NAME*TNSListener

1 Overview of Oracle Collaboration Suite

Oracle Collaboration Suite is an integrated, standards-based collaboration solution. It has a multitier architecture and is built on proven Oracle technology, Oracle9*i* Database and Oracle9*i* Application Server.

In the current business scenario, the availability of the collaboration system directly affects business processes, user productivity, and cost. Oracle Collaboration Suite consists of different components deployed on multiple tiers. The availability of each component has a direct impact on the availability of the system.

Besides providing high-availability features, Oracle Collaboration Suite must also be secure. This would ensure that both Internet and intranet users can use the system without compromising availability and security.

This chapter provides an overview of the following components of Oracle Collaboration Suite:

- Section 1.1, "Infrastructure Database and Oracle Internet Directory"
- Section 1.2, "Oracle9iAS Single Sign-On and Oracle Delegated Administration Services"
- Section 1.3, "Oracle Calendar Server and Oracle Files Domain Controller"
- Section 1.4, "Information Storage"
- Section 1.5, "Middle Tier Components"

1.1 Infrastructure Database and Oracle Internet Directory

Oracle Collaboration Suite Release 2 (9.0.4) Infrastructure is based on Oracle9*i* Application Server Release 2 (9.0.2). The Infrastructure consists of the Metadata Repository, an HTTP Server, and the `OC4J_DAS` instance. The Metadata Repository is based on Oracle9*i* Database release 9.0.1.4, and it stores Oracle Internet Directory information and Oracle9*i*AS Single Sign-On metadata.

The Infrastructure database and Oracle Internet Directory components are based on Oracle9*i* Application Server Infrastructure. Typically, these components are deployed behind a firewall on the intranet. In the deployment architecture described in this document, the Infrastructure is deployed on two tiers. The Infrastructure database and Oracle Internet Directory components are deployed on one tier. The Oracle9*i* Application Server Single Sign-On and Oracle Delegated Administration Services components, which are covered in the next section, are deployed on two or more servers on a single tier in the demilitarized zone (DMZ).

1.2 Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services

To secure the Infrastructure, the Middle Tier provides Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services to the application components. Together, the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components and the Infrastructure database and Oracle Internet Directory components provide the Oracle Identity Management service.

1.3 Oracle Calendar Server and Oracle Files Domain Controller

The Oracle Calendar Server and Oracle Files Domain Controller components are not deployed on the Middle Tier. They are deployed on a separate tier behind a firewall on the intranet. Oracle Calendar Server includes the file system level database that stores all calendar-related data. This database is not the Oracle Database, and it does not provide the same high-availability features.

The Oracle Calendar Server (one server per calendar node ID) and Oracle Files Domain Controller components are placed on a cold failover cluster because they are single processes. Alternatively, the Oracle Files Domain Controller can remain on the Middle Tier with proper monitoring and restart capabilities.

1.4 Information Storage

Information Storage is based on Oracle9*i* Database Release 2 (9.2). It is the data store for Oracle Collaboration Suite components and is deployed behind a firewall on the intranet.

1.5 Middle Tier Components

The Middle Tier components are based on Oracle9*i* Application Server. They are deployed in the DMZ and provide the application platform for all Oracle Collaboration Suite components.

2

Overview of High-Availability Architecture

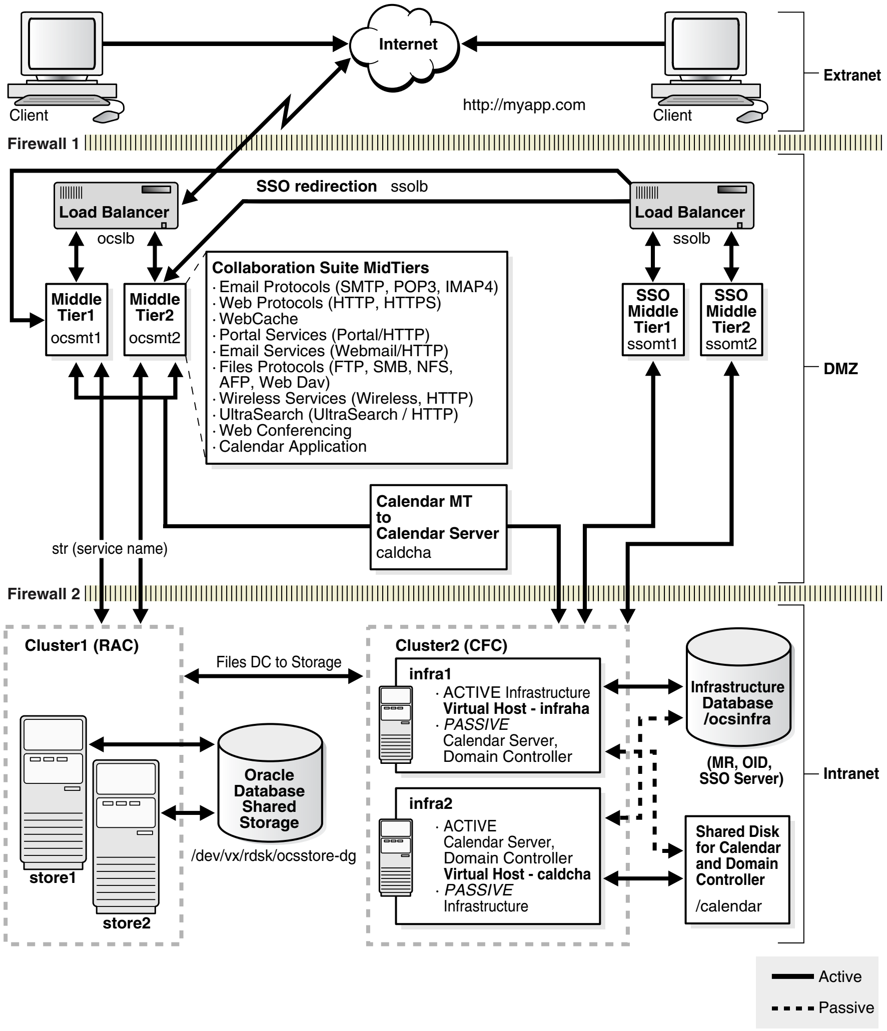
This chapter provides an overview of the high-availability architecture for deploying Oracle Collaboration Suite. It contains the following sections:

- Section 2.1, "Sample High-Availability Oracle Collaboration Suite Architecture"
- Section 2.2, "Infrastructure Database and Oracle Internet Directory Tier"
- Section 2.3, "Oracle Calendar Server and Oracle Files Domain Controller Tier"
- Section 2.4, "Oracle9iAS Single Sign-On and Oracle Delegated Administration Services Tier"
- Section 2.5, "Information Storage Tier"
- Section 2.6, "Oracle Collaboration Suite Middle Tiers"
- Section 2.7, "Network Planning for Oracle Collaboration Suite"

2.1 Sample High-Availability Oracle Collaboration Suite Architecture

Figure 2–1 displays a sample high-availability architecture for deploying Oracle Collaboration Suite. In the rest of this document, this sample architecture has been used to describe the instructions for achieving high-availability deployment.

Figure 2–1 Sample High-Availability Oracle Collaboration Suite Architecture



In this document, the Oracle domain name, `oracle.com`, has been used as an example. Where required, you must change the Oracle domain name to the domain name of your organization.

2.2 Infrastructure Database and Oracle Internet Directory Tier

The Infrastructure database and Oracle Internet Directory components are deployed on a two-node, hardware, active/passive, cold failover cluster on the intranet. The node on which these components are installed has a virtual host name. In Figure 2–1, this virtual host name is `infraha`. The setup of the Infrastructure database and Oracle Internet Directory tier is based on the instructions given in *Oracle9i Application Server Infrastructure: Improved Availability with Hardware Clusters.* This document provides information about implementing Oracle9*i* Application Server Cold Failover Clusters release 9.0.2 on Solaris. It can be accessed at

`http://www.oracle.com/technology/products/ias/hi_av/9ias_cfc.pdf`

In this setup, one node is active and the other is passive. A passive node is a node on which the operating system is running but no Oracle application has been started. There is one Oracle home directory, which is on a shared disk system along with the data files of the database. If a failover is necessary, then the database instance and Oracle Internet Directory processes will fail over to the surviving node. The Infrastructure database and Oracle Internet Directory passive node is the active node for Oracle Calendar Server and Oracle Files Domain Controller. This node has its own virtual host name.

When both nodes are available, one node will be active with the Infrastructure and Oracle Internet Directory components and the other node will be active with the Oracle Calendar Server and Oracle Files Domain Controller components. If either node fails, then the other node will have the Infrastructure, Oracle Internet Directory, Oracle Calendar Server, and Oracle Files Domain Controller running on it. This surviving node will have two virtual host names assigned to it.

2.3 Oracle Calendar Server and Oracle Files Domain Controller Tier

To set up cold failover for Oracle Calendar Server, when you install the Oracle Calendar Server and Oracle Files Domain Controller components, follow the same setup as that used for the Infrastructure. Like the Infrastructure, there is one Oracle home that is on a shared disk system. Because the Oracle Calendar Server database is on the Oracle home directory tree, it will be accessible to the surviving node in the event of a failover.

In normal mode, the Oracle Calendar Server and Oracle Files Domain Controller tier will run on the same cluster as the Infrastructure, but on the other node. In Figure 2–1, if the Infrastructure is running on `infra1` using `infraha` as the virtual host name, then Oracle Calendar Server and Oracle Files Domain Controller will run on `infra2` using `caldcha` as the virtual host name. This strategy puts both nodes of the cluster to optimal use. You must ensure that each node has the resources required to simultaneously handle Oracle Calendar Server, Oracle Files Domain Controller, the Infrastructure, and Oracle Internet Directory at the same time in the event of a failover. If a failover occurs, then both virtual host names, `infraha` and `caldcha,` will be assigned to the surviving node. The Oracle Files Domain Controller process controls and manages the nodes that constitute the Oracle Files domain.

Alternatively, the Oracle Files Domain Controller can be placed on a Middle Tier node.

2.4 Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services Tier

To install the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services tier, you must perform a single-node, Oracle Identity Management-only installation for the Infrastructure. During the installation, select only Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services as the components to be installed. Typically, this tier is installed in the demilitarized zone (DMZ).

To ensure availability, this tier has a minimum of two servers. Typically, these servers are not part of a hardware cluster. Both servers provide Oracle Delegated Administration Services and Oracle9*i*AS Single Sign-On services and are, therefore, functionally equivalent. If one server fails, then the other server continues to provide service.

In this architecture, a load balancer virtual server forms the front end of the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services tier. Middle Tier-access or end-user access to Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services is through the virtual server name of this Oracle9*i*AS Single Sign-On load-balancing server, which is `ssolb` in Figure 2–1. In this figure, incoming

HTTP traffic for the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services is distributed between the servers `ssomt1` and `ssomt2`.

Alternatives to deploying the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components to individual nodes are:

- Deploying the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components on the Middle Tier

  In such a deployment, the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components are deployed on the same nodes as the Middle Tier components in the DMZ, rather than on individual nodes. This reduces the number of servers required by half. If the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components are used for the entire organization, then combining them with the Middle Tier applications may compromise enterprise Oracle9*i*AS Single Sign-On availability during certain outages. Therefore, this is not the optimal deployment for high availability.

- Deploying the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components on the Infrastructure tier

  In such a deployment, the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components are deployed on the intranet. They would need to be configured for Internet access.

> **See Also:** For more information about configuring the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components for Internet access, refer to MetaLink note 255976.1.

2.5 Information Storage Tier

Typically, the Information Storage tier is deployed behind a firewall on the intranet. This tier uses Oracle Real Application Clusters. The default installation also sets up Oracle Net connection-time failover and cross-instance registration. The details of how this is set up are given in the `tnsnames.ora` and `listener.ora` files, which are in the `$ORACLE_HOME/network/admin` directory.

> **See Also:** *Oracle9i Net Services Administrator's Guide* and *Oracle9i Real Application Clusters Administration and Deployment Guide*

2.6 Oracle Collaboration Suite Middle Tiers

Typically, the Middle Tiers are deployed in the DMZ. In the setup illustrated in Figure 2–1, the hosts `ocsmt1` and `ocsmt2` are used for the Middle Tiers. A load balancer virtual server, `ocslb,` forms the front end of both Middle Tiers.

This tier contains all the Oracle Collaboration Suite application components, except Oracle Calendar Server and Oracle Files Domain Controller. As mentioned earlier, these two components reside on their own tier on the intranet. This tier connects to the Information Storage database by using the service name `str`.

2.7 Network Planning for Oracle Collaboration Suite

Network planning for Oracle Collaboration Suite is a key component of the procedure for setting up a high-availability Oracle Collaboration Suite solution. Features that are fundamental to such a solution include a properly planned network with sufficient bandwidth to support peak network traffic and alternate network paths to increase availability of the network.

See Also: *Network Planning for Oracle Collaboration Suite*, which you can access at

`http://www.oracle.com/broadband/showtripane.html?1656896`

For a distributed cold failover cluster, a typical installation involves deploying the servers and load balancer on the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services tier in the DMZ, and deploying the Infrastructure database and Oracle Internet Directory tier on the intranet. The installation described in this document is based on such a deployment. In some deployments, there might not be any firewalls separating the components.

By using a load balancer, you can ensure that the failure of a single server does not result in the loss of a critical resource. If one server fails, then the load balancer routes new requests to the other servers. In addition, to prevent the creation of single points of failure, you must deploy a redundant pair of load balancers. In the environment described in this document, F5 BIG-IP Load Balancer Limited has been used for the load balancer pair.

See Also: For information about using firewalls and load balancers, refer to *Oracle9i Application Server: Firewall and Load Balancer Architectures* at

`http://www.oracle.com/technology/products/ias/pdf/firewallLoadbalancer.pdf`

3

Installing and Configuring for High Availability

This chapter provides instructions on installing and configuring Oracle Collaboration Suite for high availability. It contains the following sections:

3.1 Overview of Installation and Configuration for High Availability

At a high level, the deployment of Oracle Collaboration Suite involves the following steps:

1. Implementing preinstallation recommendations
2. Installing the Infrastructure in an Oracle9*i*AS Cold Failover Cluster high-availability configuration
3. Installing and configuring Oracle9*i*AS Single Sign-On, Oracle Internet Directory, and Oracle Delegated Administration Services on the Middle Tiers
4. Installing and configuring the Information Storage database

5. Installing and configuring Oracle Calendar Server and Oracle Files Domain Controller using Oracle9*i*AS Cold Failover Cluster
6. Deploying the Oracle Collaboration Suite Middle Tiers

Note: Step 3 and Step 6 refer to different middle tiers. The Oracle9*i*AS Single Sign-On server and Oracle Delegated Administration Services are relocated to middle tiers that are different from the Oracle Collaboration Suite Middle Tiers. The applications are deployed on the Oracle Collaboration Suite Middle Tiers.

Each of these steps involves multiple setup and configuration changes. To reduce the effort required to rectify any mistake you may make, back up your work after every step before proceeding to the next step.

To back up your work, first shut down each tier in the reverse order of deployment. This means that you must first shut down the Oracle Collaboration Suite Middle Tiers, then shut down the Oracle Calendar Server and Oracle Files Domain Controller tier, and so on. To shut down these tiers, use the scripts provided in Appendix B.

Then, as displayed in the example in Appendix C, log in as `root`, and back up the entire file system. You must log in as `root` when you back up the file system so that `root` permissions and `setuid` bits on certain binaries are preserved.

For the Information Storage database on `store1` and `store2`, use the script listed in Appendix C to perform an Oracle Database Recovery Manager backup to disk.

Note: In the remaining sections of this document, the Infrastructure host and the Oracle Calendar Server and Oracle Files Domain Controller host are referred to by their virtual host names `infraha` and `caldcha`, respectively. This indicates the node in the cluster, either `infra1` or `infra2`, on which the addressed component is running.

For example, if the Infrastructure is deployed on `infra1` and Oracle Calendar Server is running on `infra2`, then the instruction to run the command `cmd` for the Infrastructure on `infraha` means that you must run the command on `infra1`.

3.2 Implementing Preinstallation Recommendations

Before you start installing and setting up the architecture, it is important to prepare the various elements that constitute the Oracle Collaboration Suite system, such as the load balancers and firewalls. You also need to determine the system kernel configuration, the amount of space required for each installation, and the amount of space required to back up each installation.

See Also: For information about platform-specific installation planning requirements, refer to the platform-specific installation and configuration guides at

`http://www.oracle.com/technology/documentation/collab.html`

Implementing preinstallation recommendations involves the following steps:

- Section 3.2.1, "Preparing Information to Be Specified During the Installation"
- Section 3.2.2, "Planning for Storage Requirements"
- Section 3.2.3, "Configuring System Kernel Parameters"
- Section 3.2.4, "Configuring Information Storage and Raw Volumes"

3.2.1 Preparing Information to Be Specified During the Installation

Use Table 3–1 as a reference during the installation. You will need to provide this information at various points during the installation.

Table 3–1 Information to Be Specified During the Installation

Role	Physical Host Name	Virtual Host Name or Load Balancer Virtual Server Name	Port Number
Infrastructure hosts	`infra1.oracle.com` and `infra2.oracle.com`	`infraha.oracle.com`	Oracle Internet Directory port 4032
Oracle9*i* Application Server Single Sign-On and Oracle Delegated Administration Services hosts	`ssomt1.oracle.com` and `ssomt2.oracle.com`	`ssolb.oracle.com` (load balancer)	80
Information Storage hosts	`store1.oracle.com` and `store2.oracle.com`		Database listener 1521
Oracle Files Domain Controller	`infra2.oracle.com` and `infra1.oracle.com`	`caldcha.oracle.com`	
Oracle Calendar Server	`infra2.oracle.com` and `infra1.oracle.com`	`caldcha.oracle.com`	Oracle Calendar Server 5730
Middle Tiers	`ocsmt1.oracle.com` and `ocsmt2.oracle.com`	`ocslb.oracle.com` (load balancer)	80

3.2.2 Planning for Storage Requirements

Before starting the installation, it is important to plan the storage requirements for all the tiers in the setup. When using hardware clusters, you also need to plan the requirements for the underlying disk groups and volumes that are used by the file systems for the software.

> **See Also:** Appendix E

3.2.3 Configuring System Kernel Parameters

Review the kernel parameter settings to ensure that they meet Oracle Collaboration Suite installation requirements. If these requirements are not met, then you may encounter errors during installation or operational errors after installation.

> **See Also:** For information about system kernel configuration, refer to the section on preparing for installation in *Oracle Collaboration Suite Installation and Configuration Guide for Solaris.*

3.2.4 Configuring Information Storage and Raw Volumes

In the configuration described in this document, the Information Storage database is deployed on a two-node cluster that is based on Oracle Real Application Clusters. The Oracle Real Application Clusters database on Solaris requires raw or shared volumes for storing data files. On some platforms, such as Linux, you can use a supported cluster file system instead of raw volumes.

If a cluster file system is not used, then depending on the shared storage attached to the cluster and the volume manager on the system, you must create the volumes that will be required later for the Oracle Real Application Clusters database. The Information Storage installer relies on the existence of certain volumes. Before you install Information Storage, you must create the following volumes:

- Section 3.2.4.1, "Base Tablespace Volumes"
- Section 3.2.4.2, "Oracle Files Store Volumes"
- Section 3.2.4.3, "Oracle Email Store Volumes"

3.2.4.1 Base Tablespace Volumes

You must create the volumes required for Oracle Real Application Clusters. The names and sizes of the required tablespaces are listed in Appendix D.

The Information Storage installer does not create all the tablespaces that are required. Before you can start the Middle Tier installation, you must run certain SQL scripts to create the missing tablespaces.

3.2.4.2 Oracle Files Store Volumes

If you are creating locally managed custom tablespaces, then the default options are recommended. You must not specify automatic segment space management for the tablespaces, because almost all Oracle Files data is stored as large objects (LOBs) and automatic segment space management does not support LOBs. In the installation described in this document, a single tablespace, `ofiles,` is used. The command for creating this tablespace is as follows:

```
CREATE TABLESPACE ofiles
DATAFILE '/dev/vx/rdsk/ocsstore-dg/ifs.dbf' SIZE 1000m REUSE;
```

See Also: *Oracle Files Planning Guide*

3.2.4.3 Oracle Email Store Volumes

The names of Information Storage tablespaces and their default storage parameters are mentioned in the `$ORACLE_HOME/oes/install/sql/tblspc.sql` script. The corresponding `CREATE` commands for Oracle Email tablespace raw volumes are given in Appendix D.

3.3 Installing the Infrastructure in a Cold Failover Cluster

For instructions about implementing the Oracle9*i*AS Cold Failover Cluster solution on Solaris, Linux, or HP-UX, refer to the corresponding *Oracle9i Application Server Infrastructure: Improved Availability with Hardware Clusters* document at

`http://www.oracle.com/technology/products/ias/hi_av/9ias_cfc.pdf`

For the Infrastructure installation, note the following exceptions to the setup procedure:

1. Follow the instructions given in *Oracle9i Application Server Infrastructure: Improved Availability with Hardware Clusters* up to the step that precedes the step involving running the `root.sh` script.
2. Before you run the `root.sh` script, perform the following steps:

   a. Run the following command to stop all processes managed by `opmn`:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

   > **Note:** At this stage of the installation, only the `opmn` and `dcm` daemons should be running. These daemons are shut down when you perform this step.

   b. Edit the `$ORACLE_HOME/Apache/Apache/bin/apachectl` file.

   In this file, add the entries for `LD_PRELOAD` and `LHOSTNAME` as described in *Oracle9i*AS *Infrastructure: Improved Availability with Hardware Clusters.*

   For example:

   ```
   LHOSTNAME=infraha
   LD_PRELOAD=libloghost.so.1
   export LHOSTNAME LD_PRELOAD
   ```

   c. Edit the `$ORACLE_HOME/opmn/conf/opmn.xml` file.

   In this file, add the lines for `dcm-daemon` as displayed in the following example.

   ```
   <custom gid="dcm-daemon" numProcs="1" noGidWildcard="true">
   <start path="/infracfc/oracle/902infra/dcm/bin/dcmctl daemon -logdir
   /infracfc/oracle/902infra/dcm/logs/daemon_logs"/>
   <stop path="/infracfc/oracle/902infra/dcm/bin/dcmctl shutdowndaemon"/>
   <environment>
   <prop name="DISPLAY" value="infraha.oracle.com:0.0"/>
   <prop name="LD_LIBRARY_PATH" value="/infracfc/oracle/902infra/lib"/>
   <prop name="LHOSTNAME" value="infraha"/>
   <prop name="LD_PRELOAD" value="libloghost.so.1"/>
   </environment>
   </custom>
   ```

   In this example: `ORACLE_HOME=/infracfc/oracle/902infra`

3. Change the following environment values:

   `DISPLAY=`*`virtual_hostname:display.screen`*
   `LD_LIBRARY_PATH=$ORACLE_HOME/lib`
   `LHOSTNAME=`*`virtual_hostname`* (short name, not fully qualified)

> **Note:** Depending on your platform, you also need to perform the following steps:
>
> - On HP-UX, include one additional line within the `environment` section for
>
>   `SHLIB_PATH=$ORACLE_HOME/lib32`
>
>   For example:
>
>   ```
>   <prop name="SHLIB_PATH"
>   value="/infracfc/oracle/902infra/lib32"/>
>   ```
>
> - On HP-UX, replace `libloghost.so.1` with `libloghost.sl.`
> - On Linux, fully qualify *`virtual_hostname.`*
>
>   For example: Use `infraha.oracle.com` instead of `infraha.`

4. Run the following command to start the `opmn` daemon:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl start
   ```

5. Run the following command to start the `dcm` daemon :

   ```
   $ORACLE_HOME/opmn/bin/opmnctl startproc type=custom gid=dcm-daemon
   ```

6. Run the `root.sh` script as instructed by the installer, and proceed with the installation.
7. After the installation is completed, run the following command to stop everything:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

   This command will stop Oracle Internet Directory, shut down the database, and stop the listener.
8. Edit the `$ORACLE_HOME/opmn/conf/opmn.xml` file.

   In this file, add lines for `OC4J_DAS` as displayed in the following example:

   ```
   <oc4j maxRetry="3" instanceName="OC4J_DAS" gid="OC4J_DAS" numProcs="1">
         <config-file path="/u01/app/orainf/product/infra904/j2ee/OC4J_
   DAS/config/server.xml"/>
         <java-option value="-server -Xincgc -Xnoclassgc -Xmx256m "/>
         <oc4j-option value="-properties"/>
         <port ajp="3001-3100" jms="3201-3300" rmi="3101-3200"/>
         <environment>
           <prop name="DISPLAY" value="infraha.oracle.com:0.0"/>
           <prop name="LD_LIBRARY_PATH" value="/infracfc/oracle/902infra/lib"/>
           <prop name="LHOSTNAME" value="infraha"/>
           <prop name="LD_PRELOAD" value="libloghost.so.1"/>
         </environment>
   </oc4j>
   ```

   In this example: `ORACLE_HOME=/infracfc/oracle/902infra`
9. Restart the listener, database, Oracle Internet Directory, and the processes managed by `opmn.`

Note: The Oracle9*i*AS Cold Failover Cluster document mentions the use of a reregistration script, `reregister.sh,` to reregister a node after a cold cluster node failover. Each time this script is run, it creates a new partner application. This buildup of partner applications is harmless, but it can clutter things. You can prevent this buildup of partner applications by saving a copy of the `$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf` file after the initial registration for each node.

The following is an example of the steps to be performed before starting Oracle Internet Directory and the `opmn` processes:

a. Make a copy of the `$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf` file on node 1 `(infra1)`.

To do this, run the following command:

```
cp $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf \
$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf.infra1
```

b. Follow the complete procedure for setting up the environment, and then test the Infrastructure failover process. When the first failover occurs, follow the reregistration steps given in the Oracle9*i*AS Cold Failover Cluster document.

c. After node 2, `infra2,` is failed over to and the new `osso.conf` file is re-created by the reregistration procedure, save a copy of this `osso.conf` file.

To do this, run the following command:

```
cp $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf \
$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf.infra2
```

For subsequent failovers, use the Infrastructure startup script given in Appendix B. This script includes the command for copying the saved `osso.conf` file.

10. Test the Oracle9*i* Application Server Single Sign-On administration application and the partner application Oracle Delegated Administration Services by using the following URLs:

    `http://`*`virtualhostname:port`*`/pls/orasso`
    For example: `http://infraha.oracle.com:7777/pls/orasso`

    `http://`*`virtualhostname:port`*`/oiddas`
    For example: `http://infraha.oracle.com:7777/oiddas`

11. After testing the `pls/orasso` URL, log in to the Oracle9*i*AS Single Sign-On server, click **SSO Server Administration,** and then click **Administer Partner Application.** Check the partner applications that have been registered.

    There should be two partner applications: the Oracle9*i*AS Single Sign-On server and the HTTP Oracle9*i*AS Single Sign-On `(mod_osso)` module on the Infrastructure. Note the `site_id` of the HTTP partner application.

12. After failover takes place, reset the Oracle9*i*AS Single Sign-On instance password and reregister the `mod_osso` partner application.

    The steps for doing this are defined in the Oracle9*i*AS Cold Failover Cluster document. After the reregistration, log in to `pls/orasso` and delete the old HTTP partner application whose `site_id` you had recorded in the previous step.

> **Note:** If the `orasso.conf` file was saved after the initial reregistration, then instead of reregistering and deleting the old partner application, replace the current `osso.conf` file with the saved `osso.conf` file, `osso.conf.infra1`.

13. Perform Step 10 to test the Oracle9*i*AS Single Sign-On (`orasso`) and Oracle Delegated Administration Services (`oiddas`) logins.

3.4 Moving Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services to the DMZ

When you perform the instructions described in Section 3.3, the Infrastructure and all of its components are installed in an Oracle9*i*AS Cold Failover Cluster environment. You must move the Oracle9*i*AS Single Sign-On server and Oracle Delegated Administration Services to separate nodes in the DMZ.

In the setup described in this chapter, the nodes for hosting the Oracle9*i*AS Single Sign-On server and Oracle Delegated Administration Services are `ssomt1.oracle.com` and `ssomt2.oracle.com.` A load-balancer virtual server `ssolb.oracle.com` forms the front end of these nodes.

This part of the deployment involves installing the Infrastructure and Middle Tier on `ssomt1.oracle.com` and on `ssomt2.oracle.com.`

During the installation, deselect all the components. This will install the application server with minimum features, such as the HTTP Server and the mods `(mod_osso, modplsql,` and `mod_oc4j)` on the two nodes.

When prompted for the location of Oracle9*i* Application Server Single Sign-On and Oracle Internet Directory during the installation of the Middle Tiers, specify the virtual host name `infraha.oracle.com.` This host name is the same as that used for the Infrastructure cold failover cluster installation.

After you complete both installations, reconfigure Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services to be accessed from the two Middle Tiers in the DMZ through the load balancer virtual server `ssolb.oracle.com.` To do this, you must first move the Oracle9*i*AS Single Sign-On server to the Middle Tier. Note that this changes access to the Oracle9*i*AS Single Sign-On server from the Infrastructure, `infraha.oracle.com,` to the Middle Tier. However, the database still resides on the Infrastructure host and can be accessed through `modplsql` at `infraha.oracle.com:1521:iasdb` by using `orasso/`*`password.`*

The following are additional steps that you need to perform for moving Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services to the DMZ:

- Section 3.4.1, "Setting Up the HTTP Server"
- Section 3.4.2, "Updating Distributed Configuration Management"
- Section 3.4.3, "Setting Up Database Access for modplsql"

3.4.1 Setting Up the HTTP Server

The installation can be done with the HTTP port set to the default port, 7777. However, in this setup, you need to change the default port from 7777 to 80. Also, because the HTTP Server will be accessed through the load balancer, change the

ServerName value to the load balancer virtual server name. In this example, this virtual server name is ssolb.oracle.com.

To change the default port, first stop the HTTP Server on the two Middle Tiers by running the following command:

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
```

Next, make the following changes in the $ORACLE_HOME/Apache/Apache/conf/httpd.conf file:

Original	Change To
Port 7777	Port 80
ssomt1.oracle.com ssomt2.oracle.com	ssolb.oracle.com
Listen 7778	Listen 80

This step configures the HTTP Servers on the Oracle9*i*AS Single Sign-On Middle Tiers to listen at the effective URL, which is ssolb.oracle.com.

3.4.2 Updating Distributed Configuration Management

To update Distributed Configuration Management, run the following command:

```
$ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs
```

For the Oracle9*i*AS Single Sign-On Middle Tiers, you will not be using Oracle9*i* Application Server Web Cache. Shut down Web Cache by running the following command:

```
webcachectl stop
```

3.4.3 Setting Up Database Access for modplsql

On the two Oracle9*i*AS Single Sign-On Middle Tiers, set up database access for modplsql in the $ORACLE_HOME/Apache/modplsql/conf/dads.conf file. This file is used by the HTTP Server through modplsql to access the Oracle9*i*AS Single Sign-On server database.

To set up database access for modplsql:

1. Determine the Infrastructure database orasso password.

   This step requires the use of the orasso schema password, which is in the dads.conf file. To get this password, first connect to Oracle Internet Directory and then search for the orasso password entry. This can be done through the oidadmin GUI interface or by running the following command (all on one line):

   ```
   ldapsearch -h host -p oid-port -D "cn=orcladmin" -w oidpwd \
   -b "cn=IAS Infrastructure Databases,cn=IAS,cn=Products,cn=OracleContext" \
   -s sub "orclResourceName=orasso" orclpasswordattribute
   ```

   In this command:

   host=infraha.oracle.com
   oid-port=4032
   oidpwd=*orcladmin password*, which you specified during installation

2. Test the `orasso` password by running the following command to log in to the database on the Infrastructure host:

   ```
   sqlplus orasso/password # This is the password returned by the ldapsearch
   command
   ```

3. Copy the `dads.conf` file from the Infrastructure to the Oracle9*i* Application Server Single Sign-On Middle Tiers.

   Copy the contents of the `$ORACLE_HOME/Apache/modplsql/conf/dads.conf` file on the Infrastructure host to the `dads.conf` file on `ssomt1.oracle.com` and `ssomt2.oracle.com`.

4. Replace the password in the `dads.conf` file.

   In each Oracle9*i* Application Server Single Sign-On Middle Tier `dads.conf` file, which is located in the `$ORACLE_HOME/Apache/modplsql/conf/` directory, replace the value of `PlsqlDatabasePassword` with the `orasso` password retrieved in Step 1.

3.5 Configuring the Oracle9*i*AS Single Sign-On Server to Use a Load Balancer

The procedure for configuring the Oracle9*i*AS Single Sign-On server to use a load balancer can be divided into the following steps:

- Section 3.5.1, "Modifying the Oracle9iAS Single Sign-On Server Settings of the Oracle9iAS Single Sign-On URL"
- Section 3.5.2, "Reregistering Partner Applications"

3.5.1 Modifying the Oracle9*i*AS Single Sign-On Server Settings of the Oracle9*i*AS Single Sign-On URL

Because the two Oracle9*i*AS Single Sign-On Middle Tiers will each have a load balancer as their front end, these load balancers will provide the URLs used to access Oracle9*i*AS Single Sign-On server.

To modify the Oracle9*i*AS Single Sign-On settings of the Oracle9*i*AS Single Sign-On URL:

1. Check the partner application entries in Oracle9*i*AS Single Sign-On.

   Before changing the Oracle9*i*AS Single Sign-On server URL, check the partner application entries in Oracle9*i*AS Single Sign-On. To do this, log in to the database as the `orasso` user and run the following query on the Infrastructure host:

   ```
   SQL> SELECT SITE_NAME,SUCCESS_URL,FAILURE_URL,HOME_URL,LOGOUT_URL
   FROM wwsso_papp_configuration_inf_t
   ORDER BY site_id;
   ```

   The following entries should be displayed as the results of this query:

   SSO Server
   HTTP (`mod_osso`) entry for the Infrastructure installation
   HTTP (`mod_osso`)entry for `ssomt1.oracle.com`
   HTTP (`mod_osso`)entry for `ssomt2.oracle.com`

   The entry for the Oracle9*i*AS Single Sign-On server will have the URLs pointing to `infraha.oracle.com`.

2. Run the following command to change the Oracle9*i*AS Single Sign-On server URL to point to the load balancer URL:

   ```
   $ORACLE_HOME/sso/bin/ssocfg.sh http ssolb.oracle.com 80
   ```

   Note: On HP-UX, set `SHLIB_PATH=$ORACLE_HOME/lib32` before running the command.

3. Log in to the database as the `orasso` user, and run the following query to verify that the Oracle9*i*AS Single Sign-On server URL has been modified:

   ```
   SQL> SELECT SITE_NAME,SUCCESS_URL,FAILURE_URL,HOME_URL,LOGOUT_URL
   FROM wwsso_papp_configuration_inf_t
   ORDER BY site_id;
   ```

   The first entry for the Oracle9*i*AS Single Sign-On server will be modified with the URL containing the load balancer virtual server name, `ssolb.oracle.com,` that was used with the `ssocfg.sh` script.

3.5.2 Reregistering Partner Applications

As mentioned in the preceding section, there are four partner applications registered with the Oracle9*i*AS Single Sign-On server. After running the `ssocfg.sh` script to relocate the Oracle9*i*AS Single Sign-On server, you must reregister the partner applications with Oracle9*i*AS Single Sign-On. To do this:

1. Modify the partner application in the database.

   Because Oracle9*i*AS Single Sign-On on both the Middle Tiers will be accessed through the load balancer, only one entry needs to exist in the database. To make this change, run the following Oracle9*i*AS Single Sign-On registrar script (all on one line):

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar \
   -oracle_home_path /ssomid/app/oracle/product/sso \
   -host infraha.oracle.com \
   -port 1521 \
   -sid iasdb \
   -site_name sso.ssolb.oracle.com \
   -success_url http://ssolb.oracle.com:80/osso_login_success\
   -logout_url http://ssolb.oracle.com:80/osso_logout_success \
   -cancel_url http://ssolb.oracle.com:80 \
   -home_url http://ssolb.oracle.com:80 \
   -config_mod_osso TRUE
   -u root \
   -sso_server_version v1.2
   ```

   Note: On HP-UX, set `SHLIB_PATH=$ORACLE_HOME/lib32` before running this script.

   Run this script from one of the Middle Tiers. This will create a new partner application in the database with the load balancer URL and update the `$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf` file on that Middle Tier. This file must also be updated for the second Middle Tier. However, there is no need to reregister with the database, because an entry with the load balancer has already been created.

2. Check the `mod_osso.conf` file in the Middle Tiers.

   Log in to the database with `orasso/`*`password`* and check the partner application table of the Oracle9*i*AS Single Sign-On server. There should be an additional entry for `HTTP/mod_osso` with the virtual server name of the load balancer.

   To verify that the additional entry is created, run the following query:

   ```
   SQL> SELECT * FROM wwsso_papp_configuration_inf_t ORDER BY site_id;
   ```

3. Start the HTTP Server.

   To start the HTTP Server on the first Middle Tier, where it was reregistered with the load balancer URL, run the following commands:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl start
   $ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
   ```

   Set up the load balancer and shut down `ssomt2.oracle.com`, so that the load balancer does not direct any traffic to that node.

4. Create the `osso_clear.txt` file.

   To do this:

   a. Log in to Oracle9*i*AS Single Sign-On at

      ```
      http://ssolb.oracle.com/pls/orasso
      ```

   b. Click **SSO Server Administration.**

   c. Click **Administer Partner Applications.**

      All the partner applications will be listed on this page.

   d. Click the **Edit** icon for the partner application that was registered with the load balancer URL in the previous steps to display the following values in a clear-text file:

   ```
   cipher_key=Value of the encryption key for this partner application
   site_id=value of ID
   site_token=value of Token
   login_url=value of login URL
   cancel_url=value of HOME URL
   sso_server_version=1.2
   sso_timeout_cookie_name=SSO_ID_TIMEOUT
   ```

   e. Copy these values into a clear-text file named `osso_clear.txt` in the `$ORACLE_HOME/Apache/Apache/conf/osso/` directory on `ssomt2`.

      The following are sample contents of the `osso_clear.txt` file after the required changes have been made:

      ```
      cipher_key=2419FEED96D8FA4B
      site_id=1326
      site_token=K1H0R45Y1326
      login_url=http://ssolb.oracle.com/pls/orasso/orasso.wwsso_app_admin.ls_
      login
      logout_url=http://ssolb.oracle.com:80/osso_logout_success
      cancel_url=http://ssolb.oracle.com:80
      sso_timeout_cookie_name=SSO_ID_TIMEOUT
      ```

5. Regenerate an obfuscated `osso.conf` file from the `osso_clear.txt` file by running the following command:

```
$ORACLE_HOME/Apache/Apache/bin/iasobf oss_clear.txt osso.conf root
```

The `iasobf` utility enables you to generate an obfuscated wallet password from a clear-text password.

6. Log in to Oracle9*i*AS Single Sign-On, and delete the entries for `ssomt1` and `ssomt2`.

   Only one partner application entry with `ssolb` is required.

7. Log in to the Oracle9*i*AS Infrastructure database as the `orasso` user, and update the Oracle9*i*AS Single Sign-On server configuration table so that a request coming from `ssomt1` or `ssomt2` is accepted, even though the URL is `ssolb.oracle.com`.

   To do this, run the following commands:

   ```
   SQL> UPDATE wwsec_enabler_config_info$ SET url_cookie_ip_check='N' ;
   SQL> commit;
   ```

8. Close down access to `ssomt1` so that the load balancer points to `ssomt2`.
9. Log in to the Oracle9*i*AS Single Sign-On server at `http://ssolb.oracle.com/pls/orasso` as the `orcladmin` user.

   The load balancer will divert this request to `ssomt2`. This request will access the `pls/orasso` directive in the `dads.conf` file and connect to the Oracle9*i*AS Single Sign-On server (Infrastructure database) through the entries in the `dads.conf` file and the `orasso` login.

10. Enable both the Oracle9*i*AS Single Sign-On Middle Tiers, `ssomt1.oracle.com` and `ssomt2.oracle.com`, from the load balancer.
11. Test the Oracle9*i*AS Single Sign-On logins from both the nodes.

3.6 Moving Oracle Delegated Administration Services to the Oracle9*i*AS Single Sign-On Middle Tier

After you move the Oracle9*i*AS Single Sign-On server to the middle tiers `ssomt1` and `ssomt2`, you also need to move the `OC4J_DAS` instance from the Infrastructure tier to these middle tiers.

Just as you changed access to the Oracle9*i*AS Single Sign-On server through the load balancer and `modplsql`, this procedure involves changing the access to the `OC4J_DAS` instance residing on the Infrastructure. To do this:

1. Configure `$ORACLE_HOME/Apache/Apache/conf/mod_oc4j.conf` for `oiddas` access in the Oracle9*i*AS Single Sign-On middle tier.

   To change the mount configuration `OC4J_DAS` directive in the `mod_oc4j.conf` file to point to the `OC4J_DAS` instance on the Infrastructure, you need to change:

   ```
   Oc4jMount /oiddas OC4J_DAS
   Oc4jMount /oiddas/* OC4J_DAS
   ```

   to:

   ```
   Oc4jMount /oiddas instance://iasdb.infraha.oracle.com:OC4J_DAS
   Oc4jMount /oiddas/* instance://iasdb.infraha.oracle.com:OC4J_DAS
   ```

Here, `iasdb.infraha.oracle.com` is the instance name of the Infrastructure as listed in the Enterprise Manager targets or displayed by running the `dcmctl listInstances` command.

2. Log in to Oracle Directory Manager `(oidadmin)` as `orcladmin/`*`password`*. Then:

   a. Click **cn=Entry Management.**

   b. Click **cn=OracleContext.**

   c. Click **cn=Products.**

   d. Click **cn=DAS.**

   e. Click **cn=OperationURLs.**

   Change the `orcldasurlbase` attribute from the Infrastructure HTTP URL and port to the load balancer URL and port, which is 80 in this example.

3. Edit the `opmn.xml` file on the Infrastructure.

   Update the Apache Java Protocol (AJP) port numbers for the specific ones that will be opened in the firewall, instead of the range of ports that are used by default.

4. Restart the Infrastructure and Oracle9*i*AS Single Sign-On Middle Tiers.

5. To validate the Oracle Delegated Administration Services URL change, access the partner application `oiddas` from the Middle Tier by using the following URL:

   `http://ssolb.oracle.com/oiddas`

   This connects to the `OC4J_DAS` instance on the Infrastructure through the `Oc4jMount` directive in the `mod_oc4j.conf` file.

By performing steps 2 through 5, you are updating the Oracle Internet Directory entry for the location of Oracle Delegated Administration Services.

3.7 Installing and Configuring Information Storage to Use Oracle Real Application Clusters

During the installation, Information Storage is based on Oracle9*i* Database Release 2 (9.2.0.3) and contains the schemas and tablespaces for all the Oracle Collaboration Suite applications. Setting up Information Storage involves configuring the Information Storage database on Oracle Real Application Clusters and outlining the preparation for the two nodes of the cluster for the Information Storage installation.

Remember that Oracle Calendar Server does not store any data in this database. Instead, it uses the file system on the Oracle Calendar Server node, `caldcha.oracle.com`, for its database.

Before you perform the steps described in this section, verify that you have performed all the preinstallation steps. It is also recommended that you upgrade the Information Storage database to Oracle9*i* Database Release 2 (9.2.0.5). Note that this upgrade has not been tested, and you must read the instructions on the MetaLink Web site before performing the upgrade.

The information within this section is meant for use on the Solaris platform. For information about the steps to install Information Storage in Oracle Real Application Clusters on Linux, refer to MetaLink note 281677.1.

In *Oracle Collaboration Suite Release Notes Release 2 (9.0.4.1)* for Solaris, it is mentioned that Oracle Real Application Clusters cannot be enabled with a pre-seeded Oracle

Collaboration Suite Release 2 Information Storage database. However, you *can* enable Oracle Real Application Clusters with a pre-seeded Oracle Collaboration Suite Release 2 Information Storage database by performing the steps described in this section.

This section discusses the following high-level steps involved in enabling Oracle Real Application Clusters with a pre-seeded Oracle Collaboration Suite Release 2 Information Storage database:

- Section 3.7.1, "Creating the DBCA_RAW_CONFIG File"
- Section 3.7.2, "Creating the Database with the Required Tablespaces"
- Section 3.7.3, "Unlocking the Oracle Web Conferencing Real-Time Collaboration Schemas"
- Section 3.7.4, "Creating Tablespaces That Are Not Created by the Database Configuration Assistant"
- Section 3.7.5, "Setting the MAX_COMMIT_PROPAGATION_DELAY Parameter"
- Section 3.7.6, "Copying Binary Files to Remote Nodes"

3.7.1 Creating the DBCA_RAW_CONFIG File

During installation, the installer uses the Database Configuration Assistant for creating the Oracle Real Application Clusters database. Unless you are using a cluster file system , this assistant will require raw volumes for the data files. Verify that you have created the required volumes as described in Section 3.2. Then create a file with the tablespace name and the corresponding data file name, `dbca.txt,` as follows:

dbca.txt (TABLESPACE_NAME=*`file-name`*)

```
system=/dev/vx/rdsk/ocsstore-dg/system01.dbf
temp=/dev/vx/rdsk/ocsstore-dg/temp01.dbf
undotbs1=/dev/vx/rdsk/ocsstore-dg/undotbs01.dbf
undotbs2=/dev/vx/rdsk/ocsstore-dg/undotbs02.dbf
control1=/dev/vx/rdsk/ocsstore-dg/control01.dbf
control2=/dev/vx/rdsk/ocsstore-dg/control02.dbf
control3=/dev/vx/rdsk/ocsstore-dg/control03.dbf
redo1_1=/dev/vx/rdsk/ocsstore-dg/redo01_01.log
redo1_2=/dev/vx/rdsk/ocsstore-dg/redo01_02.log
redo1_3=/dev/vx/rdsk/ocsstore-dg/redo01_03.log
redo2_1=/dev/vx/rdsk/ocsstore-dg/redo02_04.log
redo2_2=/dev/vx/rdsk/ocsstore-dg/redo02_05.log
redo2_3=/dev/vx/rdsk/ocsstore-dg/redo02_06.log
tools=/dev/vx/rdsk/ocsstore-dg/tools01.dbf
users=/dev/vx/rdsk/ocsstore-dg/users01.dbf
xdb=/dev/vx/rdsk/ocsstore-dg/xdb01.dbf
cwmlite=/dev/vx/rdsk/ocsstore-dg/cwmlite01.dbf
drsys=/dev/vx/rdsk/ocsstore-dg/drsys01.dbf
EXAMPLE=/dev/vx/rdsk/ocsstore-dg/example01.dbf
INDX=/dev/vx/rdsk/ocsstore-dg/indx01.dbf
ODM=/dev/vx/rdsk/ocsstore-dg/odm01.dbf
spfile=/dev/vx/rdsk/ocsstore-dg/spfilestr.ora
```

> **See Also:** For the names of Information Storage e-mail tablespaces and their default storage parameters, refer to the following script:
>
> `$ORACLE_HOME/oes/install/sql/tblspc.sql`

3.7.2 Creating the Database with the Required Tablespaces

Set up the environment variable DBCA_RAW_CONFIG to point to the dbca.txt file. You can use the following command to do this:

```
export DBCA_RAW_CONFIG=$ORACLE_HOME/dbca.txt
```

Then run the installer. This will create a database with the tablespaces covered in the preceding section.

During the installation, you must specify the primary Oracle Real Application Clusters node, which is store1 in this case. Later, you will need to modify the database Oracle Internet Directory registration to make it Oracle Real Application Clusters aware.

3.7.3 Unlocking the Oracle Web Conferencing Real-Time Collaboration Schemas

During the installation, unlock the RTC and RTC_APP schemas. To unlock these schemas, use the Password management tab of the Database Configuration Assistant. If this cannot be done, then connect to the database as sysdba after the installation, and run the following command:

```
ALTER USER [rtc|rtc_app] ACCOUNT UNLOCK
```

Note down the SYS and SYSTEM passwords during the installation, because you will need to use these passwords later.

3.7.4 Creating Tablespaces That Are Not Created by the Database Configuration Assistant

You must create the tablespaces that are not created by the Database Configuration Assistant. This section provides information about these tablespaces.

3.7.4.1 Oracle Web Conferencing Real-Time Collaboration Store

```
RTC_BIG_DATA=/dev/vx/rdsk/ocsstore-dg/RTC_BIG_DATA.dbf
RTC_DATA=/dev/vx/rdsk/ocsstore-dg/RTC_DATA.dbf
RTC_INDEX=/dev/vx/rdsk/ocsstore-dg/RTC_INDEX.dbf
RTC_LARGE_DATA=/dev/vx/rdsk/ocsstore-dg/RTC_LARGE_DATA.dbf
```

3.7.4.2 Oracle Email Store

For the names of Information Storage tablespaces and their default storage parameters refer to the $ORACLE_HOME/oes/install/sql/tblspc.sql script.

```
esbigtbl=/dev/vx/rdsk/ocsstore-dg/esbigtbl.dbf
esfreqidx=/dev/vx/rdsk/ocsstore-dg/esfreqidx.dbf
esfreqtbl=/dev/vx/rdsk/ocsstore-dg/esfreqtbl.dbf
ESFREQIDX=/dev/vx/rdsk/ocsstore-dg/esinfreqidx.dbf
ESMRLMNR=/dev/vx/rdsk/ocsstore-dg/eslmmr.dbf
ESNEWS=/dev/vx/rdsk/ocsstore-dg/esnews.dbf
ESORATEXT=/dev/vx/rdsk/ocsstore-dg/esoratext.dbf
ESPERFTBL=/dev/vx/rdsk/ocsstore-dg/esperftbl.dbf
ESSMLTBL=/dev/vx/rdsk/ocsstore-dg/essmltbl.dbf
ESTERSTORE=/dev/vx/rdsk/ocsstore-dg/esterstore.dbf
ESTEMP=/dev/vx/rdsk/ocsstore-dg/estemp.dbf
```

The following is a sample script for creating Oracle Email storage tablespaces:

```
CREATE TABLESPACE ESBIGTBL
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esbigtbl.dbf' SIZE 100m REUSE;
```

```
CREATE TABLESPACE ESSMLTBL
DATAFILE '/dev/vx/rdsk/ocsstore-dg/essmltbl.dbf' SIZE 20m REUSE;
CREATE TABLESPACE ESFREQTBL
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esfreqtbl.dbf' SIZE 20m REUSE;
CREATE TABLESPACE ESFREQIDX
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esfreqidx.dbf' SIZE 10m REUSE;
CREATE TABLESPACE ESINFREQIDX
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esinfreqidx.dbf' SIZE 10m REUSE;
CREATE TABLESPACE ESTERSTORE
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esterstore.dbf' SIZE 20m REUSE;
CREATE TABLESPACE ESPERFTBL
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esperftbl.dbf' SIZE 20m REUSE;
CREATE TABLESPACE ESORATEXT
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esoratext.dbf' SIZE 20m REUSE;
CREATE TABLESPACE ESNEWS
DATAFILE '/dev/vx/rdsk/ocsstore-dg/esnews.dbf' SIZE 10m REUSE;
CREATE TABLESPACE ESMRLMNR
DATAFILE '/dev/vx/rdsk/ocsstore-dg/eslmmr.dbf' SIZE 50m REUSE;
CREATE TEMPORARY TABLESPACE ESTEMP
TEMPFILE '/dev/vx/rdsk/ocsstore-dg/estemp.dbf' SIZE 50M;
```

3.7.4.3 Oracle Files

You can use the default USERS tablespace that is listed during the Oracle Files installation. However, it is recommended that you create separate tablespaces for the Oracle Files installation.

> **See Also:** *Oracle Files Planning Guide* for information about the recommended Oracle Files tablespace configuration

3.7.5 Setting the MAX_COMMIT_PROPAGATION_DELAY Parameter

To ensure that commits made by one connection to one database instance are immediately visible to a connection against the other database instance, you must set the MAX_COMMIT_PROPAGATION_DELAY parameter to 1. The default setting of 700, which is 7 seconds, needs to be changed because it will not work. Resetting this parameter requires restarting the Information Storage database instances.

> **See Also:** MetaLink note 259454.1

3.7.6 Copying Binary Files to Remote Nodes

Due to a known issue documented under bug 3098122, three files do not get copied to the remote Oracle Real Application Clusters nodes. You must manually transfer these files to the remote Oracle Real Application Clusters nodes. These files are in the $ORACLE_HOME/bin directory. On Solaris, these files are named dbsnmp, oidpasswd, and oradism. You can use either a remote copy command or perform a binary FTP operation.

3.8 Installing and Configuring Oracle Calendar Server and Oracle Files Domain Controller

Set up the Oracle Calendar Server and the Oracle Files Domain Controller components on the same cluster as the Infrastructure but on the second node, infra2, as displayed in Figure 2–1. Use a mount point that is different from the Infrastructure Oracle home mount point. You must use a different operating system user, for example, calendar.

3.8.1 Installing Oracle Calendar Server and Oracle Files Domain Controller

To install Oracle Calendar Server and Oracle Files Domain Controller:

1. Set up Library Interpositioning.

   Follow the Oracle9*i*AS Cold Failover Cluster document to set up Library Interpositioning, exactly the way it was done for the Infrastructure installation. Because Oracle Calendar Server and Oracle Files Domain Controller use the same cluster that was used for the Infrastructure, Library Interpositioning should have already been set up on this node. Note that a different virtual host name, `caldcha.oracle.com,` is used for this node.

   When setting up Library Interpositioning, you must apply the following changes to the instructions given in Section 3.3:

   - `ORACLE_HOME=/caldccfc/oracle/902caldc`
   - The virtual host name is `caldcha,` instead of `infraha`
   - `OPMN` is not required on this node

2. Verify the Library Interpositioning setup.
3. Leave only a single instance of the Information Storage database running. Shut down all other Information Storage database instances.

   If there is more than one instance of the Information Storage database, then the Files Configuration Assistant, `ifsca,` will fail. This is because the assistant uses the JDBC thin driver.

4. Install Oracle Calendar Server and Oracle Files Domain Controller in the same Oracle home. Use the virtual host name, `caldcha.oracle.com,` for the host name during this installation.
5. During the installation, select **Oracle Calendar Server** and **Oracle Files** on the Select Components screen.
6. Select the default node ID of 1 for Oracle Calendar Server. Enter values for the Host (virtual host name, for example, `caldcha.oracle.com`), Port (usually 5730), and Node-ID (1) for Oracle Calendar Server.
7. During the Oracle Files installation, select **Domain Controller,** and deselect **HTTP node** and **Regular node.**
8. During the Oracle Files Domain Controller installation, specify the schema and tablespace for Oracle Files. It is recommended that you do not use the default tablespace, `USERS,` when prompted by `ifsca.` Select the Oracle Files tablespace, which is `ofiles` in the example in this document, for all objects, such as tables and indexes. The tablespaces must exist so that they can be selected during the installation.

   See Also: *Oracle Files Planning Guide* for more information about Oracle Files database sizing recommendations

3.8.2 Modifying the unison.ini File for Oracle Calendar Server

For a cold failover of Oracle Calendar Server to work correctly, you must ensure that the virtual host name is used in the main configuration file of Oracle Calendar Server, `$ORACLE_HOME/ocal/misc/unison.ini.` During the installation, the `unidas` section of the `unison.ini` file is set to the local host. To change the local host name to the virtual host name:

1. Shut down Oracle Calendar Server by running the following command:

```
$ORACLE_HOME/ocal/bin/unistop
```

2. In the *local-host*.unidas line of the unison.ini file, replace the local host name with the virtual host name. The following illustrates these changes for the configuration described in this document:

Original	Change To
[infra1,unidas]	[caldcha,unidas]
numconnect = 50	numconnect = 50
enable = TRUE	enable = TRUE

3. Restart Oracle Calendar Server by running the following command:

```
$ORACLE_HOME/ocal/bin/unistart
```

3.8.3 Modifying the registry.xml File for Oracle Files Domain Controller

Add a line for the DatabaseUrl element in the $ORACLE_HOME/ifs/common/registry.xml file, as displayed in the following example:

```
<Instances>
   <Instance>
      <Domain>ifs://store1.oracle.com:1522:str.oracle.com:IFS</Domain>
      <DomainType>files</DomainType>
      <Registered>1099611880481</Registered>
      <LastModified>1099612384746</LastModified>
      <LastStarted>1099682252758</LastStarted>
      <DatabaseUrl>jdbc:oracle:oci8:@str.oracle.com</DatabaseUrl>
      <Ports/>
   </Instance>
</Instances>
```

In this example, the line added for the DatabaseUrl element points to the database connection string str.oracle.com. This connection string must include the names of both instances of the Oracle Real Application Clusters database. It must also exist in the tnsnames.ora file as displayed in the following entry from the file:

```
STR.ORACLE.COM =
(DESCRIPTION =
 (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = store1.oracle.com)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = store2.oracle.com)(PORT = 1521))
    (LOAD_BALANCE = yes)
  )
 (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = str)
 )
 (FAILOVER_MODE=
    (TYPE=select)
    (METHOD=basic)
    (RETRIES=20)
    (DELAY=15)
  )
)
```

3.8.4 Verifying the Oracle Calendar Server and Oracle Files Domain Controller Installation

Before proceeding to install the Middle Tier components, you must verify whether Oracle Calendar Server and Oracle Files Domain Controller have been installed successfully. To do this:

1. Ensure that the environment is set properly by checking the values of variables such as ORACLE_HOME, PATH, LHOSTNAME, and LD_PRELOAD.
2. Run the following commands:

```
# Determine the status of the calendar server and nodes
$ORACLE_HOME/ocal/bin/unistatus
# Shut down all calendar server daemons and services.
$ORACLE_HOME/ocal/bin/unistop
# Start all calendar server daemons or services that are not already started.
$ORACLE_HOME/ocal/bin/unistart
```

3. Log in as root, set LD_PRELOAD because the original value will be lost, and then check files status:

```
LD_PRELOAD=libloghost.so.1; export LD_PRELOAD
$ORACLE_HOME/ifs/files/bin/ifsctl status -n
$ORACLE_HOME/ifs/files/bin/ifsctl [start|stop]
```

> **Note:** On HP-UX, use libloghost.sl instead of libloghost.so.1.

4. Check the $ORACLE_HOME/install/portlist.ini file, and note the port number for Oracle Calendar Server. This port number will be required later for the Oracle Calendar Server Middle Tier installation.

3.9 Installing and Configuring Oracle Collaboration Suite Middle Tiers

In the setup described in this document, the ocsmt1.oracle.com and ocsmt2.oracle.com hosts form the Middle Tiers. The load-balancer virtual server ocslb.oracle.com serves as the front end of these Middle Tiers.

This part of the deployment covers the installation of all the Oracle Collaboration Suite components, except Oracle Calendar Server and Domain Controller. These components have already been installed in a high-availability configuration.

This section discusses the following steps involved in installing and configuring the Middle Tiers:

- Section 3.9.1, "Installing the Middle Tiers"
- Section 3.9.2, "Verifying the Middle Tier Login"
- Section 3.9.3, "Configuring the Oracle Email Information Storage and Middle Tier"
- Section 3.9.4, "Configuring Oracle Files"

3.9.1 Installing the Middle Tiers

Perform the following steps on both the Middle Tier nodes, ocsmt1 and ocsmt2:

1. Verify the kernel configuration for the Middle Tiers.
2. Stop Sendmail if it is running.

Sendmail runs on port 25. Remove Sendmail from the system startup sequence for future system restarts.

3. Leave only a single instance of the Information Storage database running. Shut down all other Information Storage database instances.

   If there is more than one instance of the Information Storage database, then the Files Configuration Assistant, `ifsca,` will fail. This is because the assistant uses the JDBC thin driver.

4. Start the installer.
5. Deselect **Calendar Server**, and enter the Oracle Calendar Server host, **caldcha.oracle.com,** and port during the interview phase of the installation.
6. For Oracle Files, select only **Regular Node** and **HTTP Node.** Specify **`caldcha.oracle.com`** as the Oracle Files Domain Controller host.
7. For Oracle9*i*AS Single Sign-On, specify **`ssolb.oracle.com:80`** as the *`host:port.`*
8. For Oracle Internet Directory, specify **`infraha.oracle.com:4032`** as the *`host:port.`*
9. Enter **`store1.oracle.com:1521`** as the *`host:port`* for Information Storage and the `SID` or the `Service` that was created when the Information Storage was installed.

At the end of the installation, all the Middle Tier components are installed. Installing the second Middle Tier causes the portlet provider URLs in the portlet repository to be overwritten. When the two Middle Tiers are configured with a load balancer, these URLs will be changed to the load balancer URL.

The remaining topics of this section cover the steps related to Oracle Files and Oracle Email.

3.9.2 Verifying the Middle Tier Login

To verify the Middle Tier login:

1. Stop the Oracle Collaboration Suite Middle Tier and Oracle Files Domain Controller domain.

   To do this, first running the following command:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

   Then log in as `root,` and run the following command:

   ```
   $ORACLE_HOME/ifs/bin/ifsctl stop
   ```

2. Update the Oracle9*i*AS Single Sign-On server configuration table for `orasso` and `portal.` This involves the following steps:

   a. Get the `orasso` and `portal` passwords from Oracle Internet Directory by running the `ldapsearch` command.

      For the `portal` password, run the following `ldapsearch` command, which uses `portal` as the value of `orclResourceName:`

      ```
      ldapsearch -h host -p oid-port -D "cn=orcladmin" \
      -w oidpwd -b "cn=IAS Infrastructure Databases,\
      cn=IAS,cn=Products,cn=OracleContext" \
      -s sub "orclResourceName=portal" orclpasswordattribute
      ```

b. Log in to the Infrastructure database as the orasso and portal user, and update the WWSEC_ENABLER_CONFIG_INFO$ table by running the following commands:

```
SQL> UPDATE wwsec_enabler_config_info$
SET url_cookie_ip_check = 'N';
SQL> commit;
```

3. Log in to the Middle Tier URLs, and check sign on.

3.9.3 Configuring the Oracle Email Information Storage and Middle Tier

To configure Oracle Email Information Storage:

1. From the first Middle Tier, run the $ORACLE_HOME/oes/bin/umconfig.sh script to display the Unified Messaging Configuration screen.
2. Select the **Configure Mail Store** option in the installer.

   This will configure the mail schemas in the database. The database information must be provided in *host:port:sid* format. In this case, it is store1:1521:str.
3. Check the alert.log file on the mail store instance for any database errors. These would be mostly "Lack of database space" errors or "Out of rollback or temp space" errors. Fix these database errors, and rerun the umconfig.sh script.
4. After the database is populated with mail objects, rerun umconfig.sh on the first Middle Tier and select the **Configure the mail middle tier** option to configure the Oracle Email Middle Tier.
5. To configure e-mail, rerun the umconfig.sh script on the second Middle Tier. Because the database is already populated, the umconfig.sh script needs to be run only once on the second Middle Tier.

   The Middle Tier configuration will create a listener entry in the listener.ora file. By default this will be in the $ORACLE_HOME/network/admin/listener.ora file. This entry will be for a listener named LISTENER_ES to listen for mail protocols.
6. Start LISTENER_ES by running the following commands:

   ```
   id # Get the userid and group id of the Middle Tier user
   su # switch to root
   cd $ORACLE_HOME/bin
   tnslsnr LISTENER_ES -user userid -group group_id &
   ```

   In this command, userid and group_id are the values returned by the id command.
7. Check whether the listener is running and listening for all mail protocols by running the following command:

   ```
   lsnrctl status LISTENER_ES
   ```

8. Modify the database connection string ID in Oracle Internet Directory to enable Oracle Real Application Clusters access. To do this:

   a. Start the oidadmin tool on the Infrastructure host.

   b. Log in as orcladmin.

   c. Click **Entry Management,** click **cn=OracleContext,** and then click **cn=*dbname*.** Here, *dbname* is the name of the Information Storage database.

On the right side, the properties of this database are displayed.

d. One of the properties listed is the connection descriptor for the database, `orclnetdescstring`, which will have the following format:

```
(DESCRIPTION=(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCP)(HOST=store1.oracle.com)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=str)))
```

Change this to:

```
(DESCRIPTION=(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCP)(HOST=store1.oracle.com)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=store2.oracle.com)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=str)))
```

Note: In this example, `str` is the same as the `SERVICE_NAMES` database parameter of the store database. It is usually the same as `DB_NAME`.

Alternatively, you can use the `ldapmodify` command to modify this property.

See Also: For information about using the `ldapmodify` command to modify this property, refer to MetaLink note 257949.1

9. Install the Oracle Email libraries on the Information Storage database nodes.

   The following tasks need to be performed for each of the Information Storage database nodes:

   a. Copy the `$ORACLE_HOME/oes/umbackend.tar` file from the Middle Tier to a temporary directory on the Information Storage database nodes.

      If the Middle Tier and Information Storage servers are not running on the same operating system, then you must obtain the `umbackend.tar` file for your Information Storage servers.

   b. Extract the files from the `umbackend.tar` file.

   c. Run the `runInstaller` program, which is located in `Disk1` of the extracted directory tree.

      This will launch Oracle Universal Installer.

   d. Follow the installer prompts to install the libraries.

3.9.4 Configuring Oracle Files

Oracle Files is installed and set up after the completion of the Oracle Collaboration Suite Middle Tier installation. After the first Middle Tier is installed, perform the following steps to create the default subscriber:

1. Browse to the Administrator Login page, which is at

   `http://ocsmt1.oracle.com:7777/files/app/AdminLogin`

2. Log in by using the `SITE_ADMIN` account.
3. Click **New Subscriber** to create a new subscriber.
4. Select all the default settings for this subscriber.

5. Select a high value for the quota.
6. Specify that this subscriber can allocate more space.
7. Select the maximum number of users for this subscriber. For example, select **256** or **1024.**
8. Specify that the administrator can increase the maximum number of users.
9. Specify a value that is far off in the future as the end date for this subscriber.
10. Set Subscriber Administrator User ID to **filesadmin.**

> **Note:** Do not use an existing Oracle Internet Directory user. This administrator is specific to Oracle Files and does not need to log in. If you select an Oracle Internet Directory user as the Oracle Files administrator, then the synchronization process tries to create that user as a duplicate, because the user already exists in Oracle Files as an administrator.

11. Specify the e-mail address of the subscriber.
12. Specify that the status of the subscriber must be changed to `inactive` after 365 days.
13. Set the default user quota to **100 MB.**
14. Specify that this subscriber must always be prompted for a password.
15. Specify that you do *not* want to enable user control for password prompt.
16. Set Public Folder to **On.**
17. Enable user control of public folders.
18. Select your default display language.
19. Select your default document language.
20. Select your default document character set.
21. Select your default time zone.
22. Set your default workspace quota to **100MB.**
23. Set Public Folder to **On.**
24. Enable workspace administration control of public folders.
25. Review the information you have provided, and then submit it.

See Also: *Oracle Files Administrator's Guide*

Modify the `registry.xml` file for Oracle Files by following the instructions given in Section 3.8.3.

3.10 Setting Up a Load Balancer for the Oracle Collaboration Suite Middle Tiers

After installing the Middle Tiers, you need to set up the load balancer virtual server, `ocslb.oracle.com`, as the front end of the Middle Tiers. The HTTP Server and Web Cache components require reconfiguring for the load balancer. These are the access points for the Middle Tier components and the Oracle9*i* Application Server

Portal. This section details the steps required to reconfigure the HTTP Server and Oracle9*i*AS Portal for access through the load balancer.

As mentioned in the earlier section, each HTTP Server/`mod_osso` module is a partner application of Oracle9*i*AS Single Sign-On. When installing the two Middle Tiers, there is an HTTP Server installed on each Middle Tier, which is registered as a partner application with the Oracle9*i*AS Single Sign-On server. In addition, Oracle9*i*AS Portal on each Middle Tier is registered with the Oracle9*i*AS Single Sign-On server as a partner application.

Setting up a load balancer for the Oracle Collaboration Suite Middle Tiers involves the following steps:

- Section 3.10.1, "Validating the Partner Applications"
- Section 3.10.2, "Configuring HTTP Server and Web Cache to Use Load Balancer URL and Port 80"
- Section 3.10.3, "Reregistering the Two Middle Tiers with the Oracle9iAS Single Sign-On Using the Virtual Server of the Load Balancer"
- Section 3.10.4, "Obfuscating the osso.conf File"
- Section 3.10.5, "Reconfiguring Oracle9iAS Portal"
- Section 3.10.6, "Deleting Old Partner Applications"
- Section 3.10.7, "Updating the Oracle9iAS Single Sign-On Server Configuration Table"
- Section 3.10.8, "Changing Portlet URLs"
- Section 3.10.9, "Updating Portlet URLs"
- Section 3.10.10, "Restarting the Middle Tiers"

3.10.1 Validating the Partner Applications

Validate the partner applications by logging in to Oracle9*i*AS Single Sign-On administration pages as the Oracle9*i*AS Single Sign-On administrator. To do this:

1. Log in to

   `http://ssolb.oracle.com/pls/orasso`

2. Click **SSO Server Administration**.
3. Click **Administer Partner Applications**.

   On this page, in addition to the Oracle9*i*AS Single Sign-On server, HTTP Server on the Infrastructure, and the Oracle9*i*AS Single Sign-On Middle Tiers, the following partner applications should be listed:

   HTTP Server with `http://ocsmt1.oracle.com URL`
   HTTP Server with `http://ocsmt2.oracle.com URL`
   Portal with `http://ocsmt1.oracle.com URL`
   Portal with `http://ocsmt2.oracle.com URL`

3.10.2 Configuring HTTP Server and Web Cache to Use Load Balancer URL and Port 80

Make the following changes in the `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` file:

Original	Change To
Port 7777	Port 80
`ssomt1.oracle.com` `ssomt2.oracle.com`	`ocslb.oracle.com`
Listen 7778	Listen 80

3.10.3 Reregistering the Two Middle Tiers with the Oracle9*i*AS Single Sign-On Using the Virtual Server of the Load Balancer

Run the registration script to reregister the two Middle Tiers with Oracle9*i*AS Single Sign-On. The following is a sample registration script. Before you run this script from the first node, `ocsmt1.oracle.com,` substitute values appropriate to your installation.

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar \
-oracle_home_path /ocsmid/app/oracle/product/mid \
-host infraha.oracle.com \
-port 1521 \
-sid iasdb \
-site_name mid.ocslb.oracle.com \
-success_url http://ocslb.oracle.com:80/osso_login_success \
-logout_url http://ocslb.oracle.com:80/osso_logout_success \
-cancel_url http://ocslb.oracle.com:80 \
-home_url http://ocslb.oracle.com:80 \
-config_mod_osso TRUE \
-u root \
-sso_server_version v1.2
```

3.10.4 Obfuscating the osso.conf File

To obfuscate the `osso.conf` file:

1. Log in to Oracle9*i*AS Single Sign-On administration.

   Determine the values of the following parameters for the new partner application:

   ```
   sso_server_version
   cipher_key
   site_id
   site_token
   login_url
   logout_url
   cancel_url
   sso_timeout_cookie_name
   ```

2. Put these values in a clear-text file on the second Middle Tier, `ocsmt2.oracle.com.`

   The following is a sample clear-text file that can be used for `iasobf`:

   ```
   sso_server_version=v1.2
   cipher_key=A4051CF38030DF54
   site_id=1333
   site_token=2WI395111333
   login_url=http://ssolb.oracle.com/pls/orasso/orasso.wwsso_app_admin.ls_login
   logout_url=http://ocslb.oracle.com:80/osso_logout_success
   cancel_url=http://ocslb.oracle.com:80
   sso_timeout_cookie_name=SSO_ID_TIMEOUT
   ```

3. Obfuscate the `osso.conf` file on `ocsmt2` by running the following command:

   ```
   $ORACLE_HOME/Apache/Apache/bin/iasobf oss_clear.txt osso.conf root
   ```

   This will create the new `osso.conf` file on `ocsmt2`.

After you perform these steps, a new partner application for the HTTP Server is created with Oracle9*i*AS Single Sign-On and the two `mod_osso` modules are reconfigured.

3.10.5 Reconfiguring Oracle9*i*AS Portal

Oracle9*i*AS Portal is also registered as a partner application with Oracle9*i*AS Single Sign-On and needs to be reconfigured with the URL of the load balancer. The Web Cache invalidation specification is included in this reconfiguration. The Web Cache clustering must be completed for the reconfiguration to work correctly. You can ensure this by running the Oracle9*i*AS Portal Configuration Assistant, `opca.` Oracle9*i*AS Portal provides the `ptlasst.csh` file as a wrapper to `opca.` Run the following command from one of the Middle Tiers:

```
$ORACLE_HOME/assistants/opca/ptlasst.csh -mode SSOPARTNERCONFIG \
-i typical -sdad portal -host ocslb.oracle.com \
-port 80 -silent -verbose \
-chost ocslb.oracle.com -cport_i 4001 -cport_a 4000
```

3.10.6 Deleting Old Partner Applications

After the earlier steps, two new partner applications will be created with Oracle9*i*AS Single Sign-On, one each for the HTTP Server and Oracle9*i*AS Portal through the load balancer URL. To delete the old partner applications:

1. Log in to Oracle9*i*AS Single Sign-On at

   `http://ssolb.oracle.com/pls/orasso`

2. Click **SSO Server Administration.**
3. Click **Administer Partner Applications.**

   All the partner applications are listed on this page.

   There are four old entries for HTTP Server and Oracle9*i*AS Portal with the actual host names, `ocsmt1` and `ocsmt2`, that can be deleted.

4. Click the **Delete** icon for each old partner application.

3.10.7 Updating the Oracle9*i*AS Single Sign-On Server Configuration Table

Update the Oracle9*i*AS Single Sign-On server configuration table `WWSEC_ENABLER_CONFIG_INFO$` in `portal` and `orasso`, and set `URL_COOKIE_IP_CHECK` to **N.** This table stores configuration information that enables the application to identify the Oracle9*i*AS Single Sign-On server to which it must connect. To get the password for `portal,` use the `ldapsearch` command described in Section 3.4.3. On the Infrastructure host, run the following commands:

```
SQL> UPDATE wwsec_enabler_config_info$ SET url_cookie_ip_check='N'
SQL> commit;
```

3.10.8 Changing Portlet URLs

All the Oracle Collaboration Suite Middle Tier components appear as portlets when logged in to Oracle9*i*AS Portal. Each portlet has a portlet provider URL, which is used to render the portlet. The portlet provider URL is in the `portal` schema. It is the URL of the most recently installed Middle Tier. For example, if `ocsmt1.oracle.com` is the first installed Middle Tier, then the portlet provider URLs will be `ocsmt1.oracle.com.` However, when `ocsmt2.oracle.com` is installed, these URLs are overwritten by `ocsmt2.oracle.com.`

In the deployment example covered in this document, because a load balancer is used as a front end for the Middle Tiers, these URLs must be updated to the URL of the load balancer.

To change all the portlet URLs, edit the `webclient.properties` file on both the Middle Tiers and change all occurrences of the physical host name, `ocsmt1` or `ocsmt2,` to the load balancer URL, `ocslb.` In addition, because you changed the HTTP and Web Cache port to 80, you must change all occurrences of the default port to 80. The `webclient.properties` file is located at

```
$ORACLE_
HOME/webclient/classes/oracle/collabsuite/webclient/resources/we
bclient.properties
```

3.10.9 Updating Portlet URLs

After editing the webclient.properties file, rerun the Web Client Command Line Installer to update all the portlet URLs. To do this, run the following command:

```
$ORACLE_HOME/webclient/bin/webclient_installer.sh
```

3.10.10 Restarting the Middle Tiers

Restart all the Middle Tiers by using the start and stop scripts given in Appendix B.

3.11 Configuring Web Cache Clustering

To increase the availability and scalability of your Web site, you can configure multiple instances of Web Cache to run as members of a cache cluster. A cache cluster is a loosely coupled collection of Web Cache instances working together to provide a single logical cache.

Cache clusters provide failure detection and failover of caches. If a cache fails, then other members of the cache cluster detect the failure and take over ownership of the cached content of the failed cluster member. This increases the availability of your Web site.

By distributing the content of the Web site across multiple Web caches, more content can be cached and more client connections can be supported. This improves the scalability of your Web site.

> **See Also:** *Oracle9i*AS Web Conferencing Administration and Deployment Guide

3.12 Addressing Firewall Configuration Considerations

You may need to enable access to some ports on the firewall. The `$ORACLE_ HOME/install/portlist.ini` file contains a list of the default ports used on each node. Remember that because there is a portlist.ini file for each component, you must look for the portlist.ini file on each node.

> **See Also:** For a comprehensive list of default ports, refer to *Oracle9i* Application Server Administrator's Guide

If you are going to use Oracle Calendar Client, then you need to determine the Oracle Calendar Engine port setting, which is 5730 by default. This is mentioned in the ENG section of the $ORACLE_HOME/ocal/misc/unison.ini file.

The Oracle Files Domain Controller talks to the NodeGuardian and NodeManager ports. Similarly, NodeManager talks to the Oracle Files Domain Controller on the Oracle Files Domain Controller port, which is 53140 by default. You need to open all these ports between the DMZ and the intranet. You can find these port values in the $ORACLE_HOME/ifs/common/registry.xml file on the Middle Tiers in the DMZ and the Oracle Files Domain Controller server on the intranet. These port numbers are automatically generated, so they may be different for each deployment.

4

Applying the 9.0.4.2 Patch Set

This chapter supplements the instructions in the `readme` file for applying the 9.0.4.2 patch set. It contains the following sections:

- Section 4.1, "Downloading and Applying the 9.0.4.2 Patch Set"
- Section 4.2, "Configuring Oracle Web Conferencing Real-Time Collaboration After Applying the Patch Set"

4.1 Downloading and Applying the 9.0.4.2 Patch Set

You can download the 9.0.4.2 patch set from

`http://metalink.oracle.com/`

On the Patches Web page of this Web site, search for patch set number 3564610 for your platform.

The 9.0.4.2 patch set must be applied on each host in the Oracle Collaboration Suite environment. To apply this patch set:

1. Read the instructions in the `readme` file.
2. Back up all the tiers.
3. Ensure that the prerequisites mentioned in the `readme` file are met.

   These prerequisites include a recommendation to upgrade the Information Storage database to 9.2.0.5 by using the 3501955 patch.
4. Follow the instructions on creating the Oracle Web Conferencing Real-Time Collaboration volumes and tablespaces given in Appendix D. These raw volumes and tablespaces are required by the Information Storage database for Oracle Web Conferencing Real-Time Collaboration.

   > **Note:** If you have a clustered file system on which volumes need not be created manually, then you can skip this step. For example, Oracle Cluster File System on Linux is a clustered file system that does not require manual creation of volumes.
5. Apply the patch set to the Infrastructure node. Do not shut down the database before you perform this step.
6. Apply the patch set to the Information Storage database tier.
7. Install the 9.0.4.2 patch set on the Oracle Calendar Server and Oracle Files Domain Controller tier.

8. Install the patch set on all the Middle Tiers.
9. Follow the post-installation instructions given in the `readme` file.

4.2 Configuring Oracle Web Conferencing Real-Time Collaboration After Applying the Patch Set

To use an Oracle Real Application Clusters-enabled Information Storage, you must configure the Oracle Web Conferencing Real-Time Collaboration component after applying the patch set. To do this:

1. Shut down all Oracle Web Conferencing Real-Time Collaboration components on the current instance by running the following commands:

```
$ORACLE_HOME/imeeting/bin/imtctl stop
$ORACLE_HOME/dcm/bin/dcmctl stop -co OC4J_imeeting -v
```

2. Edit the `$ORACLE_HOME/imeeting/conf/imtinit.conf` file.

   In this file, specify the full JDBC connection string. The following are sample contents of the `imtinit.conf` file:

```
oracle.imt.database.sid=str1
oracle.imt.instancename=OUIHome.ocslb.oracle.com
oracle.imt.schema.password.encrypted=27250A0179786675780C0272534812
oracle.imt.database.hostname=store1.oracle.com
oracle.imt.database.port=1521
oracle.imt.schema.name=rtc_app
oracle.rtc.instance.version=2.0.4.3.0
```

Note: In the default configuration, connection information for the Oracle Web Conferencing Real-Time Collaboration database is specified in terms of the `hostname, port,` and `sid` properties. Oracle Web Conferencing Real-Time Collaboration 2.0.4.3 adds support for a new property called `oracle.imt.database.jdbc.connect.` When this property is present, the `hostname, port,` and `sid` properties are ignored even if they are present.

Add the following property in the `imtinit.conf` file:

```
oracle.imt.database.jdbc.connect=FULL_JDBC_CONNECT_STRING
```

Without any modification or validation, the value of `FULL_JDBC_CONNECT_STRING` will be used to establish connections to the Oracle Web Conferencing Real-Time Collaboration repository. This means that the value can be any valid JDBC 9.0.1.4 connection string. Unlike the entries in the `tnsnames.ora` file, the entire connection string must be specified on a single line in the `imtinit.conf` file.

The following is an example of the syntax you can use for specifying JDBC connection information. Substitute appropriate `HOST, PORT,` and `SERVICE_NAME` values in this syntax.

```
oracle.imt.database.jdbc.connect=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=store1.oracle.com)(PORT=1521)))(CONNECT_
DATA=(SERVICE_NAME=str.oracle.com)))
```

The following is sample JDBC connection information. Multiple listeners, each specified by its IP address, have been used in this example.

```
oracle.imt.database.jdbc.connect=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=store1.oracle.com)(PORT=1521))(ADDRESS=(PROTO
COL=TCP)(HOST=store2.oracle.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
NAME=str.oracle.com)))
```

The old database connection settings are usually ignored, but some commands may still expect these settings to exist for validation purposes. Therefore, do not change these connection settings.

3. Restart all Oracle Web Conferencing Real-Time Collaboration components on the current instance by running the following commands:

```
$ORACLE_HOME/imeeting/bin/imtctl start
$ORACLE_HOME/dcm/bin/dcmctl start -co OC4J_imeeting
```

4. Verify that the Oracle Web Conferencing Real-Time Collaboration components connected to the database are using the new connection string.

To do this on UNIX or Linux, first run the following command:

```
grep "Database Connection Info" \ $ORACLE_HOME/imeeting/logs/imtcontrol/*.xml
```

View the contents of the files returned by the command. The following are examples of entries that the older files must contain:

```
<record timestamp="2003-10-22T02:02:16.811-07:00" time-local="true"
severity="config" source-path="oracle.imt.application.db"
source="SrvDBConnProvider"><message>Database Connection Info:
jdbc:oracle:thin:@store1.oracle.com:1521:str1 (Schema rtc_app)</message>
```

The latest log file, which was created when you ran the `imtctl start` command, must contain an entry with the new JDBC syntax.

For example:

```
<record timestamp="2003-10-23T02:21:27.994-07:00" time-local="true"
severity="config" source-path="oracle.imt.application.db"
source="SrvDBConnProvider"><message>Database Connection Info:
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=store1.oracle.com)(PORT=1521))) (CONNECT_
DATA=(SERVICE_NAME=str.oracle.com))) (Schema rtc_app)</message>
```

Perform the same check on the `OC4J_imeeting` logs.

To do this on UNIX or Linux, run the following commands:

```
grep "Database Connection Info" \ $ORACLE_HOME/imeeting/logs/application/*.xml
```

If the new log files still contain the old connection string syntax, then recheck the previous steps to make sure that you specified the correct property, edited the correct file, and restarted all the Oracle Web Conferencing Real-Time Collaboration components. In addition, check your Oracle Web Conferencing Real-Time Collaboration version to ensure that you are using 2.0.4.3 or later. To do this, run the following command:

```
$ORACLE_HOME/imeeting/bin/imtctl versions
```

If the log files show that Oracle Web Conferencing Real-Time Collaboration is using the new connection string, then you have successfully completed all the steps.

5

Applying the 9.0.1.5 Patch Set

This chapter supplements the instructions in the readme file for applying the 9.0.1.5 patch set. It contains the following sections:

- Section 5.1, "Addressing the Requirements for Applying the Patch Set"
- Section 5.2, "Applying the Patch Set to the Infrastructure"
- Section 5.3, "Applying the Patch Set to the Other Tiers"

5.1 Addressing the Requirements for Applying the Patch Set

You can download the 9.0.1.5 patch set from

`http://metalink.oracle.com/`

On the Patches Web page of this Web site, search for patch set number 3301544 for your platform. The `readme` file for the patch set lists the steps required to apply the patch set to a database server. However, there are fixes in the patch set for the JDBC driver and other dependent components, like Oracle Call Interface and Oracle Net, which are required for some of the Oracle Real Application Clusters failover scenarios. Therefore, in a high-availability setup, this patch set needs to be applied on all the tiers, except the Information Storage database tier, which is already on Oracle9*i* Database release 9.2.

Before applying the patch set, shut down all the tiers. To do this, use the shutdown scripts listed in Appendix B.

5.2 Applying the Patch Set to the Infrastructure

To apply the 9.0.1.5 patch set to the Infrastructure:

1. Follow the instructions in the `readme` file of the patch set. Because the Infrastructure is on a cold failover cluster, if the `oraInventory` directory is not at a shared location, then run the installer from the node on which the `oraInventory` directory is located.

2. For the postinstallation steps, follow the instructions given in the `readme` file. Note the following exceptions to these instructions:

   a. Label security is not installed in the Infrastructure for Oracle Collaboration Suite. Therefore, skip the `make lbac_off` step given in the `readme` file.

   b. Skip Step 4 because the Infrastructure database is not Java enabled.

   c. Skip Step 5 because it is related to label security, which is not installed.

   d. Skip Step 6 because the Infrastructure database is not Java enabled.

e. Perform Step 7a, and skip Step 7b.

f. Skip Step 11 and Step 12

For instructions specific to the Linux platform, refer to MetaLink note 264056.1. Follow the instructions given in this note to replace the `$ORACLE_HOME/lib/libjmisc.so` file.

5.3 Applying the Patch Set to the Other Tiers

For applying the patch set to the Oracle9*i*AS Single Sign-On server and the Oracle Collaboration Suite Middle Tiers, copy the patch set from the Infrastructure node to the other nodes and run the installer on each one of them. Alternatively, download the patch set for the appropriate platform if the Infrastructure and Middle Tier platforms are different.

Before you start applying the patch set, shut down all the tiers. After applying the patch set to a tier, ensure that the tier processes are started before applying the patch set to the next tier.

After applying the patch set to the Infrastructure, to apply it to the other tiers:

1. Start the Infrastructure.
2. Apply the patch set to the Oracle9*i*AS Single Sign-On tiers.
3. Start the Oracle9*i*AS Single Sign-On tiers.
4. Start Information Storage.

> **Note:** The patch set need not be applied to the Information Storage tier. You only need to restart it before performing the next step.

5. Apply the patch set to the Oracle Calendar Server and Oracle Files Domain Controller.
6. Start Oracle Calendar Server and Oracle Files Domain Controller.
7. Apply the patch set to the Oracle Collaboration Suite Middle Tiers.
8. Start the Oracle Collaboration Suite Middle Tiers.

Before applying the patch set, ensure that the `oraInventory` directory exists on all the nodes. This directory is usually located at *`ORACLE_BASE`*`/oraInventory.` When you run the installer, it automatically detects and patches the appropriate components.

6

Applying the 3620912 Patch

This chapter provides instructions for applying the 3620912 patch.

This patch enables Oracle Web Conferencing Real-Time Collaboration to continue functioning normally as long as at least one Information Storage Oracle Real Application Clusters database instance is running. A prerequisite for applying this patch is to apply the 9.0.1.5 patch set, which is described in Chapter 5.

The 3620912 patch must be applied to the Middle Tier nodes. Before applying this patch, you must shut down the Middle Tier processes.

To apply this patch:

1. Read the `readme` file for this patch.
2. Ensure that the 9.0.1.5 patch set has been applied.
3. Stop all Middle Tier processes.
4. Apply the patch.
5. Edit the `$ORACLE_HOME/imeeting/conf/imtinit.conf` file.

   In this file, add the following line:

   ```
   oracle.imt.database.cleancache.connections=true
   ```

6. Restart the Middle Tier processes.

If you have multiple Middle Tiers, then this patch must be sequentially applied to each Middle Tier. By doing this, you can ensure that availability is not affected while the patch is being applied.

A

Acknowledgments

The authors wish to thank the following Oracle partners for their valuable contribution to the test environment used for developing this document:

- EMC Corporation
- F5 Networks, Inc.
- Sun Microsystems
- VERITAS Software Corporation

B

Component Startup and Shutdown Scripts

This appendix provides scripts for starting up and shutting down Oracle Collaboration Suite components. These scripts are specific to the Solaris operating system. You may need to modify these scripts before using them on other platforms.

This appendix contains the following sections:

B.1 Starting Up and Shutting Down Oracle Collaboration Suite Components

The order of startup of Oracle Collaboration Suite components is as follows:

1. Start the Infrastructure.
2. Start the Oracle9*i*AS Single Sign-On server and Oracle Delegated Administration Services.
3. Start the Information Storage listener and database.
4. Start the Oracle Calendar Server and Oracle Files Domain Controller.
5. Start the Middle Tier nodes.

To shut down the Oracle Collaboration Suite system, shut down the components in the reverse order of startup.

B.2 Setting Up Environment Variables

For each component, set up the appropriate environment variables, such as:

```
ORACLE_HOME
ORACLE_SID
PATH
```

```
LD_LIBRARY_PATH
SHLIB_PATH (on HP-UX only)
```

In addition, for the Infrastructure, Oracle Calendar Server, and Oracle Files Domain Controller, the following environment variables must be set:

```
LD_PRELOAD
LHOSTNAME
```

When you change shells, for example from a regular user to root, LD_PRELOAD is not exported to the child. Therefore, whenever you run the su command, set up the environment by sourcing the right file.

The examples in this appendix are based on the use of ksh.

B.3 Infrastructure Components

This section contains scripts for starting up and shutting down the Infrastructure components.

Note: The following script contains a password and must be protected.

Startup

```
#!/bin/ksh
# If this is the initial startup following a cold failover, then
# supply the parameter "failover" when running this script
# For example startup failover
typeset -i fover=0
export ORACLE_HOME=/ocsinfra/app/oracle/product/infra/904
hostname=`hostname`
[[ $1 == "failover" ]] && fover=1
lsnrctl start
sqlplus "/ as sysdba" << !
startup
!
oidmon start
oidctl server=oidldapd configset=0 instance=1 start
sleep 15
# These steps are dependent on the osso.conf file being saved to
# osso.conf.hostname following the initial reregistration
# These are only necessary following a failover
# If the osso.conf was not saved, then use the reregister script
# from the 9iAS Infrastructure Improved Availability document.
if (($fover ))
then
echo "Starting for the first time after failover..."
echo "Will reset iAS password and copy the right osso.conf file"
sleep 5
resetiASpasswd.sh "cn=orcladmin" welcome1 welcome1 $ORACLE_HOME
cp -p $ORACLE_HOME/Apache/Apache/conf/osso/osso.hostname \
$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
else
echo "No need to reset password and replace osso.conf file"
fi
$ORACLE_HOME/opmn/bin/opmnctl start
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

```
$ORACLE_HOME/opmn/bin/opmnctl startproc type=custom gid=dcm-daemon
$ORACLE_HOME/opmn/bin/opmnctl startproc type=oc4j gid=OC4J_DAS1
```

Shutdown

```
#!/bin/ksh
#
# Filename : stopall.sh
#
$ORACLE_HOME/opmn/bin/opmnctl stopall
oidctl server=oidldapd configset=0 instance=1 stop
sleep 15
# Increase this sleep if Oracle Internet Directory does not stop in 15 seconds
oidmon stop
sqlplus "/ as sysdba" <<!
shutdown immediate
!
lsnrctl stop
echo "Check if anything is running..."
ps -ef | grep -i ocsinfraSSO Server Middle Tiers
```

Startup

```
$ORACLE_HOME/opmn/bin/opmnctl start
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

Shutdown

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
$ORACLE_HOME/opmn/bin/opmnctl stopall
```

B.4 Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services Components

This section contains scripts for starting up and shutting down the Oracle9*i*AS Single Sign-On and Oracle Delegated Administration Services components.

Startup

```
#!/bin/ksh
$ORACLE_HOME/opmn/bin/opmnctl start
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

Shutdown

```
#!/bin/ksh
$ORACLE_HOME/opmn/bin/opmnctl stopall
```

B.5 Information Storage Oracle Real Application Clusters Instances

This section contains scripts for starting up and shutting down the Information Storage Oracle Real Application Clusters instances.

Startup

```
#!/bin/ksh
lsnrctl start
sqlplus "/ as sysdba" <<!
startup
!
```

Shutdown

```
#!/bin/ksh
sqlplus "/ as sysdba" <<!
shutdown immediate
!
lsnrctl stop
```

B.6 Oracle Calendar Server and Oracle Files Domain Controller

This section contains scripts for starting up and shutting down the Oracle Calendar Server and Oracle Files Domain Controller components.

The scripts given in this section must be run as `root`.

When you run the `ifsctl stop` command in the shutdown script, it shuts down all Oracle Files processes on all nodes, including the Middle Tiers. If you want the Middle Tier Oracle Files processes to keep running, then you must manually shut down the Oracle Files Domain Controller.

Note: The following script contains a password and must be protected.

Startup

```
#!/bin/ksh
#
# Filename : startall.sh
# Run this script as root with environment set
#
# If this is the initial startup following a cold failover, then
# supply the parameter "failover" when running this script
# For example, startup failover
typeset -i fover=0
[[ $1 == "failover" ]] && fover=1
su - calendar << !
. /home/calendar/calendar.env
if (($fover ))
then
echo "Starting for the first time after failover..."
echo "Will reset iAS password"
resetiASpasswd.sh "cn=orcladmin" welcome1 $ORACLE_HOME
fi
#
echo "Starting calendar server .."
$ORACLE_HOME/ocal/bin/unistart
!
LD_PRELOAD=libloghost.so.1;export LD_PRELOAD
$ORACLE_HOME/ifs/files/bin/ifsctl start << EOPASSWD
ifs
EOPASSWD
echo "Check if anything is running..."
ps -ef | grep -i calendar
```

Shutdown

```
#!/bin/ksh
#
# Filename : stopall.sh
# Run this script as root with environment set
```

```
#
su - calendar << !
echo "Stopping calendar server .."
$ORACLE_HOME/ocal/bin/unistop -y
!
LD_PRELOAD=libloghost.so.1;export LD_PRELOAD
# This will shut down all Oracle Files processes on all nodes
# To only stop the Oracle Files Domain Controller
# kill the Oracle Files Domain Controller process manually
$ORACLE_HOME/ifs/files/bin/ifsctl stop << EOPASSWD
ifs
EOPASSWD
echo "Check if anything is running..."
ps -ef | grep -i calendar
```

B.7 Oracle Collaboration Suite Middle Tiers

This section contains scripts for starting up and shutting down the Oracle Collaboration Suite Middle Tiers. These scripts must be run as `root`.

Startup

```
#!/bin/ksh
nohup $ORACLE_HOME/bin/tnslsnr LISTENER_ES -group gid -user uid &
$ORACLE_HOME/ifs/files/bin/ifsctl start <<EOPASSWD
<ifs schema password>
EOPASSWD
# gid and uid are the group id and user id of the owner of the Middle Tier
# software. In this example, ocsmid, and dba are the owner and group,
respectively.
su - ocsmid <<!
. /home/ocsmid/ocsmid.env
echo "Starting webcache .."
webcachectl start
echo "Starting opmn managed processes .."
$ORACLE_HOME/opmn/bin/opmnctl startall
echo "Starting em processes .."
oesctl startup ocsmt1.oracle.com:um_system:smtp_in
oesctl startup ocsmt1.oracle.com:um_system:smtp_out
oesctl startup ocsmt1.oracle.com:um_system:imap
oesctl startup ocsmt1.oracle.com:um_system:gc
oesctl startup ocsmt1.oracle.com:um_system:list
oesctl startup ocsmt1.oracle.com:um_system:pop
oesctl startup ocsmt1.oracle.com:um_system:nntp_in
oesctl startup ocsmt1.oracle.com:um_system:nntp_out
oesctl startup ocsmt1.oracle.com:um_system:vs
!
```

Shutdown

```
#!/bin/ksh
# This script is run as root. Will su to the Middle tier owner and shutdown the
# components
su - ocsmid << !
. /home/ocsmid/ocsmid.env
oesctl shutdown ocsmt1.oracle.com:um_system:smtp_in
oesctl shutdown ocsmt1.oracle.com:um_system:smtp_out
oesctl shutdown ocsmt1.oracle.com:um_system:imap
oesctl shutdown ocsmt1.oracle.com:um_system:gc
oesctl shutdown ocsmt1.oracle.com:um_system:list
oesctl shutdown ocsmt1.oracle.com:um_system:pop
oesctl shutdown ocsmt1.oracle.com:um_system:nntp_in
oesctl shutdown ocsmt1.oracle.com:um_system:nntp_out
oesctl shutdown ocsmt1.oracle.com:um_system:vs
echo "Starting webcache .."
webcachectl start
echo "Starting opmn managed processes .."
$ORACLE_HOME/opmn/bin/opmnctl stopall
lsnrctl stop LISTENER_ES
!
$ORACLE_HOME/ifs/files/bin/ifsctl stop <<EOPASSWD
<ifs schema password>
EOPASSWD
```

C

Backing Up Information Storage and Software

You must back up Information Storage and the software during installation and after completing the setup. This appendix provides instructions for performing these backups.

C.1 Information Storage Backup

Follow these steps to back up the database during the installation process. Backup performed during installation is termed as cold backup. Backup performed during normal operation, when the database is open, is different. The Information Storage database is not open, but it must be mounted for Oracle Database Recovery Manager backups.

To back up Information Storage:

1. Shut down the database, and then mount it.

   To do this, run the following commands:

   ```
   sqlplus "/ as sysdba"
   SQL> shutdown immediate;
   SQL> startup mount;
   SQL> quit
   ```

2. Create the `infobackup.rman` script file with the following contents:

   ```
   connect target
   configure controlfile autobackup on;
   configure controlfile autobackup format for device type disk to '/ocsstore_db_
   backup/%F';
   run {
   allocate channel bkp device type disk format '/ocsstore_db_backup/%U' ;
   backup database;
   release channel bkp;
   }
   ```

3. Run the `infobackup.rman` script by using the following command:

   ```
   rman infobackup.rman
   ```

C.2 Software Backups

Software backups must be taken after each major installation and configuration step for each tier. All the processes on a tier must be shut down before you perform the backup.

To back up software:

1. Log in as `root`.
2. Run the following command:

   ```
   cd ORACLE_BASE
   ```

3. Run the following command:

   ```
   tar -cvf backup_directory/step_name.tar *
   ```

   For example, to back up the Infrastructure following the Oracle Calendar Server and Domain Controller step, run the following command:

   ```
   tar -cvf /ocsinfra_backup/afterCalSrvr.tar *
   ```

D Creating Information Storage Tablespaces

This appendix provides information and scripts for creating Information Storage tablespaces. It contains the following sections:

- Section D.1, "Recommended Sizes of Information Storage Tablespaces"
- Section D.2, "Creating the Tablespaces Required for Applying the 9.0.4.2 Patch Set"

Note: In the environment described in this document, the Veritas volume manager is used to manage disk volumes. It is recommended that you use a clustered file system.

D.1 Recommended Sizes of Information Storage Tablespaces

The required size of Information Storage tablespaces depends on the number of users of your system.

The following table provides the recommended sizes of Information Storage tablespaces:

Creating a Raw Volume for...	File Size (MB)
`SYSTEM` tablespace	380
`server` parameter file	5
`USERS` tablespace	25
`TEMP` tablespace	40
`UNDOTBS` tablespace 1	250
`UNDOTBS` tablespace 2	250
`EXAMPLE` tablespace	160
`CWMLITE` tablespace	20
`XDB` tablespace	50
`ODM` tablespace	45
`INDX` tablespace	25
`TOOLS` tablespace	10
`DRSYS` tablespace	20
First control file	110
Second control file	110

Creating a Raw Volume for...	File Size (MB)
At least 2 redo log files for each instance	500
`srvcfg` (Voting disk for clusterware)	100
`RTC_BIG_DATA`	100
`RTC_DATA`	100
`RTC_INDEX`	100

See Also: For more information about sizing the database, refer to the Oracle Collaboration Suite documentation at

`http://www.oracle.com/technology/documentation/collab.html`

D.2 Creating the Tablespaces Required for Applying the 9.0.4.2 Patch Set

Run the following commands to create the tablespaces required for applying the 9.0.4.2 patch set.

Note: If you are going to use raw volumes, then you will have to create the raw volumes before running the following scripts.

```
CREATE TABLESPACE rtc_lookup_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_lookup_data' SIZE 16m REUSE;
CREATE TABLESPACE rtc_lookup_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_lookup_index' SIZE 8m REUSE;
CREATE TABLESPACE rtc_transaction_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transaction_data' SIZE 256m REUSE;
CREATE TABLESPACE rtc_transaction_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transaction_index' SIZE 64m REUSE;
CREATE TABLESPACE rtc_archive_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_archive_data' SIZE 64m REUSE;
CREATE TABLESPACE rtc_archive_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_archive_index' SIZE 16m REUSE;
CREATE TABLESPACE rtc_document_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_document_data' SIZE 64m REUSE;
CREATE TABLESPACE rtc_document_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_document_index' SIZE 8m REUSE;
CREATE TABLESPACE rtc_recording_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_recording_data' SIZE 64m REUSE;
CREATE TABLESPACE rtc_recording_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_recording_index' SIZE 8m REUSE;
CREATE TABLESPACE rtc_transient_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transient_data' SIZE 128m REUSE;
CREATE TABLESPACE rtc_transient_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transient_index' SIZE 500m REUSE;
CREATE TABLESPACE rtc_transient_lob_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transient_lob_data' SIZE 64m REUSE;
CREATE TABLESPACE rtc_transient_lob_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_transient_lob_index' SIZE 8m REUSE;
CREATE TABLESPACE rtc_report_data
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_report_data' SIZE 64m REUSE;
CREATE TABLESPACE rtc_report_index
DATAFILE '/dev/vx/rdsk/ocsstore-dg/rtc_report_index' SIZE 8m REUSE;
```

```
CREATE TEMPORARY TABLESPACE rtc_temp
tempfile '/dev/vx/rdsk/ocsstore-dg/rtc_temp' SIZE 128m REUSE;
```

E

Storage and Backup Planning Table

In this appendix, Table E–1 provides information that you can use to plan for meeting the storage and backup requirements of Oracle Collaboration Suite tiers.

Table E–1 Storage and Backup Requirements of Oracle Collaboration Suite Tiers

Host (Virtual Host)	User	Disk Group	Physical Disk	Volume	File System	Comment
infra1 (infraha)	ocsinfra	ocsinfra-dg	c2t0d0	ocsinfra_vol (8 GB)	/ocsinfra	Infrastructure software and database (Infrastructure will fail over to infra2)
				ocsinfra_vol_backup (16 GB)	/ocsinfra_backup	Backup of the Infrastructure software and database
infra2 (caldcha)	calendar	calendar-dg	c2t1d0	calendar_vol (8 GB)	/calendar	Oracle Calendar Server/Oracle Files Domain Controller software (will fail over to infra1)
				calendar_vol_backup (16gb)	/calendar_backup	Backup of the Oracle Calendar Server
store1	ocsstore ocsstore	ocsstore1-dg	c2t0d0	ocsstore1_vol	/ocsstore_sw	Information Storage software on Oracle Real Application Clusters node 1 (store1)
		ocsstore-dg (shared by store1 and store2 Oracle Real Application Clusters nodes)	c2t1d0	db vols	shared	Raw data file volumes (or data files on a supported Cluster File System)
		ocsstore_sw_backup1-dg	c2t2d0	ocsstore_sw_backup1_vol	/ocsstore_sw_backup1	Backup of Information Storage software on node 1

Table E–1 (Cont.) Storage and Backup Requirements of Oracle Collaboration Suite *Tiers*

Host (Virtual Host)	User	Disk Group	Physical Disk	Volume	File System	Comment
		ocsstore_db_backup-dg	c2t3d0	ocsstore_db_backup_vol	/ocsstore_db_backup	Backup of Information Storage database (only from one node, the Oracle Real Application Clusters database)
store2		ocsstore2-dg	c2t8d0	ocsstore2_vol	/ocsstore_sw	Information Storage software on Oracle Real Application Clusters node 2 (store2)
		ocsstore-dg (shared by store1 and store2 Oracle Real Application Clusters nodes)	c2t1d0	db vols	shared	Raw data file volumes (or data files on a supported cluster file system)
		ocsstore_sw_backup2-dg	c2t9d0	ocsstore_sw_backup2_vol	/ocsstore_sw_backup2	Backup of Information Storage software on node2
ocsmt1 (ocslb)	ocsmid	not applicable	/dev/dsk/c1t10d0s4	not applicable	/ocsmid	Oracle Collaboration Suite Middle Tier software, node1
			/dev/dsk/c1t10d0s5	not applicable	/ocsmid_backup	Backup of Oracle Collaboration Suite Middle Tier software on node1
ocsmt2 (ocslb)	ocsmid	not applicable	/dev/dsk/c2t3d0s4	not applicable	/ocsmid	Oracle Collaboration Suite Middle Tier software node2
			/dev/dsk/c2t3d0s5	not applicable	/ocsmid_backup	Backup of Oracle Collaboration Suite Middle Tier software on node2
ssomt1 (ssolb)	ssomid	not applicable	/dev/dsk/c1t9d0s4	not applicable	/ssomid	Oracle9*i*AS Single Sign-On Middle Tier software
			/dev/dsk/c0t0d0s5	not applicable	/private	Home directories
			/dev/dsk/c1t11d0s2	not applicable	/ssomid_backup	Oracle9*i*AS Single Sign-On software backup
ssomt2 (ssolb)	ssomid	not applicable	/dev/dsk/c1t10d0s4	not applicable	/ssomid	Oracle9*i*AS Single Sign-On Middle Tier software
			/dev/dsk/c0t0d0s5	not applicable	/private	Home directories
			/dev/dsk/c1t12d0s2	not applicable	/ssomid_backup	Oracle9*i*AS Single Sign-On software backup

F

Installation Checklist

In this appendix, Table F–1 provides a checklist that is based on the installation and configuration steps defined in this document. Use this checklist to ensure that you perform all the installation steps in the prescribed order.

Table F–1 Installation Checklist

Section	Installation Step	Status
3	Installing and Configuring for High Availability	
3.2	Implementing Preinstallation Recommendations	
3.2.1	Preparing Information to Be Specified During the Installation	
3.2.2	Planning for Storage Requirements	
3.2.3	Configuring System Kernel Parameters	
3.2.4	Configuring Information Storage and Raw Volumes	
3.3	Installing the Infrastructure in a Cold Failover Cluster	
3.4	Moving Oracle9iAS Single Sign-On and Oracle Delegated Administration Services to the DMZ	
3.4.1	Setting Up the HTTP Server	
3.4.2	Updating Distributed Configuration Management	
3.4.3	Setting Up Database Access for modplsql	
3.5	Configuring the Oracle9iAS Single Sign-On Server to Use a Load Balancer	
3.5.1	Modifying the Oracle9iAS Single Sign-On Server Settings of the Oracle9iAS Single Sign-On URL	
3.5.2	Reregistering Partner Applications	
3.6	Moving Oracle Delegated Administration Services to the Oracle9iAS Single Sign-On Middle Tier	
3.7	Installing and Configuring Information Storage to Use Oracle Real Application Clusters	
3.7.1	Creating the DBCA_RAW_CONFIG File	
3.7.2	Creating the Database with the Required Tablespaces	
3.7.3	Unlocking the Oracle Web Conferencing Real-Time Collaboration Schemas	
3.7.4	Creating Tablespaces That Are Not Created by the Database Configuration Assistant	
3.7.5	Setting the MAX_COMMIT_PROPAGATION_DELAY Parameter	
3.7.6	Copying Binary Files to Remote Nodes	
3.8	Installing and Configuring Oracle Calendar Server and Oracle Files Domain Controller	
3.8.1	Installing Oracle Calendar Server and Oracle Files Domain Controller	
3.8.2	Modifying the unison.ini File for Oracle Calendar Server	

Table F–1 (Cont.) Installation Checklist

Section	Installation Step	Status
3.8.3	Modifying the registry.xml File for Oracle Files Domain Controller	
3.8.4	Verifying the Oracle Calendar Server and Oracle Files Domain Controller Installation	
3.9	Installing and Configuring Oracle Collaboration Suite Middle Tiers	
3.9.1	Installing the Middle Tiers	
3.9.2	Verifying the Middle Tier Login	
3.9.3	Configuring the Oracle Email Information Storage and Middle Tier	
3.9.4	Configuring Oracle Files	
3.10	Setting Up a Load Balancer for the Oracle Collaboration Suite Middle Tiers	
3.10.1	Validating the Partner Applications	
3.10.2	Configuring HTTP Server and Web Cache to Use Load Balancer URL and Port 80	
3.10.3	Reregistering the Two Middle Tiers with the Oracle9iAS Single Sign-On Using the Virtual Server of the Load Balancer	
3.10.4	Obfuscating the osso.conf File	
3.10.5	Reconfiguring Oracle9iAS Portal	
3.10.6	Deleting Old Partner Applications	
3.10.7	Updating the Oracle9iAS Single Sign-On Server Configuration Table	
3.10.8	Changing Portlet URLs	
3.10.9	Updating Portlet URLs	
3.10.10	Restarting the Middle Tiers	
3.11	Configuring Web Cache Clustering	
3.12	Addressing Firewall Configuration Considerations	
4	Applying the 9.0.4.2 Patch Set	
4.1	Downloading and Applying the 9.0.4.2 Patch Set	
4.2	Configuring Oracle Web Conferencing Real-Time Collaboration After Applying the Patch Set	
5	Applying the 9.0.1.5 Patch Set	
5.1	Addressing the Requirements for Applying the Patch Set	
5.2	Applying the Patch Set to the Infrastructure	
5.3	Applying the Patch Set to the Other Tiers	
6	Applying the 3620912 Patch	

G

References

This appendix provides references to documents and MetaLink notes that contain information about Oracle Collaboration Suite high availability.

G.1 Documentation

- Oracle9*i* Application Server High Availability

  `http://www.oracle.com/technology/products/ias/hi_av/content9ias.html`

- Oracle Collaboration Suite Documentation

  `http://www.oracle.com/technology/documentation/collab.html`

- Oracle Application Server Documentation

  `http://www.oracle.com/technology/documentation/appserver10g.html`

- Oracle Collaboration Suite Architecture

  `http://www.oracle.com/technology/products/cs/html/cs_architecture.html`

- OTN Oracle Collaboration Suite Site

  `http://www.oracle.com/technology/products/cs/index.html`

- Oracle9*i* Application Server: Firewall and Load Balancer Architectures

  `http://www.oracle.com/technology/products/ias/pdf/firewallLoadbalancer.pdf`

- Configuring Highly Available Oracle9*i*AS Infrastructure with BIG_IP Load Balancer of F5

  `http://www.oracle.com/technology/technology/products/ias/hi_av/Oracle-BigIP.pdf`

G.2 MetaLink Notes

- **230168.1:** *Moving Oracle9i*AS Single Sign-On *Server to the Middle Tier*
- **215955.1:** *How to Create an Obfuscated* `osso.conf` *File*
- **243214.1:** *How to Install Collaboration Suite release 2 (9.0.4.X)*
- **250525.1:** *ALERT Free Space in LOB Tablespace not Reused when Using Auto Segment Space Management*

- **245366.1:** *Certification Matrix for Oracle iFS/CMSDK/Files*
- **259454.1:** *MAX_COMMIT_PROPAGATION_DELAY in a Oracle Real Application Clusters Environment*
- **257949.1:** *How to Change Store Database Registration in Oracle Internet Directory to Use a Connection Descriptor for Oracle Real Application Clusters*
- **228805.1:** *Using the resetIASpasswd Command*
- **255976.1:** Single Sign-On Accessibility Through a Firewall
- **263792.1:** *9.2.0.5 Patch Set - Known Issues*
- **263791.1:** *9.2.0.5 Patch Set - List of Bug Fixes by Problem Type*
- **281677.1:** *How To Verify The Oracle Real Application Clusters Instance Registration In Oracle Collaboration Suite OID*

Index