Oracle® Collaboration Suite

Deployment Guide

10*g* Release 1 (10.1.1)

B14479-02

October 2005

ORACLE®

Oracle Collaboration Suite Deployment Guide, 10*g* Release 1 (10.1.1)

B14479-02

Primary Authors: Charles Colt, Madhubala Mahabaleshwar, Neal Kaplan, David Wood

Contributors: Laureen Asato, Vinay Athma, Marla Azriel, Mario Bonin, M. Brown, Warren Briese, K Burridge, Marco Carrer, Chaddy Chaar, Will Chin, Tanya Correia, Jason Davis, K. deSmidt, C. G. Doherty, Ray Dutcher, Niel Evans, Natasha Fattedad, Joseph Garcia, Arun Gopalan, Meeta Gupta, Raj Gupta, Marc Houle, Soulaiman Htite, Duane Jenson, Rajesh Kadem, Valarie Kane, M. Kavanaugh, Richard Hall, Barbar Heninger, Tom Kraikit, Sandra Lee, Sunnia Lin, Tait McCarthy, Rami Musa, Jayashree Natarajan, Mark Paterson, Ricardo Rivera, Jean-Marc Robillard, Valarie Rosamond Moore, Sudip Roy, Pavi Sandhu, S. Sharma, P.V. Shivkumar, U. Srinivasan, Richard Strohm, R. Sunkara, Lyju Vadassery, Ramesh Vasudevan, Derek Wichmann, Adrian Yau

Contents

2 Planning for Oracle Collaboration Suite Deployment

3 Deploying Oracle Collaboration Suite

4 Interoperability with Other Oracle Products

Part II Application-Level Deployment

5 Deploying Oracle Calendar

6 Deploying Oracle Content Services

7 Deploying Oracle Discusssions

8 Deploying Oracle Mail

9 Deploying Oracle Mobile Collaboration

10 Deploying Oracle Real-Time Collaboration

11 Deploying Oracle Collaboration Suite Search

12 Deploying Oracle Voicemail & Fax

13 Deploying Oracle Workspaces

Index

List of Figures

Preface

This guide is your source for the deployment of Oracle Collaboration Suite.

Audience

This document describes deployment strategies for Oracle Collaboration Suite. This document is intended for administrators who are planning on deploying and installing Oracle Collaboration Suite. This document should be read after *Oracle Collaboration Suite Concepts 10g Release 1 (10.1.1)* and before *Oracle Collaboration Suite Pre-installation Requirements 10gRelease 1 (10.1.1)*.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

For more information, see these Oracle resources:

- *Oracle Collaboration Suite Concepts Guide*
- *Oracle Collaboration Suite Security Guide*
- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*
- *Oracle Collaboration Suite Installation Guide for Linux*
- *Oracle Collaboration Suite Installation Guide for hp-ux*

Many of the examples in this book use the sample schemas, which are installed by default when you select the Basic Installation option with an Oracle Database installation. Refer to *Oracle Database Sample Schemas* for information on how these schemas were created and how you can use them yourself.

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

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 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.

Convention	Meaning	Example
UPPERCASE monospace (fixed-width) font	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, Recovery Manager 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.
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executable programs, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names and connect identifiers, 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 start SQL*Plus. The password is specified in the orapwd file. Back up the datafiles 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 *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
[ ]	Anything enclosed in brackets is optional.	DECIMAL (*digits* [, *precision*])
{ }	Braces are used for grouping items.	{ENABLE | DISABLE}
|	A vertical bar represents a choice of two options.	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	Ellipsis points mean repetition in syntax descriptions. In addition, ellipsis points can mean an omission in code examples or text.	CREATE TABLE ... AS *subquery*; SELECT *col1*, *col2*, ... , *coln* FROM employees;
Other symbols	You must use symbols other than brackets ([ ]), braces ({ }), vertical bars (|), and ellipsis points (...) exactly as shown.	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	CONNECT SYSTEM/*system_password* DB_NAME = *database_name*

Convention	Meaning	Example

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. Because these terms are not case sensitive, you can use them in either UPPERCASE or lowercase.	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

lowercase	Lowercase typeface indicates user-defined programmatic elements, such as 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 Windows Operating Systems

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

Convention	Meaning	Example
Choose **Start** > *menu item*	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 filename 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>`
Special characters	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 HR/HR TABLES=emp QUERY=\"WHERE job='REP'\"`
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`

Convention	Meaning	Example
ORACLE_HOME and *ORACLE_BASE*	In releases prior to Oracle8*i* release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level *ORACLE_HOME* directory. The default for Windows NT was `C:\orant`. This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level *ORACLE_HOME* directory. There is a top level directory called *ORACLE_BASE* that by default is `C:\oracle\product\10.1.0`. If you install the latest Oracle release on a computer with no other Oracle software installed, then the default setting for the first Oracle home directory is `C:\oracle\product\10.1.0\db_`*n*, where *n* is the latest Oracle home number. The Oracle home directory is located directly under *ORACLE_BASE*. All directory path examples in this guide follow OFA conventions. Refer to *Oracle Database Installation Guide for Microsoft Windows (32-Bit)* for additional information about OFA compliances and for information about installing Oracle products in non-OFA compliant directories.	Go to the *ORACLE_BASE*`\`*ORACLE_HOME*`\rdbms\admin` directory.

Part I

Suite-Level Deployment

Part I provides information to help you understand Oracle Collaboration Suite deployment issues and available deployment options. Chapters include:

1

Understanding the Oracle Collaboration Suite Architecture

This chapter provides an overview of the Oracle Collaboration Suite architecture in the following topics:

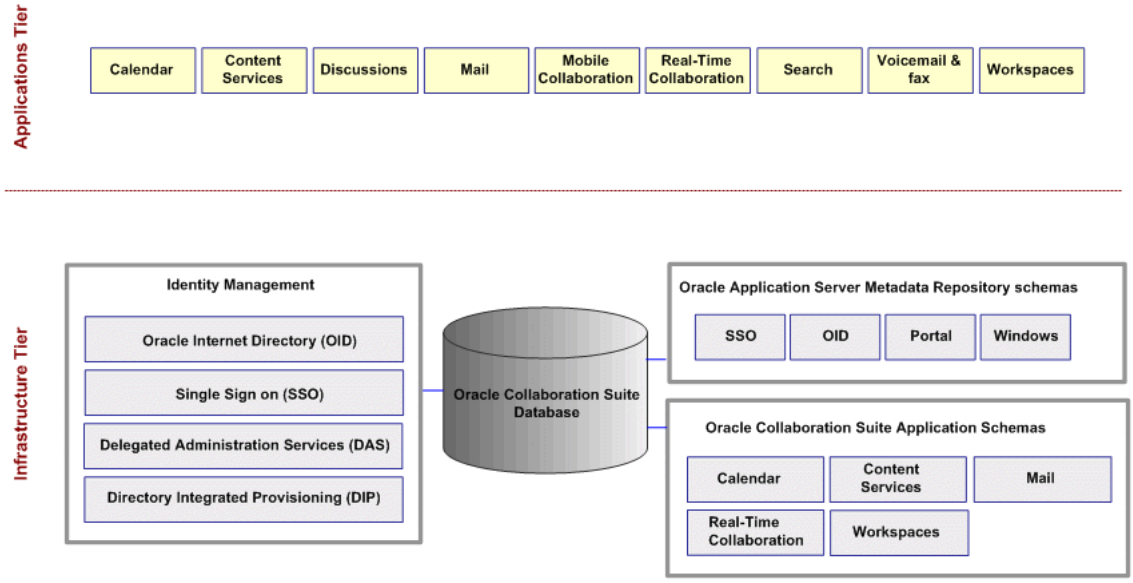
Introduction To Deploying Oracle Collaboration Suite

The *Oracle Collaboration Suite Deployment Guide* provides an understanding of the Oracle Collaboration Suite architecture, deployment planning issues, and deployment configuration examples. It also provides deployment information for individual Oracle Collaboration Suite applications. The information in this guide helps you to evaluate the network of your organization and architectural requirements based on considerations such as traffic size, reliability, scalability, and security and to optimally deploy Oracle Collaboration Suite. For this reason, Oracle encourages you to read this guide before installing and administering Oracle Collaboration Suite.

Oracle Collaboration Suite Architecture

The Oracle Collaboration Suite architecture is built on Oracle Collaboration Suite Infrastructure and Oracle Collaboration Suite Applications. Oracle Collaboration Suite Infrastructure is deployed on the Infrastructure tier and Oracle Collaboration Suite Applications is deployed on the Applications tier. The following figure provides an overview of the Oracle Collaboration Suite architecture:

Figure 1–1 Oracle Collaboration Suite Architecture



Note: You can deploy the Identity Management binaries and schemas on different homes if required.

Oracle Collaboration Suite Infrastructure Tier

The Infrastructure tier is the base tier for Oracle Collaboration Suite and consequently must be deployed before the Applications tier. The Infrastructure tier consists of the components that provide services, such as identity management and metadata storage, for the Applications tier. Components of the Infrastructure tier include Oracle Collaboration Suite Database and Oracle Internet Directory.

Identity Management

Oracle Collaboration Suite Identity Management components are as follows:

- Oracle Internet Directory (OID)
- Oracle Application Server Single Sign-On
- Delegated Administration Services (DAS)
- Directory Integrated Provisioning (DIP)

Oracle Collaboration Suite Database

The Oracle Collaboration Suite database is an Oracle10*g* Relational Database Management System (RDBMS) that serves as the repository for the Oracle Collaboration Suite component schema information and Oracle Application Server Release 10.1.2.0.2 metadata repository. When the RDBMS is installed, its default version is 10.1.0.5. It is also possible to create and then Oracle 10*g* Database and then install the Oracle Collaboration Suite component schema and Oracle Application

Server Metadata Repository in this database. The processes in this tier are the database instance processes and the database listener.

Oracle Internet Directory (OID)

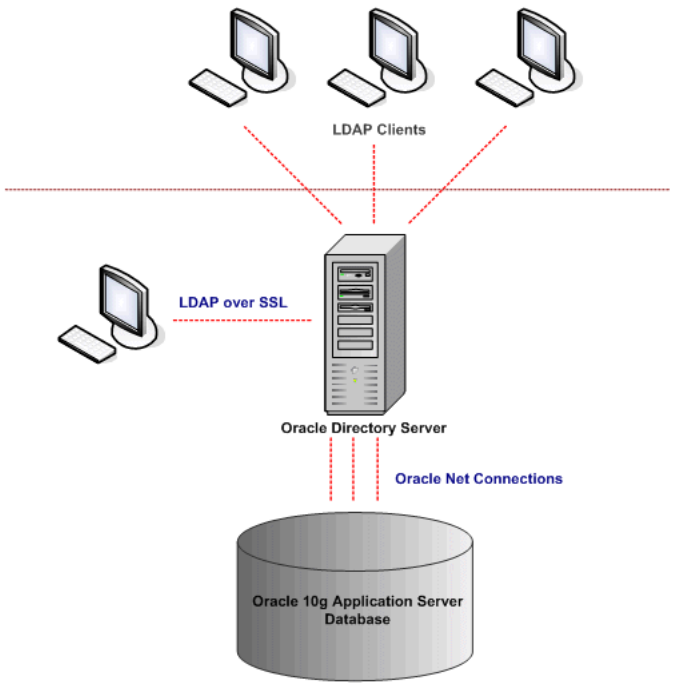
Oracle Internet Directory is a general-purpose directory service that stores security and management information for Oracle Application Server and Oracle Collaboration Suite instances, components, and Infrastructure. It provides authentication and a centralized user model, which enables the creation and management of users on an enterprise scale. It also enables fast retrieval and centralized management of information about dispersed users and network resources.

Oracle Internet Directory is a combination of Lightweight Directory Access Protocol Version 3 (LDAP v3) and Oracle 10*g* Database technology. As a result, it offers the extensibility and lightweight quality of LDAP v3 along with the high performance, security, scalability, robustness, and availability features of Oracle 10*g* Database.

Oracle Internet Directory Architecture

Oracle Internet Directory runs as an application on the Oracle Database 10*g*, which may not be on the same operating system. Oracle Internet Directory communicates with the database by using Oracle Net Services, an operating system-independent database connectivity solution offered by Oracle.

Figure 1–2 Oracle Internet Directory Architecture



Oracle Internet Directory Components

Oracle Internet Directory comprises of the following components:

- Oracle directory server, which responds to client requests for information about people and resources, by using a multiple-tiered architecture, directly over TCP/IP.

- Oracle directory replication server, which replicates LDAP data on Oracle directory servers.
- Directory administration tools are as follows:
  - Oracle Directory Manager, which simplifies directory administration through a Java-based graphical user interface.
  - A variety of command-line administration and data management tools that can be called by LDAP clients.
  - Directory server management tools within Oracle Enterprise Manager Application Server Control. These tools enable you to:
    * Monitor real-time events and statistics by using a browser.
    * Collate statistical data in a new repository.
  - Oracle Internet Directory Software Developer Kit (SDK).

Oracle Internet Directory Benefits

Oracle Internet Directory provides scalability, high availability, security, and tight integration with the Oracle environment. These benefits are described in the following sections:

- Scalability
- High Availability
- Security
- Integration with the Oracle Environment

Scalability

Oracle Internet Directory utilizes the Oracle 10*g* database to support large amounts of directory information. Oracle Internet Directory uses shared LDAP servers and database connection pooling to support thousands of concurrent clients in subsequent search response times.

Oracle Internet Directory also provides data management tools, such as Oracle Directory Manager, and a variety of command-line tools to manipulate large volumes of LDAP data.

High Availability

Oracle Internet Directory also takes advantage of the High Availability features of the Oracle 10*g* Database. The directory information, which is stored securely in the Oracle 10*g* Database, uses the backup capabilities of the Database. Additionally, the Oracle 10*g* Database that supports large datastores, heavy loads and RAC. It can recover from system failures quickly.

Security

Oracle Internet Directory offers secure and flexible access control. An administrator can grant or restrict access to a specific directory object or to an entire list of subdirectories. Moreover, Oracle Internet Directory implements three levels of user authentication: anonymous, password-based, and certificate-based, using Secure Socket Layer (SSL) Version 3 for authenticated access and data privacy.

Integration with the Oracle Environment

By using the Oracle Directory Integration and Provisioning platform, Oracle Internet Directory provides a single point of integration between the following:

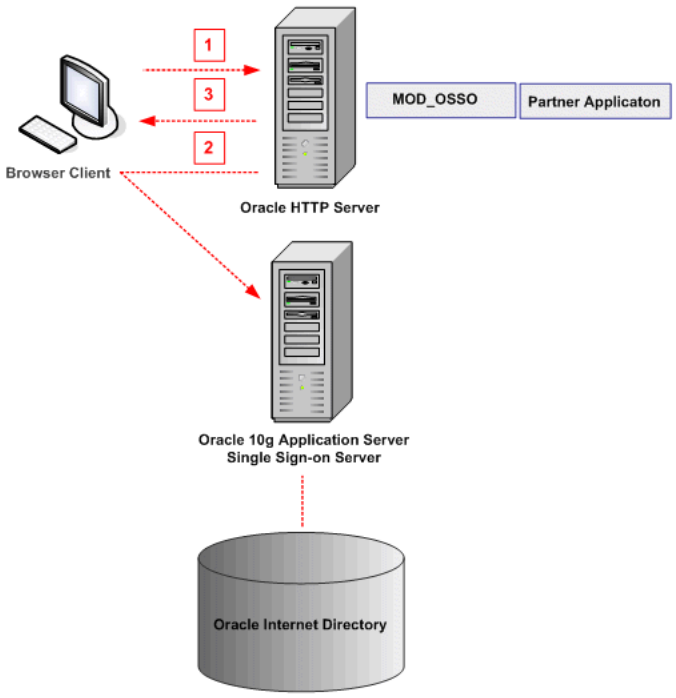
- Oracle environment and other directories, such as Network Operating System (NOS) directories
- Third party enterprise directories
- Application-specific user repositories

Oracle Application Server Single Sign-On

Oracle Application Server Single Sign-On (OracleAS Single Sign-On) enables you to use a single user name and password to access all features, applications, and accounts of Oracle Collaboration Suite as well as other Web applications. By using the OracleAS Single Sign-On feature, you can access all Web applications for which you are authorized, without having to reenter a user name and password for each application.

OracleAS Single Sign-On retrieves user information from Oracle Internet Directory.

Figure 1–3 Role of OracleAS Single Sign-On During User Authentication



OracleAS Single Sign-On Components

- Oracle Application Server Single Sign-On server: The OracleAS Single Sign-On server works with Oracle Application Server Database, Oracle HTTP Server, and OC4J server and enables you to log on securely to applications.
- Partner applications: A partner application is responsible for determining whether a user authenticated by Oracle Application Server Single Sign-On has the required application privileges. Examples of partner applications include Oracle Application Server Portal, Oracle Application Server Discoverer, and the OracleAS Single Sign-On server itself.

- External applications: External applications do not delegate authentication to the OracleAS Single Sign-On server. Instead, they display HTML login forms that ask for application user names and passwords. Each external application may require a unique user name and password. Yahoo Mail is an example of an external application that uses HTML login forms.
- `mod_osso`: This is an Oracle HTTP Server module that provides authentication to Oracle Application Server applications. It is an alternative to the OracleAS Single Sign-On SDK, used in earlier releases of OracleAS Single Sign-On to integrate partner applications. Located on the application server, `mod_osso` simplifies the authentication process by serving as the sole partner application to the OracleAS Single Sign-On server. In this way, `mod_osso` renders authentication transparent to Oracle Application Server applications. Also, the administrator for these applications is spared the burden of integrating them with the SDK.

In addition to the preceding components, Oracle Application Server Single Sign-On interacts with the following components for successful authentication of user credentials:

- Oracle Internet Directory: This is the repository for all OracleAS Single Sign-On user accounts and passwords, administrative and non administrative. The OracleAS Single Sign-On server authenticates users against their entry in the directory. At the same time, it retrieves user attributes from the directory that enable applications to validate the user.
- Oracle Identity Management Infrastructure: Oracle Application Server Single Sign-On is just one link in an integrated infrastructure that also includes Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, and Oracle Application Server Certificate Authority. Together, these components, called the Oracle Identity Management Infrastructure, manage the security life cycle of users and other network entities in an efficient, cost-effective way.

Delegated Administration Services (DAS)

For information about Delegated Administration Services (DAS), see "Identity Management Components" in Chapter 2 of *Oracle Collaboration Suite Concepts Guide* .

Directory Integrated Provisioning (DIP)

For information about Directory Integrated Provisioning (DIP), see "Identity Management Components" in Chapter 2 of *Oracle Collaboration Suite Concepts Guide* .

Application Server Metadata

- Oracle Internet Directory
- OracleAS Single Sign-On
- Portal
- Windows

Oracle Collaboration Suite Application Schemas

- Calendar
- Content Services
- Mail
- Real-Time Collaboration

- Workspaces

Oracle Collaboration Suite Applications Tier

The Applications tier relies on the Infrastructure tier and includes the following applications:

- Oracle Calendar
- Oracle Content Services
- Oracle Discusssions
- Oracle Mail
- Oracle Mobile Collaboration
- Oracle Real-Time Collaboration
- Oracle Collaboration Suite Search
- Oracle Voicemail & Fax
- Oracle Workspaces

Users can access these services using a variety of access methods including the Web, fax, voice, or phones and PDAs over wireless networks.

Services and Protocols

The Applications tier provides the following services and protocols:

- **E-mail protocols**
  - **Simple Mail Transfer Protocol (SMTP)**. This protocol is used for transmitting e-mail across the Internet.
  - **Post Office Protocol, version 3 (POP3)**. This protocol is used for the retrieval of e-mails. When you use POP3, all e-mail messages are downloaded onto your computer from the server and subsequently can also be accessed offline. Once the e-mail messages are downloaded, they can only be accessed from the computer on which they are stored.
  - **Internet Message Access Protocol, version 4 (IMAP4)**. This protocol is used to access e-mails from the mail server. By using IMAP, you can retrieve e-mails and also you can manipulate e-mails on the server itself. Because the e-mails are on the server, they can be accessed from any computer.
- **File protocols**
  - **File Transfer Protocol (FTP)**. This protocol is used for transferring files from one computer to another. FTP is the most widely used protocol for uploading or downloading files to and from the Internet.
  - **FTP Over SSL (FTPS)**. In addition to FTP, FTPS is supported. You can access Oracle Content Services using either implicit or explicit FTPS. Because FTPS does not send unencrypted passwords over the network, an FTP password is not necessary.
  - **Hyptertext Transfer Protocol (HTTP)**. The Hypertext Transfer Protocol, is used for Web browser-based access.
  - **Web-based Distributed Authoring and Versioning (WebDAV)**. This protocol It is a set of extensions to Hypertext Transfer Protocol (HTTP), which defines a

standard for all the authoring operations, such as editing and managing the files, on a remote server.

- **Web protocols**
  - **Hypertext Transfer Protocol (HTTP)**. This protocol defines a set of rules for exchanging files across the Internet.
  - **HTTP-Secure (HTTPS)**. HTTPS is the HTTP protocol implemented over Secure Sockets layer (SSL) or Transport Layer Security (TLS).
- **E-mail services, including Webmail/HTTP**. Webmail is an application that enables users to access e-mail messages from any Web browser.
- **File services, including Oracle Files/HTTP**. Oracle Content Services is designed as an enterprise file server replacement, with added content management features that enable users to collaborate more efficiently
- **Calendar services**
  - **SyncML/HTTP**. SyncML is the standard language that is used to enable synchronization of remote data and personal information between various devices and networks.
  - **Oracle Calendar Access Protocol (OCAP)**. OCAP is the access protocol through which Oracle Calendar Application System (OCAS) sessions communicate with the Oracle Calendar server (OCAL) and through which desktop clients communicate with OCAL. OCAP connections must be fixed, persistent, and cannot be load balanced.
- **Wireless services, including Wireless/HTTP**. By using wireless services, employees can access their e-mail and voicemail, manage their appointments, lookup into corporate directory, browse and fax shared online files from any mobile device with browser, through speech from any telephone, or instantly by SMS.
- **Portal services, including Oracle10*g*** Application Server Portal**/HTTP**. Oracle10*g* Application Server Portal enables companies to quickly build, administer, and deploy enterprise portals that are standards-driven, scalable, secure and dynamic.
- **Oracle Collaboration Suite Search services, including Oracle UltraSearch and Oracle Collaboration Suite Content Search**. Oracle Collaboration Suite Search Search offers a highly-configurable, all-in-one search solution across Oracle Mail, Oracle Calendar, and Oracle Content Services. Oracle Collaboration Suite Search can also search across HMTL pages that are accessible by Oracle UltraSearch. Oracle UltraSearch enables users to search a variety of content, including text and multimedia across heterogeneous sources. Ultra Search includes a web interface, web crawling and search administration facilities, as well as a programmable Java API, to provide a unified interface for enterprise and vertical portal search applications.
- **Web Cache**. Web Cache monitors requests from a client and stores information that it retrieves from the server. On subsequent requests for the same information, the Web cache delivers the content from its memory rather than passing on the request to the server. So, it improves the access time and efficiency and reduces the overall traffic.

Deployment Configurations

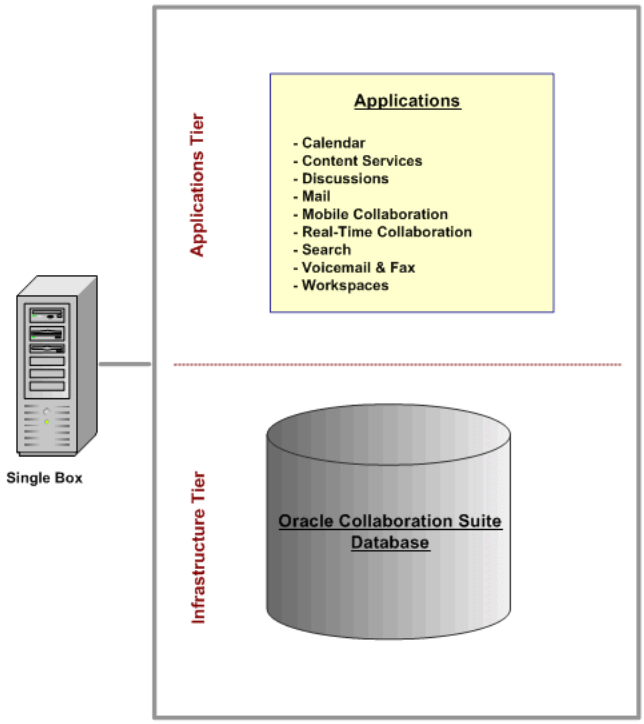
This section provides an overview of the different types of Oracle Collaboration Suite deployment configurations. Subsequent chapters provide more detailed guidelines for

deploying should always begin by configuring the Infrastructure tier. Once this process is complete, you can then configure the required applications on one or more Applications tiers.

Single-computer Deployment

The single-computer deployment is the simplest Oracle Collaboration Suite deployment configuration. It is generally used by small organizations, or for testing and demonstration purposes, or pilot programs. Single-computer deployments may be cost effective for small organizations, however they provide no allowance for high availability since all components are stored on the same machine. Figure 1-3 illustrates the Oracle Collaboration Suite single box deployment.

Figure 1–4 Single-Computer Deployment



In this figure, the Infrastructure tier and Applications tier components are all stored on the same computer. The Oracle 10*g* Database contains all of the Infrastructure tier components and acts as the mail server and file server. It also stores the identity management components including Oracle Internet Directory, Oracle Application Server Single Sign-On, and Delegated Administration Services. Applications include Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, Oracle Mobile Collaboration, Oracle Real-Time Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces.

Infrastructure Tier and Applications Tier on Separate Computers

The Infrastructure tier and Applications tier can be deployed on separate computers. This provides greater ease for maintenance and scalability but still places the infrastructure and applications components in a single point of failure. Figure 1–5

illustrates the Infrastructure tier and Applications tier deployed on separate computers.

Figure 1–5 Deployment with Infrastructure tier and Application Tier on Separate computers

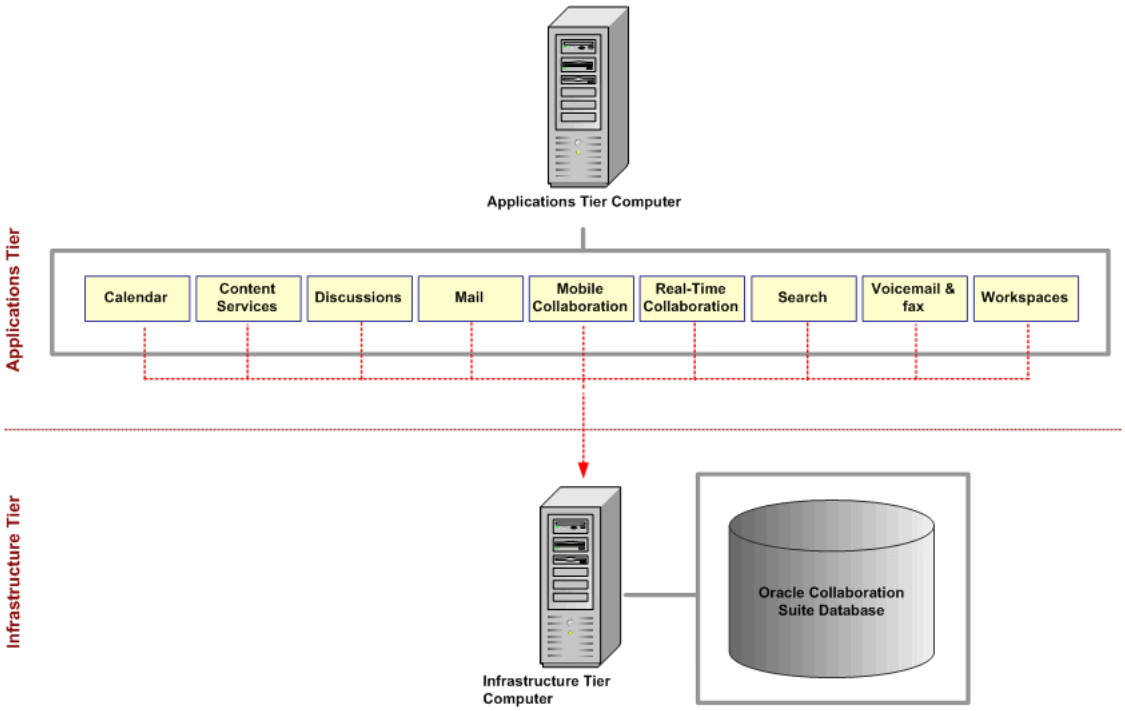


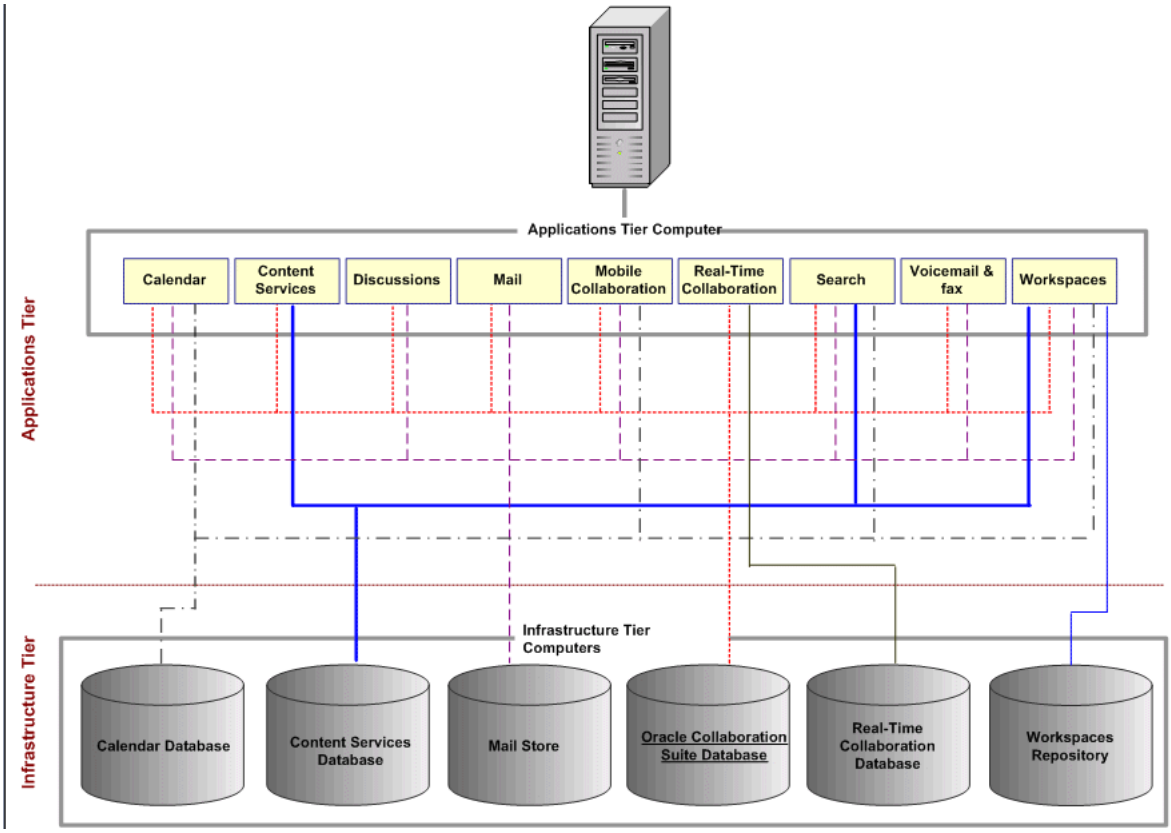
Figure 1–5 illustrates the Infrastructure tier and Applications tier deployed on separate computers. The Infrastructure tier is on one computer that contains the Oracle Collaboration Suite database with Infrastructure tier components including the Oracle Collaboration Suite schemas, Identity Management binaries, and Oracle Application Server Metadata schemas.

The Applications tier is on another computer that contains Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, Oracle Mobile Collaboration, Oracle Real-Time Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces.

Multiple Infrastructure Tier Computers

You can deploy the Infrastructure tier over several computers in which applications such as Oracle Calendar, Oracle Content Services, Oracle Mail, Oracle Real-Time Collaboration, and Oracle Workspaces have their own dedicated database. This configuration improves performance and simplifies maintenance and administration. In this configuration, at least one computer must include the Oracle Collaboration Suite Database.

Figure 1–6 Deployment with Multiple Infrastructure Tier Computers



The preceding figure illustrates the Applications tier deployed on one computer and the Infrastructure tier deployed across six computers. In this figure, the Calendar database, Content Services database, Mail store, Oracle Collaboration Suite database with Infrastructure tier components, Real-Time Collaboration database, and Workspaces repository are each deployed on an individual computer on the Infrastructure tier.

All applications on the Applications tier run on the same computer and each communicates with the relevant repository on the Infrastructure tier and with the Oracle Collaboration Suite database accordingly:

- **Calendar database**. Oracle Calendar, Oracle Mobile Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces access the Calendar database.
- **Content Services database**. Oracle Content Services, Oracle Collaboration Suite Search, and Oracle Workspaces access the Content Services database.
- **Mail Store**. Oracle Calendar, Oracle Discusssions, Oracle Mail, Oracle Mobile Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces access the Mail store.
- **Oracle Collaboration Suite database**. All applications access the Oracle Collaboration Suite Database.
- **Real-Time Collaboration repository**. Oracle Real-Time Collaboration accesses the Real-Time Collaboration repository.
- **Workspaces repository**. Oracle Workspaces access the Workspaces repository

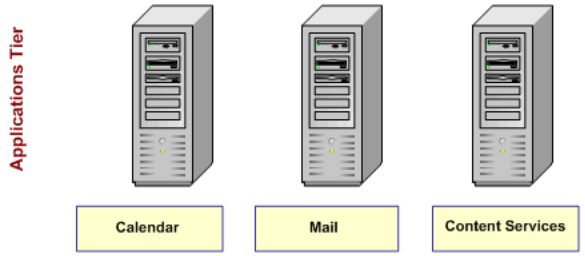
Multiple Applications Tier Computers

You can deploy Oracle Collaboration Suite across multiple Applications tier computers using one of the options described in this section.

Dedicated Applications Tiers Deployment

In a dedicated Applications tiers deployment, individual Oracle Collaboration Suite applications are each deployed on a dedicated computer.

Figure 1–7 Dedicated Application Tiers Deployment

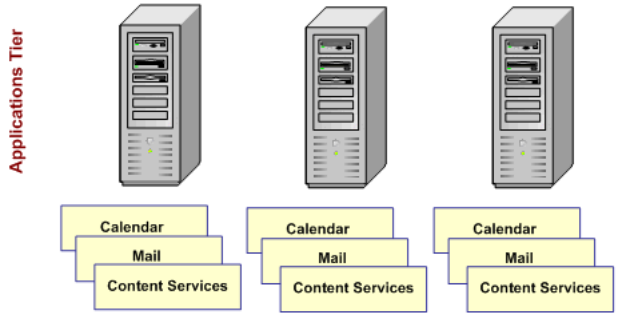


The dedicated Applications tiers deployment provides greater flexibility for tuning specific server functions and it enables you to scale by component. This is the preferred configuration if you wish to implement components in a phased approach, and if your organization's budget permits a more resource-intensive deployment.

Duplicated Application Tiers

In a duplicated Applications tiers deployment, all Oracle Collaboration Suite applications are deployed together on a single machine that is duplicated as many times as required.

Figure 1–8 Duplicated Applications Tiers Deployment



The duplicated Applications tiers deployment simplifies Applications tier management by providing a uniform process for managing each computer. This deployment configuration also makes better use of Applications tier resources since all Applications tier computers can respond to the change in application demand that occurs throughout the day. For example, peak e-mail usage generally takes place at the

start of the day while peak file usage is distributed throughout the latter parts of the day.

Multiple Infrastructure Tier and Multiple Application Tier computers

You can deploy both the Infrastructure tier and Applications tier across multiple computers. In addition to improving performance, ease of maintenance and administration, it also reduces the possibility that a single failure will take down all of Oracle Collaboration Suite. With this configuration, a failure on either tier may take down an application while the rest of Oracle Collaboration Suite remains operational. This should not be confused, however, with a high availability solution.

Figure 1–9 Deployment with Multiple Infrastructure Tier and Multiple Application Tier Computers

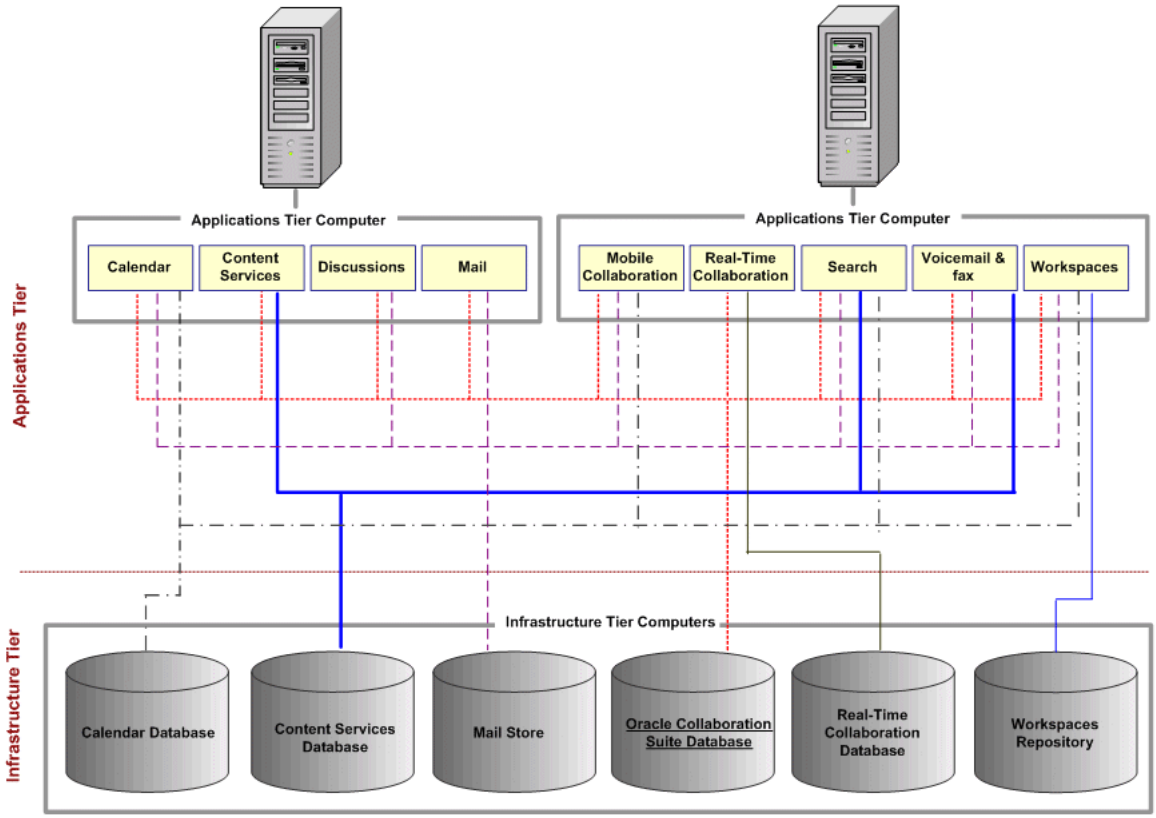


Figure 1–9 illustrates the Applications tier deployed on two computers and the Infrastructure tier deployed across six computers. In this figure, Oracle Calendar, Oracle Content Services, Oracle Discusssions, and Oracle Mail run on one Applications tier computer while Oracle Mobile Collaboration, Oracle Real-Time Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces run on another Applications tier computer. The Calendar database, Content Services database, Mail store, Oracle Collaboration Suite database, Real-Time Collaboration database, and Workspaces repository are each deployed on an individual computer on the Infrastructure tier.

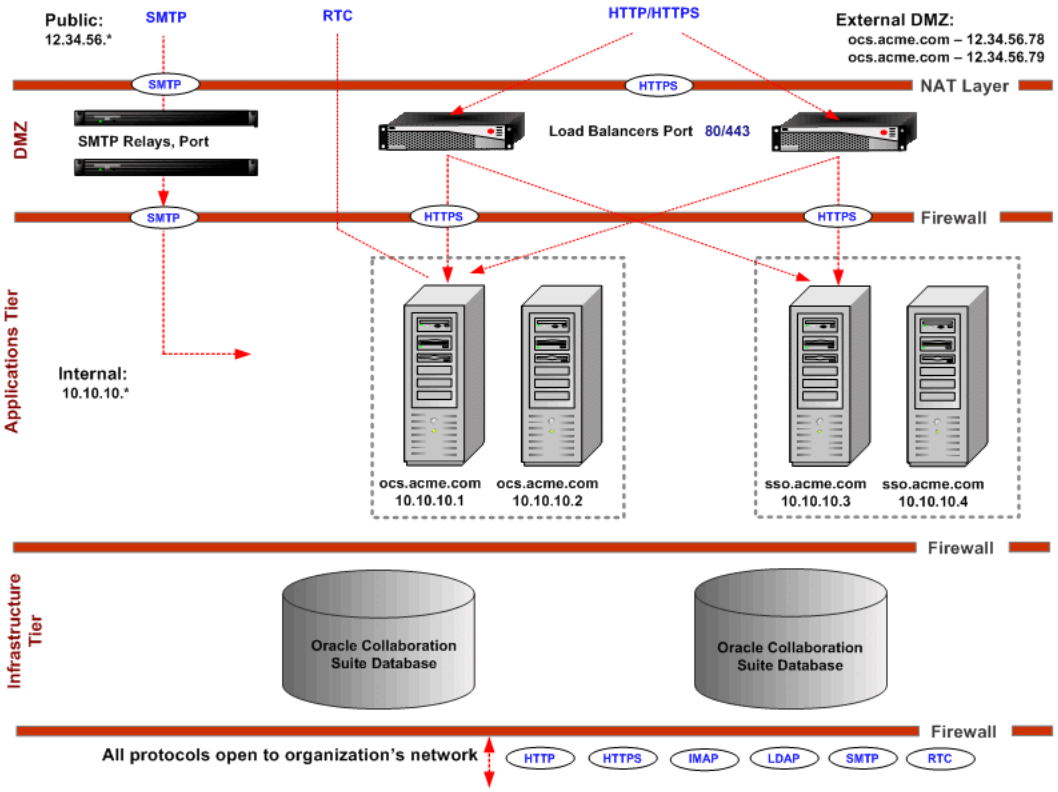
All applications on the Applications tier communicate with the relevant repository on the Infrastructure tier and with the Oracle Collaboration Suite database accordingly:

- **Calendar database**. Oracle Calendar, Oracle Mobile Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces access the Calendar database.
- **Content Services database**. Oracle Content Services, Oracle Collaboration Suite Search, and Oracle Workspaces access the Content Services database.
- **Mail Store**. Oracle Calendar, Oracle Discusssions, Oracle Mail, Oracle Mobile Collaboration, Oracle Collaboration Suite Search, and Oracle Workspaces access the Mail store.
- **Oracle Collaboration Suite database with Infrastructure tier components**. All applications access the Oracle Collaboration Suite Database for identity management and metadata repository services.
- **Real-Time Collaboration repository**. Oracle Real-Time Collaboration accesses the Real-Time Collaboration repository.
- **Workspaces repository**. Oracle Workspaces access the Workspaces repository

High Availability

The availability of a system or any component in that system is defined by the percentage of time that it works normally. For example, a system that works normally for twelve hours each day is 50% available. A system that has 99% availability is down 3.65 days each year on average. Critical systems may need to meet exceptionally high availability standards, and experience as little as four to five minutes of downtime each year. There are different strategies such as clustering for making a system highly available. Figure 1–10 provides an example of a high availability deployment for Oracle Collaboration Suite hardware components.

Figure 1–10 High Availability Deployment Example



In this example two tiers including network services servers are all duplicated. Load balancers are used to distribute HTTP and HTTPS traffic. NAT is used to tunnel Web Conferencing to the Applications tier. Network services run on servers residing in the DMZ, including the Postfix mail relay on port 25 and Apache 2.0 Reverse Proxy on ports 80 (HTTP) and 443 (HTTPS). Though it is not shown, a BIND DNS server runs on port 53.

The use of a second, internal, DNS server enables internal users to connect directly to the internal servers. External users connect to the Oracle Collaboration Suite domain on routable 12.x.x.x IP addresses, and are served content by the proxy server, which communicates with Oracle Collaboration Suite through a firewall.

The interior network provides open access for its users, while the exterior network (the Internet) will have access to HTTPS, SMTP and Web Conferencing traffic. Web Conferencing and Files traffic are still being determined, and require appropriate increases in bandwidth where necessary.

For a user base of 1,000 to 1,500 users, four moderately sized servers, each with two CPUs, can be used. For larger user bases, increase sizing as needed. For instance, for 4,000 users, servers with four to eight CPUs and large amounts of RAM are recommended.

Clients may reside on the internal network or on a separate neighboring network, which could theoretically be in a separate physical location.

2

Planning for Oracle Collaboration Suite Deployment

Oracle Collaboration Suite Deployment Planning Overview

Once you understand the Oracle Collaboration Suite architecture, the next step is to plan your deployment. This process involves two basic issues, network and architectural configuration. Because network configuration varies according to the unique requirements of each organization, this chapter does not provide specific network setup instructions. Instead it discusses the basic network issues that organizations must address when deploying Oracle Collaboration Suite. This chapter also provides a comprehensive discussion of the architectural issues and available configurations that organizations must consider when deploying Oracle Collaboration Suite.

Oracle Collaboration Suite Network Planning

This section discusses network planning issues in the following topics:

Basic Considerations

The basic goal of network planning is to make optimal use of Oracle Collaboration Suite and your existing network services and components. To accomplish this, you must determine a number of issues including the amount of access permitted for external sources, the capacity needed to meet user requirements, and network availability. You must also consider business issues such as budget constraints and the strategic reasons behind each of your network planning goals. How much flexibility do you have to change your network and are you able to update business processes if necessary?

Smaller Deployments

In smaller deployments of Oracle Collaboration Suite, network and architectural planning are intertwined since smaller pools of available servers result in fewer deployment options. When planning an architecture with only one or two servers, you will often have to choose between component accessibility and server location. The location of servers is often based on security requirements and as a result, access to the severs must be planned accordingly.

Access and Security

When deploying Oracle Collaboration Suite, access and security must be planned simultaneously, since each issue has a direct impact on the other, especially with smaller deployments.

Access is arguably the more complex of these two issues. In virtually any deployment, you must account for a number of access methods (or levels) within a single environment. These depend on factors such as the location from which the user accesses the network, whether the user does so with a thick or thin client, and the component to which the user attempts to gain access.

Because access is network-dependent element, much of its setup depends on the surrounding network environment. Therefore, Domain Name Services (DNS), mail relays, reverse proxies, firewalls, network routing and other such network services must interact very closely with the components of Oracle Collaboration Suite. Understanding this interaction is the key to understanding Oracle Collaboration Suite network access in a production environment.

Security is a subset of access in many ways, as many security issues are solved simply by denying access to certain services or networks; for instance, by denying access to Internet Message Access Protocol (IMAP) from the outside world. The other element to consider is how to secure the traffic you do allow to flow, and this is where encryption plays an important role. This is especially true for external traffic.

Another critical, and often overlooked, element of security is the planning and management of administration accounts on your servers. Due to the number of administrative accounts—which provide both management flexibility and manageability—there is also the potential for a large number of passwords, and administrators are tempted to use the same password for all accounts. This is a bad idea for obvious reasons. Planning and managing the use of different passwords for different accounts improves security for your Oracle Collaboration Suite installation.

Separation of Traffic

A typical installation of Oracle Collaboration Suite may separate traffic in two ways.

Internal Traffic

Internally, all protocols are allowed and all clients may be used. This can be modified to be more granular, either by configuring access rules in the services themselves, or by separating the networks with firewalls.

Typical clients used include Oracle Connector for Outlook, Mozilla Thunderbird, Oracle Real-Time Collaboration, the Oracle Calendar server Web client, Oracle Files and the Oracle Calendar desktop clients.

External Traffic

Externally, only a few encrypted, hardened and monitored services are exposed. Hyper Text Transfer Protocol Secure (HTTPS) and Simple Mail Transfer Protocol (SMTP) are the only services typically available from the outside world

HTTPS is the HTTP protocol implemented over Secure Sockets layer (SSL) or Transport Layer Security (TLS). It provides better security than HTTP by providing authentication and data encryption. Users generally access Oracle Collaboration Suite from outside using Web based applications over HTTPS. So you can proxy HTTPS as each user requirements.

SMTP is used for the transmission of e-mails across the Internet. So you can proxy SMTP through a mail relay.

Deployment Planning Issues for a New Network

This section summarizes the issues to consider when evaluating an installation site. You should investigate these issues, then keep them in mind when reading through the detailed questions at the end of this chapter.

To meet your organization's required access options, start by asking the following questions.

- **Which Oracle Collaboration Suite components and network services will be used?**

  Choose the components of Oracle Collaboration Suite that you need, and consider which network services are necessary. For example, if you install the Mail component, you may want it to be accessible from anywhere in the world through HTTPS. Generally, the three most important Oracle Collaboration Suite network services are routing equipment, DNS and mail relay. The three most important Oracle Collaboration Suite network services are:

  - **Routing Equipment**. Routing equipment can include routers, load balancers, and firewalls.
  - **Domain Name System (DNS)**. This network service resolves domain names or host names into IP addresses. DNS maintains a database of all the host names and their respective IP address information for all the domains.
  - **Mail relay**. This network service is a server that routes e-mails to their destinations, mostly within local networks.

- **From where should these be accessible?**

  For example, if Oracle Calendar is installed, will it be accessible externally as well as internally?

- **Do your plans fit into your organization's security model?**

  Before creating an elaborate deployment plan for Oracle Collaboration Suite, make sure you know your organization's security model, if there is one. For instance, some organizations may not allow DMZ's or external access to e-mail.

- **What are the existing network services you are going to be relying on?**

  It may be practical to make use of existing network services.

- **What's the configurability of these services? Can they be changed easily to suit Oracle Collaboration Suite?**

  Check how flexible your existing network implementation is.

- **What is the size of the current network, if there is one?**

Find out what sort of upgrades and additions, if any, will have to be made to the network to accommodate Oracle Collaboration Suite.

- **How many users will there be?**

  This is a primary concern in determining the type of deployment you need. See Chapter 3, "Deploying Oracle Collaboration Suite"for more information.

- **What is your budget?**

  Cost is obviously always an important consideration in any network installation.

Answers to the preceding questions will greatly help you to evaluate:

- Which Oracle Collaboration Suite and network components need to be deployed
- How many servers they will be deployed across
- Where they will need to be deployed
- How they will need to be configured

Deployment Planning Issues for an Existing Network

This section provides the following detailed questions you should ask about an existing network before deploying Oracle Collaboration Suite.

- What kind of network/security policies does your organization have?
- Does your organization have a DMZ, and if so, what kind?
- Does your organization use (Network Address Translation) NAT to abstract its network?
- What is your organization's existing DNS strategy?
- Has your organization implemented load balancing and reverse proxy?
- Does your organization use hardware encryption acceleration?
- Does your organization have an SMTP mail relay?
- Does your organization want to expose IMAP to the rest of the world?
- Is filtering installed for spam and viruses?
- Will your organization want Oracle Real-Time Collaboration to be available through the Internet?
- What services might your organization want to deploy initially or later?

What kind of network/security policies does your organization have?

Any existing policies will have to be adhered to when installing Oracle Collaboration Suite (unless your organization is willing to re-create its policies on short notice). This is likely to affect:

- What services can be used
- Where services can be exposed; that is, internally or externally.
- Whether SSL is required to protect services. SSL is a security standard that transmits data in an encrypted and authenticated form over a network. If the services have to be protected with SSL, then it is a good idea to get SSL certificates early on in the process.

Does your organization have a DMZ, and if so, what kind?

This is crucial to the design and planning of your architecture, as it determines where components need to be placed, depending on how they are to be accessed. DMZ is a part of the network, which is in between an intranet and the Internet, and is often referred as the neutral zone. It enables only certain services of the hosts in an intranet to be accessible to the hosts on the Internet. This sub network is specially used for public access servers such as web servers.

If there is a DMZ:

- How is it used for external access?
- How is it used for internal access?
- Are DNS servers used? If so, consider the following issues.
  - Sometimes, two DNS servers (split DNS) are used, to help separate deployments reserve server names for separate internal only, and external computers.
  - DNS servers can be separated onto separate networks; for example, one in the DMZ and one in the internal network.
  - You can configure any DNS, such as Berkeley Internet Name Domain (BIND), which you use to respond to DNS requests differently, depending on where the request originates.
  - You can configure BIND (or whatever DNS server you are using) to respond to DNS requests differently, depending on where the request is originating.
  - DNS services can be further fortified when combined with Network Address Translation (NAT).

  Two DNS servers provides more flexibility than just one. In either case, clients would connect to either an external or internal IP address for the same host name, depending on where the connection originates, and client access would be properly routed by DNS connectivity.

> **Note:** For more information, see "What is your organization's existing DNS strategy?" later in this chapter.

Does your organization use (Network Address Translation) NAT to abstract its network?

NAT is the process of translation of an IP address used within one network to a different IP address of another network. Generally, organizations set up NAT to translate internal addresses into public routable addresses. The translation takes place at the firewall and protects internal addresses from external tracing or routing.

NAT has a large and beneficial impact on naming services. External IP addresses in DNS can be mapped to virtual addresses as configured in Collaboration Suite.

> **Note:** When you install a application tier, it absorbs the name of the server on which it is installed. You must configure external IPs on your DNS server, then configure Oracle Collaboration Suite to use the appropriate virtual addresses instead of the original server name.

What is your organization's existing DNS strategy?

Your organization's existing DNS strategy is crucial to planning the access options for your Oracle Collaboration Suite installation. Together with NAT, DNS regulates how protocols are routed from users to the Oracle Collaboration Suite installation. There are two basic DNS strategies to consider:

Single DNS

Configuring a single DNS instance is more difficult. Requests for OracleAS Single Sign-On have to resolve both internally and externally.

Although configuring single DNS for a small company is less complex, it is not the most secure configuration, and in fact can expose crucial information about your network if not done properly.

Has your organization implemented load balancing and reverse proxy?

Load balancing is the process of managing the distribution of inbound traffic among multiple servers. The use of load balancers and reverse proxy is an important strategy in securing your Oracle Collaboration Suite installation. With load balancing and reverse proxy, you can abstract the routing and addressing of HTTP/HTTPS traffic so that Oracle Collaboration Suite servers are not directly exposed to external users.

If your organization uses existing hardware and a switching strategy, try evaluating whether or not Oracle Collaboration Suite can be integrated into this.

The use of content switches as load balancers is recommended. Content switches can host virtual IP addresses and spread the load over multiple servers, particularly for application tier services. Traffic can be redirected based on protocols such as HTTP, HTTPS, SMTP and so on.

If your organization currently has host names for its current services running on virtual devices, then migration will be much, much easier. In fact, it is always a good idea to identify virtual services names early in the process. Embed them in documentation and get SSL certificates early if they are needed. It is also a good idea to start setting up DNS and Mail eXchange (MX) records (to map domain names to mail servers) early.

Does your organization use hardware encryption acceleration?

If you are planning on using SSL protocol to encrypt communications, it is a good idea to make use of SSL accelerators to optimize performance. SSL processing is a CPU-intensive task that can reduce performance. This is best off-loaded to hardware devices designed for this purpose.

You should consider using SSL to encrypt external access to Oracle Collaboration Suite.

Does your organization have an SMTP mail relay?

Relay services are important for filtering, limiting and routing SMTP traffic. They can be used to protect Oracle Collaboration Suite instances from external abuse and unnecessary load.

Most organizations have an existing SMTP mail relay (or Mail Transport Agent), ideally with spam services implemented on it. Take note of what kind of limitations the relay has, such as:

- Attachment size
- Throughput throttling
- Retry count

Evaluate whether or not these limitations are still realistic for your organization, and keep them in mind as you start to deploy Oracle Collaboration Suite.

It is a good strategy for many deployments to use programs such as these to handle and filter e-mail before forwarding it to the Oracle Collaboration Suite mail relay, which can reside behind a firewall or in a DMZ.

Does your organization want to expose IMAP to the rest of the world?

IMAP is used to access e-mails from the mail server. By using IMAP, you can not only retrieve e-mails but you can also manipulate the e-mails on the server itself. Many organizations will choose not to provide IMAP access directly over the internet, as they would feel overly exposed from a security standpoint. If you decide to provide IMAP access across the Internet (without the additional security of a VPN infrastructure, for instance), Oracle Corporation strongly recommends implementing SSL for those IMAP services.

Is filtering installed for spam and viruses?

For the judicious use of valuable database storage, avoid saving unnecessary information such as e-mail spam. To protect the integrity of the network, viruses (often linked directly to spam) must also be blocked. There are a number of methods of filtering out these unwanted communications.

Will your organization want Oracle Real-Time Collaboration to be available through the Internet?

The best way to make Oracle Real-Time Collaboration available externally is to install it on its own server in a DMZ. This enables direct connections from the outside world for consoles, while reducing the load on small instances by dedicating Oracle Real-Time Collaboration, a relatively high-load service, to its own box.

If Oracle Real-Time Collaboration cannot be installed on its own server, the Oracle Real-Time Collaboration server must still be available directly to clients, and not put behind a proxy server, for example (although NAT is supported). Oracle Real-Time Collaboration clients first attempt to connect directly to the Oracle Real-Time Collaboration servers, and then attempt to connect directly to the Oracle HTTP Server or Web cache.

What services might your organization want to deploy initially or later?

It is possible that in the process of deploying Oracle Collaboration Suite, your organization may want to either implement services for the first time (such as a load balancer, for example), or upgrade existing services (such as a mail relay).

Oracle Collaboration Suite Architecture Planning

Oracle Collaboration Suite can work in many different permutations, with exact placement and integration of components and servers varying greatly. Configuration depends on the needs of the organization and the existing architecture that can be leveraged.

The choice of architecture has a definite impact on performance and stability. Some organizations may require high availability, and may have moved to Oracle Collaboration Suite for this purpose. Others may not need high availability throughout an architecture, and can save money because of it. For example, implementing high availability just for some components and not for other components may save some money.

Access

Access to Oracle Collaboration Suite is determined by your network setup and security strategies. Part of your planning involves determining where components need to be accessed from, be it internally, externally or both.

You can run multiple application tier servers, depending on where your users are, perhaps with one in a DMZ and one on the internal network, and both requiring access to OracleAS Single Sign-On. More often though, one set of application tiers is deployed, with separation and access provided using NAT and DNS. This is usually due to a limited number of servers or a high availability setup.

Capacity

To provide the appropriate capacity for the number of users in your deployment, you must start by evaluating how many servers you will need. You should keep in mind not just the sheer number of users, but also the frequency and concurrency of use.

Another strategy to consider when planning capacity is the separation of tiers. Each tier uses resources in its own way, so installing them on separate servers can be beneficial. With this strategy, you can tune and grow your tiers granularly.

Finally, make sure you use appropriate hardware platforms. You can choose from several operating systems (such as Solaris, Linux, or Windows), and architectures (two or more CPUs, 32-bit or 64-bit), depending on the requirements of your organization and your existing environment. It is possible to run both heterogeneous and homogeneous platforms.

application tier systems have a shared nothing architecture, and therefore are more suitable for smaller and cheaper hardware, such as single or dual CPU. Database server systems are typically larger, multiple CPU computers with larger memory requirements.

Properly deployed application tier systems can serve as backups to each other. This style of duplicated application tiers provides flexibility of deployment and enables the load to be spread across all the application tier systems as it swings from, for example, e-mail traffic to Oracle Content Services access over the course of the day.

Recovery Strategies

Make sure you plan for the ability to restore deleted or corrupt data to its last known good state. This is a part of your backup strategy.

Availability Strategies

Availability encompasses strategies you put into place to keep things running in the case of system failures. Strategies can range from performing basic backups in-house to maintaining high-levels of redundancy for the Oracle Collaboration Suite system components. One example is making sure you have network redundancy, so that in the event that one of your network paths fails, then network traffic can be routed along a secondary or backup network route.

When deciding which components are most in need of redundancy, imagine a situation in which the whole network fails, and think about what service or component is most business critical. Make sure you put in place an efficient availability architecture plan for those components that will meet your businesses service levels. The availability strategy of the OCS system components should be driven by the service availability requirements of your business.

Scalability

With any deployment, it is important to plan for growth. You must be prepared to expand your deployment along with the size or needs of your user base. The use of virtual host names is recommended, even if you are installing on a single tier or in a non high availability environment. This will allow you to abstract services across multiple servers later on, without having to rename servers.

Make sure you have hardware that enables for growth and memory expansion. See the "Capacity" section for more information.

Workload and Security

You can deploy components and services of Oracle Collaboration Suite on a single computer. However, such a deployment architecture may not be able to meet all the availability, security, and scalability requirements of your organization. Distribution of the tiers on multiple computers makes it easier to meet these requirements.

To optimize resource utilization on a particular computer, you should not mix different types of workloads on the computer. Typically, architectures for relatively large systems feature the distribution of these tiers on different computers.

The two Oracle Collaboration Suite tiers handle different types of workloads. The Applications tier is CPU-intensive and memory-intensive with fewer disk I/O operations. The infrastructure and Infrastructure tier is disk I/O intensive.

In Oracle Collaboration Suite, the demand for application tier resources increases at a rate that is different from the rate at which the demand for infrastructure and information storage resources increases. This is another factor that justifies a distributed architecture. With a distributed architecture, you can scale up the information storage tier and application tier independently.

If you want to provide access to Oracle Collaboration Suite components from public networks, then you must take measures to secure this type of access. You can enhance the security of the system by distributing the tiers and deploying the system behind a demilitarized zone (DMZ). Standard security practices would prevent, for example, network traffic from passing directly from the Internet to the database. Instead, such traffic would be routed through a DMZ and an Application Server tier.

The DMZ must contain the hardware and software required to relay traffic securely between the public network and private network. Sometimes a network gets flooded with so many requests that the data traffic stops or becomes very slow. Then the user may not be able to access any service or resource. Such a situation is termed as Denial of Service (DoS). So, DMZ must provide protection against the security threats, such as DoS and viruses.

Organization-specific Architecture Issues

This section discusses deployment configuration issues that may vary according to the specific requirements of each organization. For this reason, the Oracle Collaboration Suite Deployment Guide does not provide specific guidance for these issues.

- How many servers are needed for the number and profile of users?
- How much hardware can your organization afford?
- How many servers is your organization willing to manage?
- What type of platform is your organization comfortable with?
- Is your organization going to grow quickly?

- Does your organization need high availability?
- What is your organization's existing backup solution?
- Does your organization have archiving needs?

How many servers are needed for the number and profile of users?

General guidelines are provided in Chapter 3, "Deploying Oracle Collaboration Suite". These purpose of these guideline is to alert you to different deployment configurations and the advantages and disadvantages of each, but not to provide specific deployment configuration information.

How much hardware can your organization afford?

In an ideal world, you would purchase as many servers as you need to build a solid, highly available Oracle Collaboration Suite installation; however, budget limitations may require you to scale back your investment and make creative use of network services and protocols to run Oracle Collaboration Suite securely and efficiently.

How many servers is your organization willing to manage?

This largely depends the size of your IT staff and availability of system management tools.

What type of platform is your organization comfortable with?

Oracle Collaboration Suite supports several chip architectures and operating systems including heterogeneous and homogeneous platforms.

Is your organization going to grow quickly?

You may want to plan your deployment in three stages:

- **Development**: Map out host names, servers, components, services and access on a small scale.
- **Staging**: Expand your initial deployment for use by a test group, to expose design flaws and test capacity and performance.
- **Production**: Official deployment for use by the organization as a whole.

To ease the transition from a development environment to a production environment, it is best to use virtual host names from the start, as described in the "Scalability" section. With this strategy, you can grow into a duplicated application tier deployment without having to greatly modify the integration of your services and components.

Does your organization need high availability?

Keep in mind that implementing high availability generally doubles the need for hardware. You will need to implement cold failover strategies and should consider becoming familiar with Oracle10*g* Real Application Clusters.

Storage strategies in a high availability deployment are much different than in a standard deployment. Shared storage is needed; you should consider external SCSI storage or a storage area network (SAN), a high-speed specialized network that interconnects different kinds of data storage devices with associated data servers, or NAS.

The increased complexity of a high availability environment means that installation and configuration involves significantly more planning and effort than does a non high availability environment. Management of high availability is also more complex and should be allocated the appropriate amount of time.

What is your organization's existing backup solution?

Recommended backup strategies for most organizations include standing policies for regular, scheduled data backups, file system backups and tape backups. As well, organizations may have mandated recovery times and granularity for data recovery. With an Oracle Collaboration Suite installation, consider the amount of data that will be backed up for Oracle Mail, Oracle Calendar and Oracle Content Services.

Does your organization have archiving needs?

Oracle Mail enables third-tier storage of old or seldom accessed messages in a tertiary tablespace, which can be economically stored on disks. Other archiving strategies for Oracle Collaboration Suite are currently being developed.

Client Deployment Using the End-User Portal

The End-User Portal, is a set of customizable HTML pages that provides an overview of Oracle Collaboration Suite clients as well as information for downloading, installing, and configuring each Oracle Collaboration Suite client. The End-User Portal also includes links to the FAQ & Troubleshooting site on the Oracle Technology Network (OTN) as well as Oracle Collaboration Suite end-user tutorials

Certain components such as Mobile Data Sync or Oracle Mobile Collaboration require frequent device certification updates. In such cases, the End-User Portal provides getting started information for these components and links to OTN for device certification and configuration information.

Administrators can easily host the End-User Portal, they can customize the default content or add more content to the portal, and they can choose to show or hide content based on the Oracle Collaboration Suite components they are deploying at their site. For example if your organization is only deploying the Oracle Calendar, Oracle Content Services, and Oracle Mail components then you can configure the End-User Portal so that it only displays client deployment information for those components.

Administrators are encouraged to customize End-User Portal content. For example, administrators can use the End-User Portal to specify download locations, mail server names, and voicemail access numbers.

How-to procedures already documented in the component online help will not be duplicated in the End-User Portal. Where relevant, users are directed to sections of the online help for more information.

Installation and Administration

The End-User Portal is included with the installation CD as a ZIP file. Further information is provided in the Instructions for using the End-User Portal in *Oracle Collaboration Suite Administrator's Guide*

See Also: For information on installing the End-User Portal, please see the following;

- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

3

Deploying Oracle Collaboration Suite

This chapter describes some real-life examples of Oracle Collaboration Suite deployments in the following topics:

Deploying Oracle Collaboration Suite Overview

This chapter provides examples of how various organizations have deployed Oracle Collaboration Suite. You can use the deployment examples in this chapter to obtain general idea of how organizations of similar size or with similar requirements to yours chose to deploy Oracle Collaboration Suite. It is strongly recommended that you use the examples in this chapter as a reference only, rather than replicating a particular setup with all of its components.

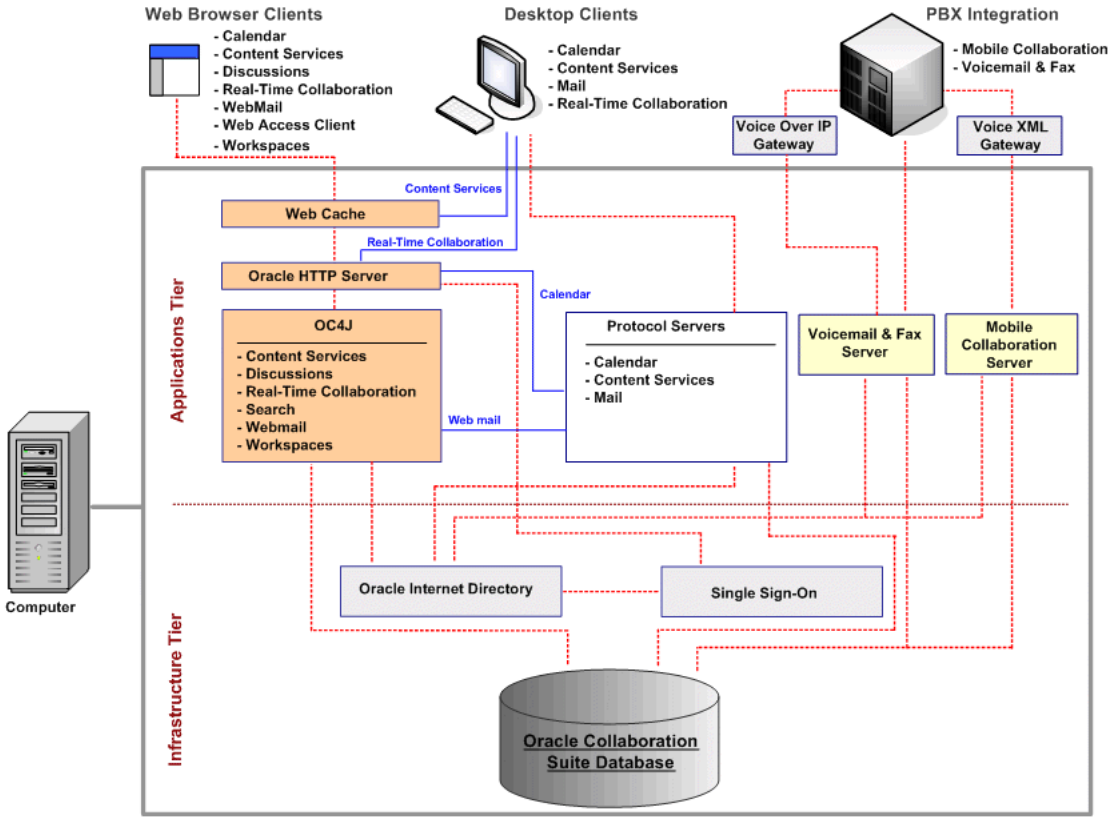
Oracle Collaboration Suite Simple Deployment (200 to 1,000 Users)

The Oracle Collaboration Suite simple deployment configuration is available for organizations of typically two hundred to one thousand users, although there is no specific user limitation. The simple deployment configuration contains the following options:

Single Computer Configuration

This section describes the Oracle Collaboration Suite components contained in a single computer deployment and explains how those components operate with each other.

Figure 3–1 Single Computer Deployment



In Figure 3–1 all Infrastructure tier and Applications tier components are deployed on a single computer and are accessed by Web browser clients, desktop clients, and telephony devices integrated with a PBX.

Infrastructure Tier

In Figure 3–1, the Infrastructure tier contains the Oracle Collaboration Suite database which is an Oracle Database 10*g* database server, the Oracle Internet Directory, and OracleAS Single Sign-On server. The Oracle Database 10*g* serves as a repository for Oracle Content Services, Oracle Mail, Oracle Real-Time Collaboration, and Oracle Workspaces. Authentication is handled by the Oracle Internet Directory, and OracleAS Single Sign-On server.

Applications Tier

The Applications tier also contains the applications and access methods for Web browser clients, desktop clients, and telephony clients that are integrated with a PBX. These include the Web cache, Oracle HTTP server, OC4J container, protocol servers, Voicemail & Fax server, and the Mobile Collaboration Server.

OC4J Containers

The OC4J containers have the following Java applications that run in the Applications tier:

- Oracle Content Services
- Oracle Discusssions

- Oracle Real-Time Collaboration
- Oracle Collaboration Suite Search
- Oracle WebMail
- Oracle Workspaces

Protocol Servers

The Applications tier contains the following protocol servers:

- Oracle Calendar
- Oracle Content Services
- Oracle Mail

Oracle Calendar is both a protocol server and a repository for calendar data and the Oracle Database does not store calendar data. See Chapter 5, "Deploying Oracle Calendar" for more information about the Oracle Calendar architecture and functionality.

Connection Flow

Figure 3–1 provides an overview of the flow of each Oracle Collaboration Suite application from the client to the repository. For a more detailed understanding of these flows, See the individual Oracle Collaboration Suite application deployment chapters in Part II, "Application-Level Deployment".

Web Browser Clients

Web Browser clients typically send an HTTP or HTTPS request to the Web cache which sends the request to the Oracle HTTP Server. The Oracle HTTP Server authenticates with the Oracle Internet Directory, and OracleAS Single Sign-On server and then sends the request to the target application in the OC4J container. Applications such as Oracle Discusssions, Oracle WebMail, and Oracle Workspaces obtain user information from the Oracle Internet Directory and all applications access data stored in the Oracle Collaboration Suite database.

There are two exceptions to this flow, Oracle Calendar, which is not an OC4J application and Oracle WebMail which typically uses the Oracle Mail protocol servers (SMTP and IMAP4) for incoming and outgoing mail.

In Figure 3–1, after Oracle Calendar accesses the Oracle Internet Directory, and OracleAS Single Sign-On server, the Oracle HTTP Server sends all Calendar HTTP or HTTPS requests to the Calendar protocol server. Oracle Calendar also does not store data in the Oracle Collaboration Suite database since it has its own repository deployed on the Applications tier.

Desktop Clients

Desktop clients typically access protocol servers on the Applications tier which authenticate with the Oracle Internet Directory. There are two exceptions to this flow, the Oracle Real-Time Collaboration console which sends TCP/IP requests to the Oracle HTTP Server, or Web cache, the Oracle Real-Time Collaboration Messenger client which connects directly with Applications tier computer that contains the Oracle Real-Time Collaboration core component instance, and the Oracle Content Services desktop client, which accesses the Web Cache.

Telephony Clients Integrated with a PBX

Oracle Mobile Collaboration, and Oracle Voicemail & Fax are both integrated with a PBX. The PBX sends voice information to the Mobile Collaboration Server through a voice XML gateway. The Mobile Collaboration Server authenticates with the Oracle Internet Directory and then accesses content in the Oracle Collaboration Suite database.

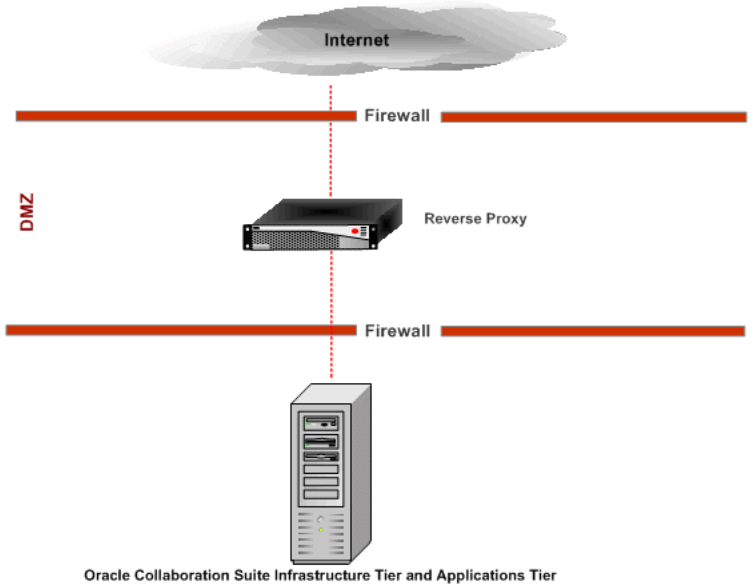
The PBX sends voice information to the Voicemail & Fax server either directly using a circuited switch, or through a Voice Over IP Gateway. The Voicemail & Fax server authenticates with the Oracle Internet Directory and then accesses content in the Oracle Collaboration Suite database.

Single Computer Configuration in a DMZ

For security reasons, you may wish to put the OracleAS Single Sign-On server within a DMZ. With a single computer configuration, however, placing the OracleAS Single Sign-On server within a DMZ places all the components in the DMZ which may be considered a security risk. To avoid this problem, you can place a reverse proxy in the DMZ and configure it to authenticate directly with the OracleAS Single Sign-On server.

Note: The reverse proxy can only proxy HTTP or HTTPS traffic. Oracle Real-Time Collaboration consoles do not use HTTP or HTTPS traffic and therefore, will not work behind a reverse proxy.

Figure 3–2 Single Computer in a DMZ



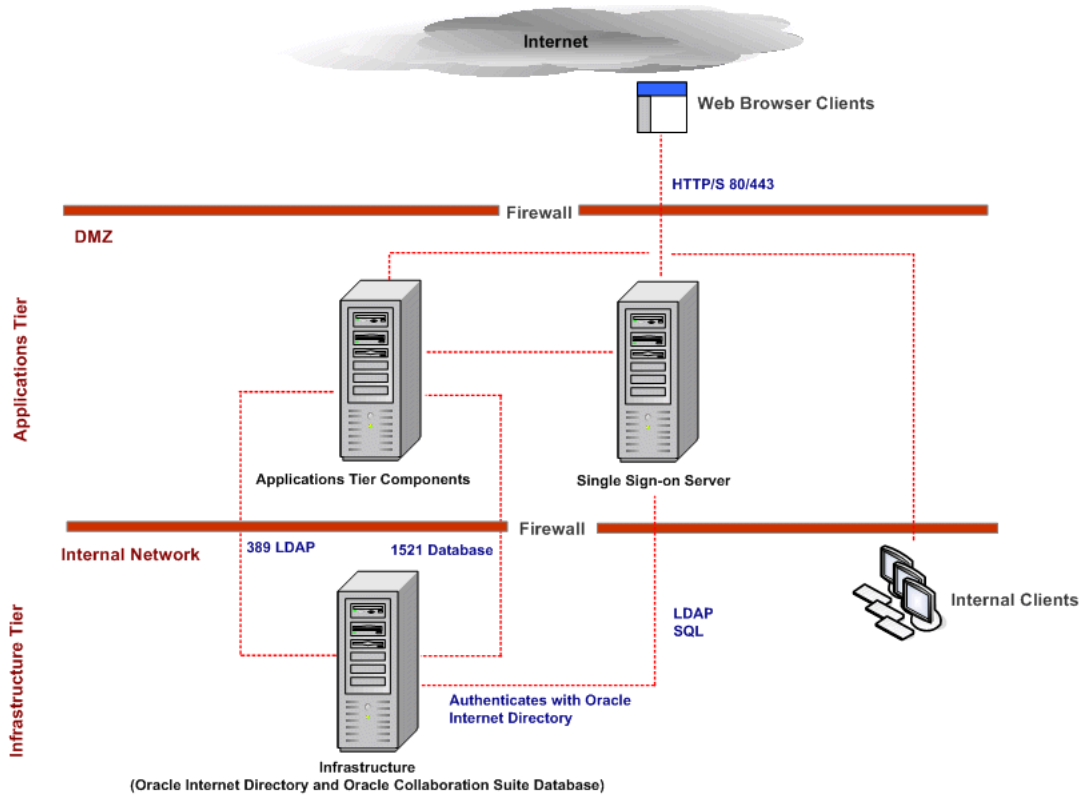
Oracle Collaboration Suite Medium Deployment (1,000 - 5,000 Users)

The Oracle Collaboration Suite medium deployment configuration is typical for organizations of typically one thousand to five thousand users, although there is no specific user limitation. The medium deployment configuration contains the following options:

Applications Tier Components and SSO Server on Separate Computers

This section describes deploying Oracle Collaboration Suite on two dedicated Applications tier computers and one Infrastructure tier computer.

Figure 3–3 Applications Tier Components and SSO Server on Separate Computers



In Figure 3–3, the Infrastructure tier contains one computer and the Applications tier contains two computers.

Infrastructure Tier

The Infrastructure tier contains one computer located behind a firewall. This computer contains the Oracle Collaboration Suite infrastructure, which consists of the Oracle Collaboration Suite database with Identity Management and the Oracle Application Server Metadata Repository.

Applications Tier

The Applications tier contains two computers located in a DMZ. One computer contains the Oracle Collaboration Suite Applications tier components and the other contains the OracleAS Single Sign-On server.

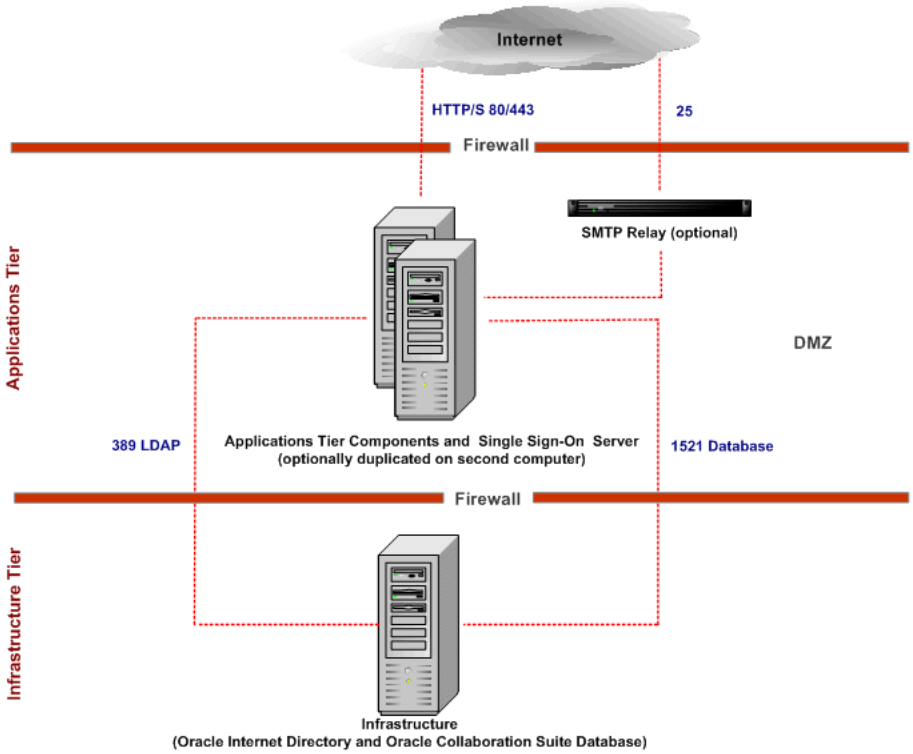
Connection Flow

In Figure 3–3, Web clients connect with the OracleAS Single Sign-On server using an HTTP/S connection through ports 80 or 443. The OracleAS Single Sign-On server authenticates login information against the Oracle Internet Directory and then passes the user request to the computer with the Applications tier components. The computer with the Applications tier components connects to the Oracle Internet Directory using an LDAP connection on port 389 or a database connection on port 1521.

Applications Tier Components and SSO Server on the Same Optionally Duplicated Computer

This section describes deploying Oracle Collaboration Suite on two duplicated Applications tier computers and one Infrastructure tier computer.

Figure 3–4 Applications Tier Components and SSO Server on the Same Optionally Duplicated Computer



In Figure 3–4, the Infrastructure tier contains one computer and the Applications tier contains two computers and an optional SMTP Relay device.

Infrastructure Tier

The Infrastructure tier contains one computer located behind a firewall. This computer contains Oracle Internet Directory and the Oracle Collaboration Suite Database.

Applications Tier

The Applications tier contains two computers located in a DMZ and an optional SMTP Relay device. Each computer contains the Oracle Collaboration Suite Applications tier components and the OracleAS Single Sign-On server.

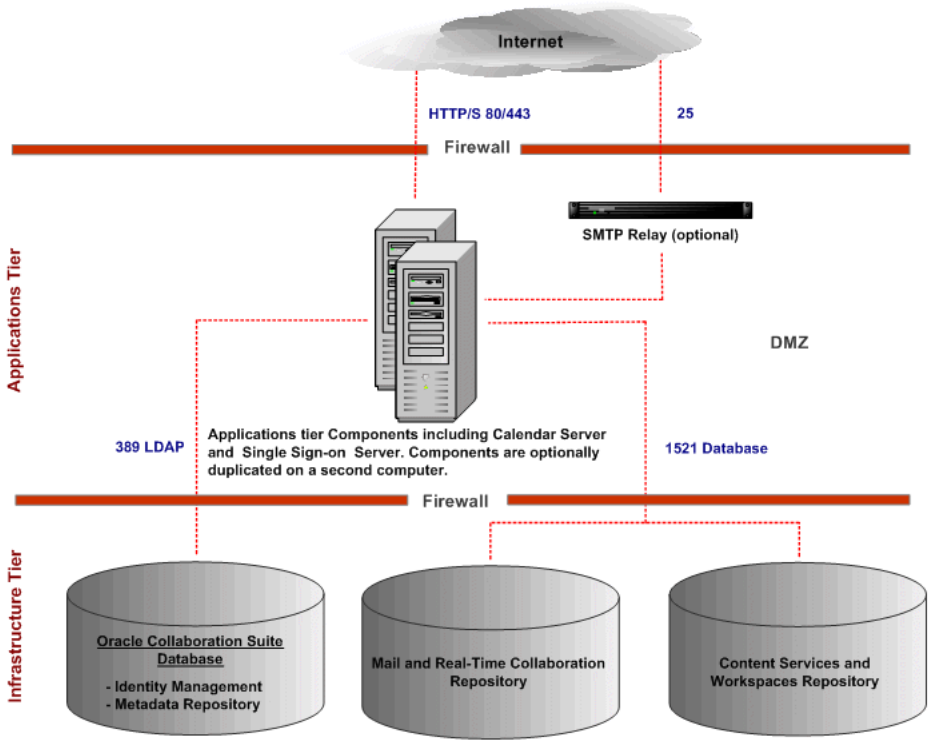
Connection Flow

In Figure 3–4, Web clients connect with the OracleAS Single Sign-On server using an HTTP or HTTPS connection through ports 80 or 443 and mail clients optionally connect through the SMTP Relay device using port 25. The OracleAS Single Sign-On server authenticates login information against the Oracle Internet Directory and then passes the user request to the computer with the Applications tier components. The Applications tier components connect to the Oracle Internet Directory using an LDAP connection on port 389 or a database connection on port 1521.

Infrastructure Components Distributed on Different Computers

This section describes deploying Oracle Collaboration Suite on two duplicated Applications tier computers and three dedicated Infrastructure tier computers.

Figure 3–5 Infrastructure Components Distributed on Different Computer



In Figure 3–5, the Infrastructure tier contains three computers and the Applications tier contains two computers and an optional SMTP Relay device.

Infrastructure Tier

The Infrastructure tier contains three computers located behind a firewall. One computer contains the Oracle Collaboration Suite database with Identity Management and Metadata Repository components, another computer contains the repositories for

Oracle Mail and Oracle Real-Time Collaboration, and the third computer contains the repositories for Oracle Content Services, and Oracle Workspaces.

Applications Tier

The Applications tier contains two computers located in a DMZ and an optional SMTP Relay device. Each computer contains the Oracle Collaboration Suite Applications tier components and the OracleAS Single Sign-On server. The Oracle Calendar server is deployed on the Applications tier.

Connection Flow

In Figure 3–5, Web clients connect with the OracleAS Single Sign-On server using an HTTP or HTTPS connection through ports 80 or 443 and mail clients optionally connect through the SMTP Relay device using port 25. The OracleAS Single Sign-On server authenticates login information against the Oracle Internet Directory and then passes the user request to the computer with the Applications tier components. The Applications tier components connect to the Oracle Internet Directory computer using an LDAP connection on port 389. Applications tier components, excluding Oracle Calendar, connect to their respective repositories on the remaining two Infrastructure tier computers using a database connection on port 1521.

Oracle Collaboration Suite Large Deployment (Several Thousand Users)

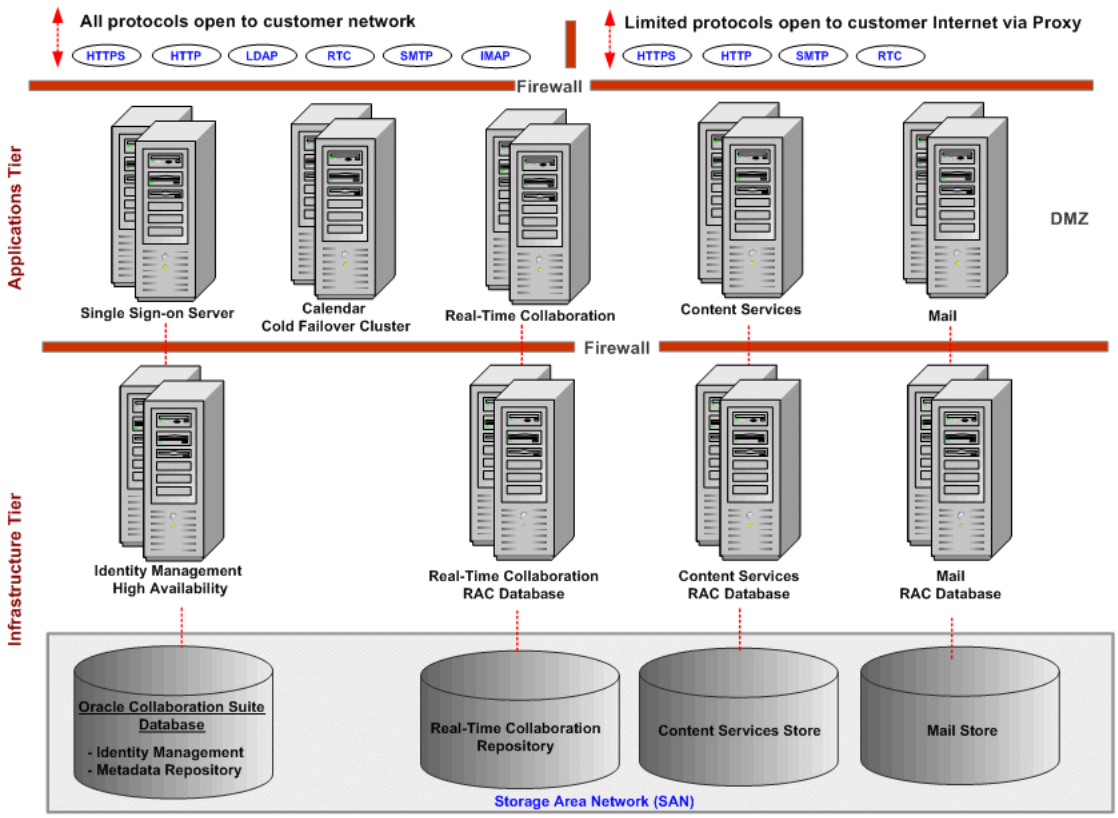
The Oracle Collaboration Suite large deployment configuration is available for organizations with several thousand users. The large deployment configuration contains the following options:

- Large Deployment with Dedicated Applications Tiers
- Large Deployment with Duplicated Applications Tiers

Large Deployment with Dedicated Applications Tiers

This section describes a large deployment of most Oracle Collaboration Suite applications with dedicated Applications tier computers.

Figure 3–6 Large Deployment with Dedicated Application Tiers



The example in Figure 3–6 is limited to a deployment of Oracle Calendar, Oracle Content Services, Oracle Mail, and Oracle Real-Time Collaboration, however, other Oracle Collaboration Suite applications can also be deployed in this configuration.

Infrastructure Tier

The Infrastructure tier contains the following:

- Two computers that provide identity management high availability
- Two computers for the Oracle Real-Time Collaboration RAC database
- Two computers for the Oracle Content Services RAC database
- Two computers for the Oracle Mail RAC database

The Infrastructure tier computers connect to the following which are located in a Storage Area Network (SAN):

- Oracle Internet Directory
- Real-Time Collaboration Repository
- Content Services Repository
- Mail Repository

Applications Tier

The Applications tier contains the following components on redundant dedicated computers:

- OracleAS Single Sign-On Server
- Oracle Calendar in a cold failover cluster
- Oracle Real-Time Collaboration
- Oracle Content Services
- Oracle Mail

Connection Flow

does not illustrate the connection flow between the various components deployed in this configuration. To understand the connection flow, please see the diagram and text in the "Single Computer Configuration" section. In this configuration, the following protocols are open to the customer network:

- HTTP
- HTTPS
- LDAP
- RTC
- SMTP
- IMAP
- Calendar and FTP protocols

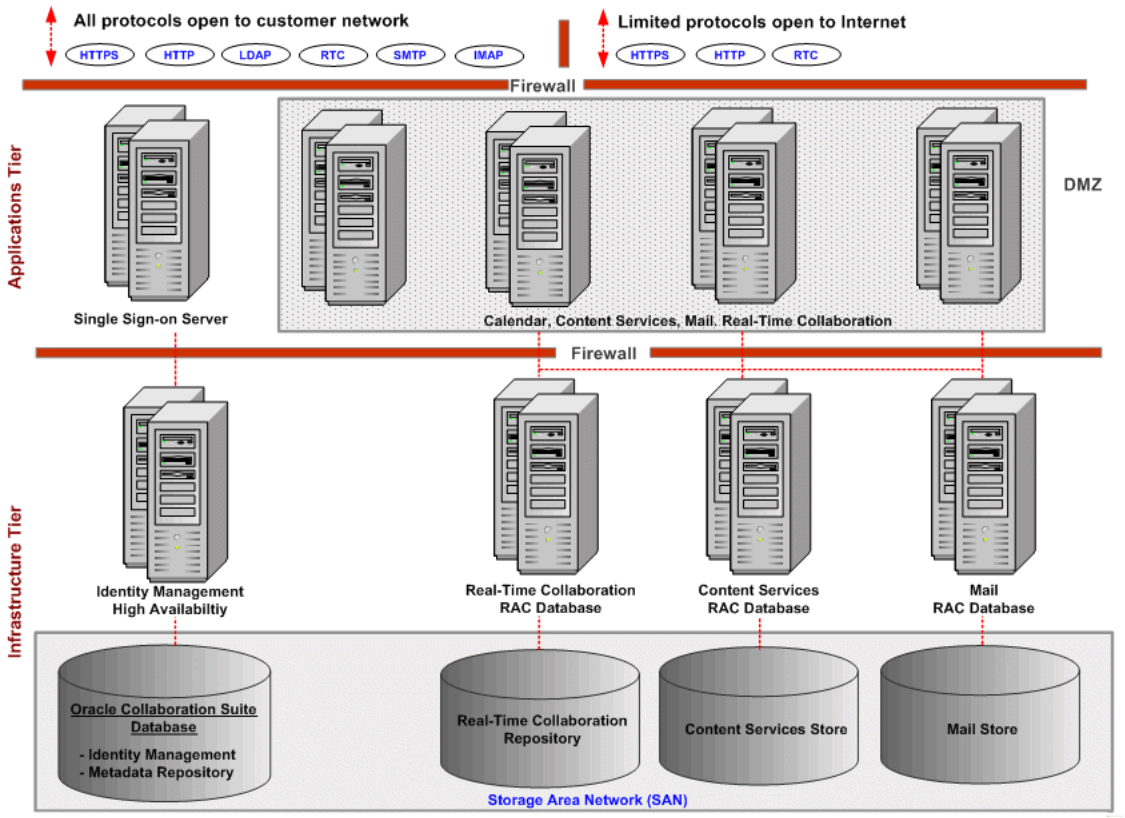
In this configuration, the following are limited protocols open to the customer Internet through Proxy:

- HTTP
- HTTPS
- SMTP
- RTC

Large Deployment with Duplicated Applications Tiers

This section describes a large deployment of most Oracle Collaboration Suite applications with duplicated Applications tier computers.

Figure 3–7 Large Deployment with Duplicated Application Tiers



The example in Figure 3–7, is limited to a deployment of Oracle Calendar, Oracle Content Services, Oracle Mail, and Oracle Real-Time Collaboration, however, other Oracle Collaboration Suite applications can also be deployed in this configuration.

Infrastructure Tier

The Infrastructure tier contains the following:

- Two computers that provide identity management high availability
- Two computers for the Oracle Real-Time Collaboration RAC database
- Two computers for the Oracle Content Services RAC database
- Two computers for the Oracle Mail RAC database

The Infrastructure tier computers connect to the following which are located in a SAN:

- Oracle Internet Directory
- Real-Time Collaboration Repository
- Content Services Repository
- Mail Repository

Applications Tier

The OracleAS Single Sign-On server is deployed on the Applications tier on redundant dedicated computers. In addition, the following components are deployed on eight pairs of duplicated computers:

- Oracle Calendar in a cold failover cluster
- Oracle Real-Time Collaboration
- Oracle Content Services
- Oracle Mail

Connection Flow

does not illustrate the connection flow between the various components deployed in this configuration. To understand the connection flow, see the diagram and text in the "Single Computer Configuration" section. In this configuration, the following protocols are open to the customer network:

- HTTP
- HTTPS
- LDAP
- RTC
- SMTP
- IMAP
- Calendar and FTP protocols

In this configuration, the following are limited protocols open to the customer Internet through Proxy:

- HTTP
- HTTPS
- SMTP
- RTC

Oracle Collaboration Suite High Availability Architectures

This section discusses Oracle Collaboration Suite High Availability Architectures

Overview

Availability is the degree to which an application or service is available with the expected functionality. This section discusses high availability deployment issues and options for Oracle Collaboration Suite.

Common Requirements

This section consists of the Oracle Collaboration Suite high-availability requirements which are common to each Oracle Collaboration Suite architecture described later. Oracle Collaboration Suite high-availability architecture consists of the following components:

- Section , "Oracle Collaboration Suite Database Tier"
- Section , "Identity Management Service"
- Section , "Oracle Calendar server"
- Section , "Oracle Collaboration Suite Applications"

When a node contains multiple Oracle homes, a single shared `oraInventory` is used on each node except for the Oracle Calendar server cold failover cluster installation which must have its own `oraInventory`.

Oracle Collaboration Suite Database Tier

For high availability, Oracle recommends that this database be deployed as a Real Application Clusters (RAC) database in an active-active configuration.

Oracle home is installed on each node of the hardware cluster.

The hardware requirements for Oracle Collaboration Suite Database tier are as follows:

- Hardware cluster with vendor clusterware and Oracle Cluster Ready Services (CRS)
- Shared storage for the RAC database files and CRS files. Oracle database files can be on raw devices, Network Attached Storage (NAS), OCFS for Linux, or use Oracle Automatic Storage Management (ASM) or SAN
- A virtual IP address for each cluster node

Identity Management Service

Oracle Internet Directory and OracleAS Single Sign-On tiers together provide the Identity Management service.

For high availability, Oracle recommends that multiple instances of Oracle Internet Directory and OracleAS Single Sign-On tiers be deployed or that the deployment be designed with redundancy to continue the Identity Management services in case there are issues with any of the Identity Management nodes. An active-active deployment of these tiers require load balancers.

Oracle home is installed on multiple nodes.

The hardware requirements for Identity Management tier are as follows:

- Single node
- Local storage
- Nodes are front-ended by a load balancer to route requests to the Identity Management services on both nodes of the cluster.

Oracle Calendar server

For high availability, Oracle Calendar server is placed on a cold failover cluster because it is a single point of failure. This cold failover cluster installation requires shared storage for the Oracle home and `oraInventory` directory trees. The Oracle Calendar server file system database is contained under the Oracle home directory tree. To facilitate a cold failover cluster, a virtual IP address and host are required.

Oracle home and `oraInventory` are located on a dedicated shared storage of the hardware cluster. This Oracle home should have a separate `oraInventory` from Oracle home of other components so that when the shared file system is failed over, `oraInventory` is also failed over with the same mount point.

The hardware requirements for Oracle Calendar server are as follows:

- Hardware cluster with vendor clusterware. The Calendar server can be on the same cluster as the Oracle Collaboration Suite Database but in the case of Linux, Oracle Cluster Ready Services and RedHat Cluster Manager cannot coexist. As a result, the failover has to be manual or Oracle Calendar server should be put on a cluster that is separate from the RAC database.

- Shared storage for the Oracle home and `oraInventory` of Oracle Calendar server
- A virtual IP address

Oracle Calendar server can be installed on its own cluster that is separate from the Oracle Collaboration Suite Database cluster, if required.

Oracle Collaboration Suite Applications

Oracle Collaboration Suite Applications nodes can be deployed in DeMilitarized Zone (DMZ). A load-balancer virtual server forms the front end for multiple application nodes. Client requests to the Oracle Collaboration Suite Application nodes are load balanced across the Oracle Collaboration Suite Applications nodes by the load balancer using the load-balancer virtual server.

An Oracle home is installed on each Oracle Collaboration Suite Applications node.

The hardware requirements for Oracle Collaboration Suite Applications node are as follows:

- Single node
- Local storage
- Configured to work with a load-balancer virtual server front-end to route requests to applications on both nodes

In the architectures documented in the following section, all Oracle Collaboration Suite Applications components are installed on each Oracle Collaboration Suite Applications node. As an alternative to installing all the Oracle Collaboration Suite Applications components on each Oracle Collaboration Suite Applications node, it may be necessary or desirable to separate some Oracle Collaboration Suite Applications components to their own set of nodes.

For example, an installation may have a very large number of e-mail users and because of this you might want to separate the Oracle Mail component from the nodes containing other Oracle Collaboration Suite Applications. This would result in two nodes, one of which would contain only the Oracle Mail component and the other two of which would contain Oracle Collaboration Suite Applications nodes would contain all Oracle Collaboration Suite Applications components except for Oracle Mail. This is based on the assumption that each unique installation of Oracle Collaboration Suite Applications should have at least two nodes to ensure the availability of Oracle Collaboration Suite Applications. Therefore, if you do decide to separate an Oracle Collaboration Suite Application component from the rest of the Oracle Collaboration Suite Applications, plan on at least two additional nodes.

Overview of High-Availability Architectures

Oracle Collaboration Suite provides high-availability solutions for maximum protection against any kind of failure with flexible installation, deployment, and security options. There are three sample high-availability architectures for Oracle Collaboration Suite defined here:

- Oracle Collaboration Suite Single Cluster Architecture
- Oracle Collaboration Suite Colocated Identity Management Architecture
- Oracle Collaboration Suite Distributed Identity Management Architecture

Details of these architectures are discussed in the following subsections.

The following table summarizes the details of Oracle home in the high-availability architectures.

Table 3–1 Oracle Home Details in High Availability Architecture

Architecture	Oracle Collaboration Suite Database	Oracle Internet Directory/Directory Integration and Provisioning	OracleAS Single Sign-On/Delegated Administration Services	Oracle Calendar server	Oracle Collaboration Suite Applications
Single Cluster Architecture with 2 nodes	Separate Oracle homes are created on Node 1 and Node 2.	Oracle homes are created on Node 1 and Node 2. Oracle Internet Directory/Directory Integration and Provisioning and OracleAS Single Sign-On/Delegated Administration Services have same Oracle homes.	Same as the previous column.	The Oracle home on shared disk is mounted and active on Node 1. If failover occurs the Oracle home on shared disk is mounted and active on Node 2.	Separate Oracle homes are created on Node 1 and Node 2.
Colocated Identity Management Architecture with 4 nodes ■ Nodes 1, 2 in one cluster containing the database ■ Nodes 3, 4 are single nodes for Identity Management and Oracle Collaboration Suite Applications	Separate Oracle homes are created on Node 1 and Node 2.	Oracle homes are created on Node 3 and Node 4. Oracle Internet Directory/Directory Integration and Provisioning and OracleAS Single Sign-On/Delegated Administration Services have same Oracle homes.	Same as the previous column.	The Oracle home on shared disk is mounted and active on Node 1. If failover occurs the Oracle home on shared disk is mounted and active on Node 2.	Separate Oracle homes are created on Node 3 and Node 4.
Distributed Identity Management Architecture with 6 nodes ■ Nodes 1, 2 in one cluster containing the database ■ Nodes 3, 4, 5, and 6 are single nodes for Identity Management and Oracle Collaboration Suite Applications	Separate Oracle homes are created on Node 1 and Node 2.	Oracle homes are created on Node 3 and Node 4.	Separate Oracle homes are created on Node 5 and Node 6.	The Oracle home on shared disk is mounted and active on Node 1. If failover occurs the Oracle home on shared disk is mounted and active on Node 2.	Separate Oracle homes are created on Node 5 and Node 6.

Note: For high availability, we require a RAC database configuration for Oracle Collaboration Suite Database which in turn requires Cluster Ready Services to be running. We cannot have a single cluster architecture on linux platform because Cluster Ready Services and RedHat Cluster Manager cannot coexist on the same hardware cluster.

Oracle Collaboration Suite Single Cluster Architecture

This architecture is a minimal box configuration so all the following tiers are installed on a single cluster.

- Oracle Collaboration Suite Database
- Identity Management Service
- Oracle Calendar server
- Oracle Collaboration Suite Applications

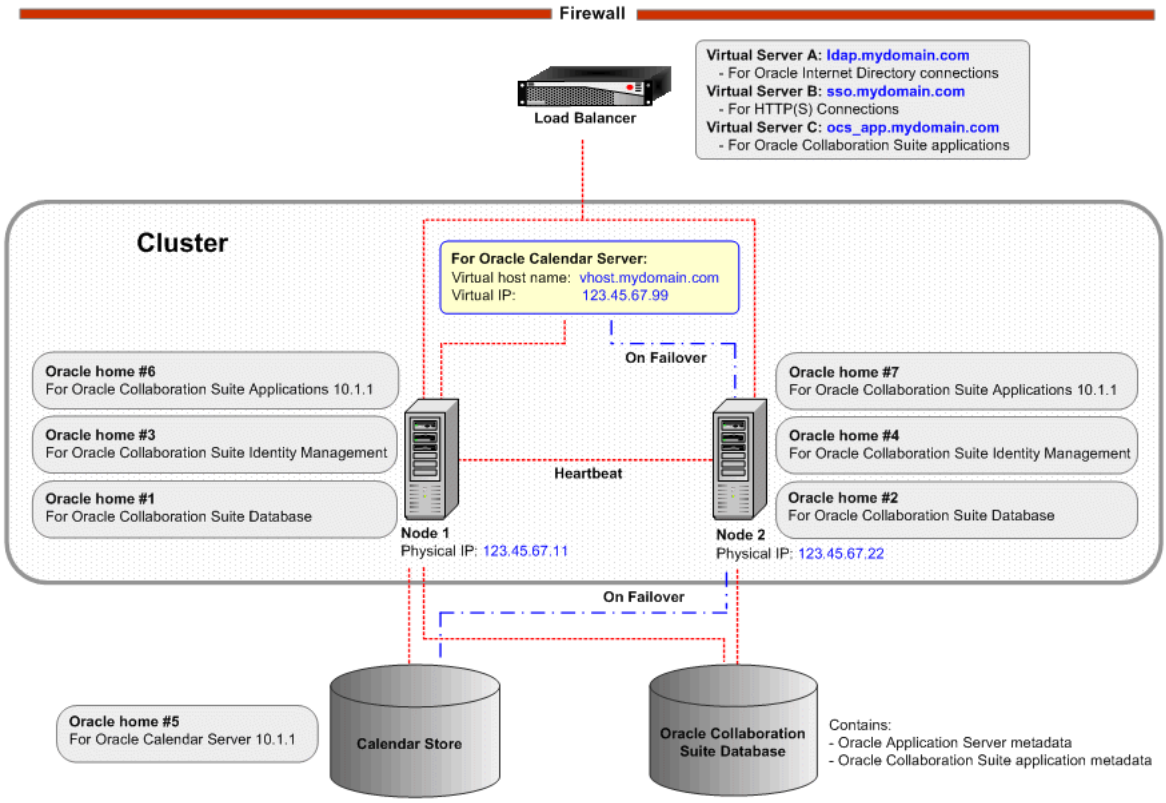
This architecture is not an out-of-box solution and requires multiple installations of Oracle Collaboration Suite and manual post-installation configuration. In this architecture, the highly available configuration is active-active or for Real Application Cluster (RAC) for Oracle Collaboration Suite Database 10.1.0.5, and active-active for Identity Management. Multiple active instances provide continued availability in case of failure of one instance. The database instance processes run on both the nodes of the hardware cluster. For the Identity Management to be highly available, the cluster is front ended by a load balancer.

See Also: For information on installing Oracle Calendar, please see the following;

- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

The cluster configuration for Oracle Collaboration Suite consists of Oracle Collaboration Suite Database deployed on a cluster with two or more nodes. Figure 3–8 shows Node1 and Node2 in the cluster. Each Oracle Collaboration Suite Database node has a local copy of the Oracle Collaboration Suite software installed. All file-system based configuration files are local to each node as well. There is one single Oracle Collaboration Suite Database shared by all the database nodes. This RAC database is installed on a shared volume accessible by all Oracle Collaboration Suite Database nodes.

Figure 3–8 Single Cluster Architecture



Oracle database instances exist on each node and concurrently open the database for read or write operation. The database instance processes and Identity Management processes run on both the nodes of the hardware cluster. Oracle home #1 and Oracle home #2 for Oracle Collaboration Suite Database are created in Node1 and Node2.

Oracle home #3 and Oracle home #4 are created for Identity Management service. Oracle home #6 and Oracle home #7 are created for Oracle Collaboration Suite Applications 10.1.1 and can include the following components:

- Oracle Mail
- Oracle Content Services
- Oracle Search
- Oracle Mobile Collaboration
- Oracle Voicemail and Fax
- Oracle Calendar
- Oracle Real Time Collaboration
- Oracle Discussions
- Oracle Workspaces

Oracle Calendar server will store its data on file system residing on shared disk, which is accessed by only one node of the cluster at any given time. So Oracle Calendar server will only be running on cluster Node1 shown in Figure 3–8. Only after a failure of Oracle Calendar server on Node1, Oracle Calendar server becomes active on cluster Node2. Oracle home #5 is created for Oracle Calendar server and it includes the file

system level database that stores all calendar-related data. This database is not an Oracle database.

Oracle Collaboration Suite Infrastructure

Oracle Collaboration Suite Infrastructure 10.1.1 requires some work around to configure highly available configuration for Identity Management and Oracle Collaboration Suite Database installation on a two-node cluster running Oracle Cluster Ready Services (CRS). If you plan to use Oracle Calendar server in a highly available configuration, you must have hardware cluster manager installed with Oracle CRS to support the cold hardware failover. Oracle home, where Oracle Collaboration Suite Infrastructure resides, must be on local file system on each node of the cluster.

The Identity Management components will be based on Oracle Application Server 10g (Release 10.1.2.0.2). The components will run on all nodes of the cluster in active-active node. A load balancer will be placed in front of Identity Management nodes to route requests to the Identity Management services on the nodes of the cluster.

Oracle Collaboration Suite Database is the Oracle 10*g* (Release 10.1.0.5) RAC database containing Oracle Collaboration Suite component schema information and Oracle Application Server 10*g* (Release 10.1.2.0.2) Metadata Repository. The RAC database will run in active-active mode. All instances of the RAC database can service requests.

Oracle Collaboration Suite Colocated Identity Management Architecture

This architecture separates the Oracle Collaboration Suite Database tier and the Identity Management tier rather than sharing nodes as in the Single Cluster Architecture. This architecture is not an out-of-box Oracle Collaboration Suite Database tier and requires multiple installations of Oracle Collaboration Suite and manual post-installation configuration.

In this architecture, the highly available configuration is active-active (RAC) for Oracle Collaboration Suite Database 10.1.0.5 and Identity Management.

The Oracle Collaboration Suite Database tier is created by using Metadata Repository Configuration Assistant (MRCA) or the Oracle Collaboration Suite Database only install option. The Identity Management tier is installed separately against the Oracle Collaboration Suite Database on multiple non-clustered machines.

Figure 3–9 Colocated Architecture

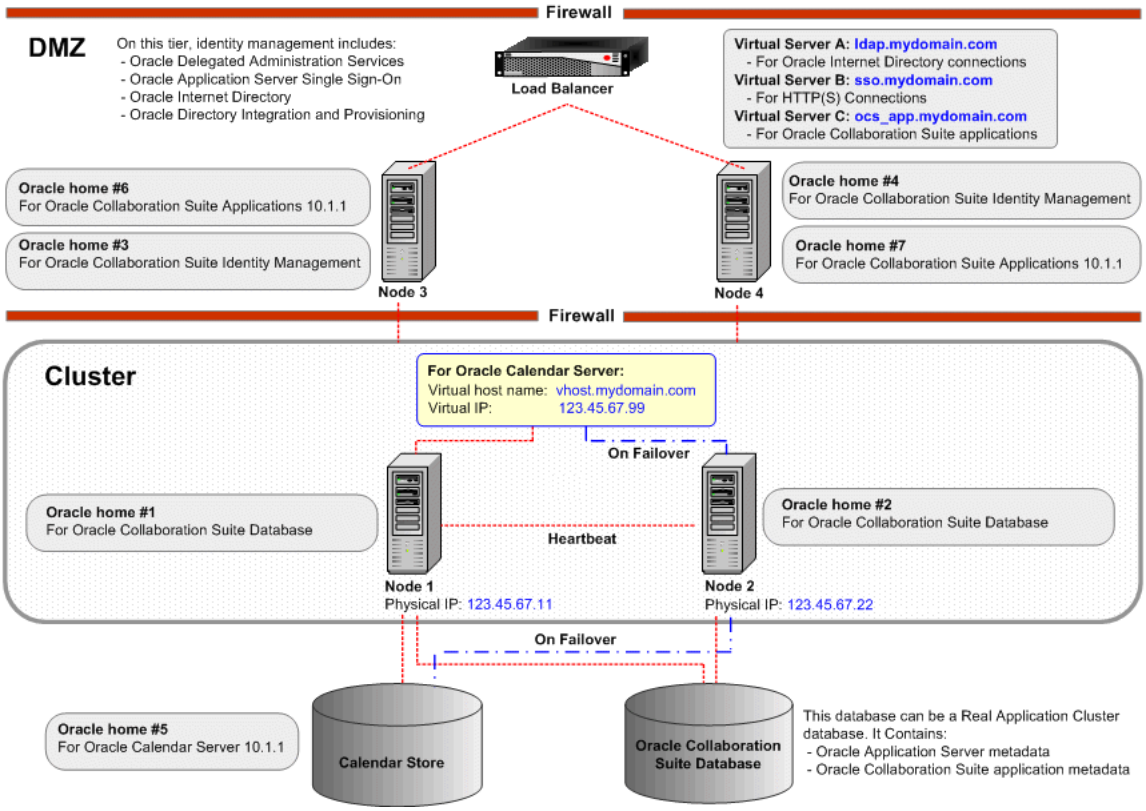


Figure 3–9 shows Node1 and Node2 in the cluster. Oracle home #1 and Oracle home #2 are created for the existing Oracle 10g database with Oracle Collaboration Suite Database 10.1.1 in Node1 and Node2 respectively.

Oracle Calendar server will store its data on file system residing on shared disk, which is accessed by only one node of the cluster at any given time. So Oracle Calendar server will only be running on cluster Node1 shown in Figure 3–9. Only after a failure of Oracle Calendar server on Node1, Oracle Calendar server becomes active on cluster Node2. Oracle home #5 is created for Oracle Calendar server and it includes the file system level database that stores all calendar-related data. This database is not an Oracle database.

Oracle home #3 and Oracle home #4 are created for Identity Management on Node3 and Node4. On this tier, Identity Management includes the following components:

- Oracle Internet Directory
- OracleAS Single Sign-On
- Delegated Administration Services
- Oracle Directory Integration and Provisioning

Oracle home #6 and Oracle home #7for Oracle Collaboration Suite Applications 10.1.1 are created. On this tier, Oracle Collaboration Suite Applications 10.1.1 can include the following components:

- Oracle Mail
- Oracle Content Services

- Oracle Search
- Oracle Mobile Collaboration
- Oracle Voicemail and Fax
- Oracle Calendar
- Oracle Real Time Collaboration
- Oracle Discussions
- Oracle Workspaces

A hardware load balancer is placed at the front end of the Identity Management machines and it balances the Identity Management traffic load.

Oracle Collaboration Suite Applications

In Colocated Identity Management Architecture, Oracle Collaboration Suite Applications is installed on separate machines outside Oracle Collaboration Suite Infrastructure. Each installation of Oracle Collaboration Suite will contain all the following components:

- Oracle Mail
- Oracle Content Services
- Oracle Search
- Oracle Mobile Collaboration
- Oracle Voicemail and Fax
- Oracle Calendar
- Oracle Real Time Collaboration
- Oracle Discussions
- Oracle Workspaces

A load balancer front ends the Oracle Collaboration Suite Applications tier to load balance the requests to all the Applications tier servers.

Oracle Collaboration Suite Distributed Identity Management Architecture

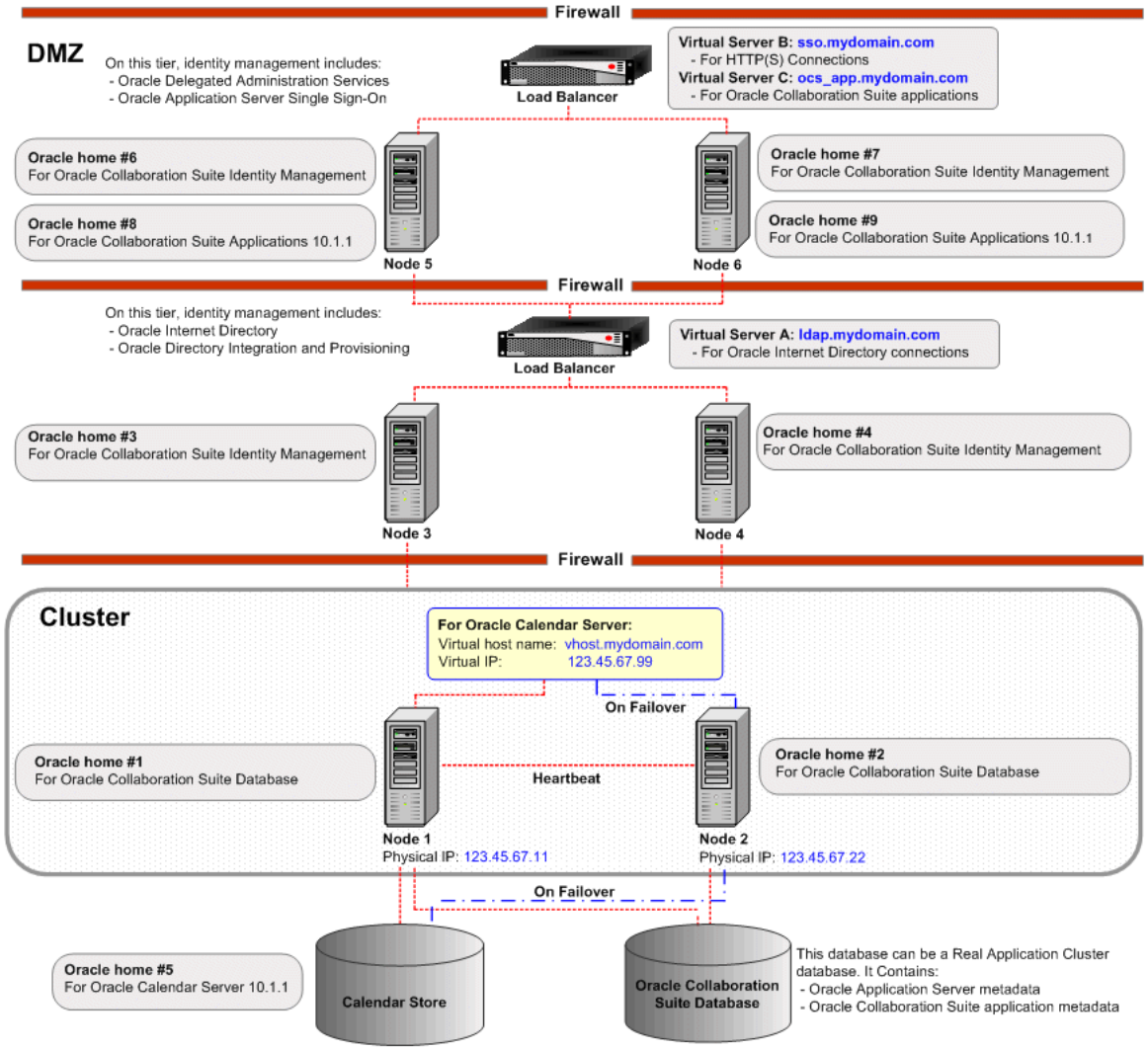
This architecture is similar to Colocated Identity Management Architecture except that the Identity Management components, Oracle Internet Directory and OracleAS Single Sign-On, are distributed across multiple non-clustered servers in a DMZ.

This architecture is not an out-of-box Oracle Collaboration Suite Database tier and requires multiple installations of Oracle Collaboration Suite and manual post-installation configuration.

In this architecture, the highly available configuration is active-active (RAC) for Oracle Collaboration Suite Database 10.1.0.5, Oracle Internet Directory and OracleAS Single Sign-On.

In this configuration, Oracle Internet Directory is deployed on multiple non-clustered servers in DMZ and OracleAS Single Sign-On is installed on multiple non-clustered servers in DMZ. This configuration is not an out-of-box Oracle Collaboration Suite high-availability solution and it requires multiple installation of Oracle Collaboration Suite Infrastructure and manual post-installation configuration.

Figure 3–10 Distributed Architecture



Oracle home #1 and Oracle home #2 are created for the existing Oracle 10*g* database with Oracle Collaboration Suite Database 10.1.1 in Node1 and Node2 respectively.

Oracle Calendar server will store its data on a file system residing on shared disk, which is accessed by only one node of the cluster at any given time. As a result, Oracle Calendar server only runs on cluster Node1 shown in Figure 3–10. Only after a failure of Oracle Calendar server on Node1, Oracle Calendar server becomes active on cluster Node2. Oracle home #5 is created for Oracle Calendar server and it includes the file system level database that stores all calendar-related data. This database is not an Oracle database.

Oracle home #3 and Oracle home #4 are created for Identity Management. On the Oracle Internet Directory tier, Identity Management includes the following components:

- Oracle Internet Directory
- Oracle Directory Integration and Provisioning

Oracle home #8 and Oracle home #9 for Oracle Collaboration Suite Applications 10.1.1 are created on Node5 and Node6. On this tier, Oracle Collaboration Suite Applications 10.1.1 includes the following components:

- Oracle Mail
- Oracle Content Services
- Oracle Search
- Oracle Mobile Collaboration
- Oracle Voicemail and Fax
- Oracle Calendar
- Oracle Real Time Collaboration
- Oracle Discussions
- Oracle Workspaces

Oracle home #6 and Oracle home #7 for Identity Management in Oracle Collaboration Suite Infrastructure 10.1.1 are created on Node5 and Node6 as shown in Figure 3–10. On the Oracle Application Server Single Sign-On tier, Identity Management includes the following components:

- Oracle Application Server Single Sign-On
- Delegated Administration Services

The firewall ports to be opened are as follows:

- Oracle Net
- Oracle Internet Directory port
- Oracle Internet Directory SSL port

A hardware load balancer is placed at the front end of the Oracle Internet Directory tier machines of Identity Management. It balances the Oracle Internet Directory traffic load. Another hardware load balancer is placed at front of the OracleAS Single Sign-On tier machines and it balances the HTTP traffic load.

Oracle Collaboration Suite Applications

In Distributed Identity Management Architecture, Oracle Collaboration Suite Applications is installed on separate machines outside Oracle Collaboration Suite Infrastructure. Each installation of Oracle Collaboration Suite will contain all the following components:

- Oracle Mail
- Oracle Content Services
- Oracle Search
- Oracle Mobile Collaboration
- Oracle Voicemail and Fax
- Oracle Calendar
- Oracle Real Time Collaboration
- Oracle Discussions
- Oracle Workspaces

A load balancer front ends the Oracle Collaboration Suite Applications tier to load balance the requests to all the Applications tier servers.

Configuration of Load Balancers

Load balancers play a key role in all the high-availability architectures. Not only can load balancers balance the load across nodes but they can also detect when a node or the necessary application on a node is down and reroute traffic to an active node. Where a hardware load balancer is required, it will be configured to direct incoming requests for Oracle Application Server Single Sign-On, Oracle Internet Directory, and Oracle Collaboration Suite Applications. The load balancer will only be used for non-Oracle Net traffic such as HTTP, LDAP, HTTPS and so on. It is configured with three virtual servers as indicated in the preceding diagrams:

1. Oracle Internet Directory/Directory Integration and Provisioning: Virtual server A, `ldap.mydomain.com`
2. OracleAS Single Sign-On/Delegated Administration Services: Virtual server B, `sso.mydomain.com`
3. Oracle Collaboration Suite Applications: Virtual server C, `ocs_app.mydomain.com`

This section describes the configuration requirements for the load balancer for all the highly available configurations of Oracle Collaboration Suite. For high availability, the recommendations for load balancers are as follows:

- The load balancer should be deployed in a fault tolerant configuration. Two load balancers should be used. These fault tolerant load balancers should be identical in terms of their configuration and capacity. Their failover should be automatic and seamless.
- The load balancer type used should be able to handle both HTTP and LDAP traffic in the highly available configurations described in this chapter. Any load balancing mechanism that supports only one of the protocols cannot be used in the default configuration.
- The load balancer should not drop idle connections. Any timeouts associated with dropping of connection should be eliminated.

Two load balancer settings are of primary importance for the highly available configuration:

- The nodes to which the load balancer directs traffic.
- The persistence setting of the load balancer

The persistence mechanism used should provide session level stickiness. By default, HTTP and Oracle Internet Directory requests both use the same virtual host address configured for the load balancer. Hence, the persistence mechanism used is available for both kinds of requests.

If the load balancer enables for the configuration of different persistence mechanisms for different server ports (LDAP and HTTP) for the same virtual server, then this is the recommended strategy. In this case, a cookie-based persistence with session-level timeout is more suitable for the HTTP traffic. No persistence setting is required for the LDAP traffic. If the load balancer does not allow specification of different persistence mechanisms for LDAP and HTTP, then the timeout value for session level stickiness should be configured based on the requirements of the deployed application. The recommended default stickiness timeout is 60 seconds. It should be adjusted based on the nature of the deployment and the load balancing achieved across the Oracle

Collaboration Suite nodes. It should be increased if session timeouts are experienced by Delegated Administration Services users. It should be decreased if even load balancing is not achieved.

Load balancers come in many flavours and each may have its own configuration mechanism. Consult your load balancer documentation for the specific instructions to achieve these configurations

Comparison of High-Availability Architectures

Each high-availability architecture option offers advantages and disadvantages.The following table summarizes the differences among the high-availability architectures.

	Single Cluster Architecture	Colocated Identity Management Architecture	Distributed Identity Management Architecture
Type of Configuration	It is a minimal box configuration because all the tiers are installed on a single cluster.	Oracle Collaboration Suite Database tier, Oracle Collaboration Suite Applications and Identity Management tier are deployed separately.	Oracle Collaboration Suite Database tier, Oracle Collaboration Suite Applications, Oracle Internet Directory and OracleAS Single Sign-On are deployed separately.
Management	More system resource is required because everything is running on only two nodes.Also, it is not easy to secure this setup.	System usage is distributed since the Oracle Collaboration Suite Database tier is separated and network security can be stronger.	System usage is distributed even further than Colocated since the Oracle Collaboration Suite Database tier, Oracle Internet Directory tier, and OracleAS Single Sign-On tier are separated and network security can be stronger.
Cost	Cheapest solution	Cheaper than Distributed architecture.	Expensive solution

4

Interoperability with Other Oracle Products

This chapter contains the following topics.

Oracle Collaboration Suite Interoperability with Oracle Database

This section contains the following topics.

Using an Existing Oracle Database with Oracle Collaboration Suite

This section provides information for using an existing Oracle database with Oracle Collaboration Suite.

Platform Dependencies of an Existing Oracle Database with Oracle Collaboration Suite

The Oracle Database 10*g* is supported on all platforms upon which Oracle Collaboration Suite is supported. Oracle Application Server Application Server Repository Creation Assistant (RepCA) however is not supported on all platforms.

Version Dependencies of an Existing Oracle Database with Oracle Collaboration Suite

Oracle Collaboration Suite must be installed with version 10.1.0.5 of the Oracle Database 10*g*.

Seeding an Existing Oracle Database for Oracle Collaboration Suite

You can optionally convert an existing Oracle Database 10*g* into an Oracle Collaboration Suite Database. The database must be version 10.1.0.5 or higher and must you must already have Oracle Internet Directory since this information is requested by the installer and there is no option to register it later.

You can choose the type of storage management you want such as File System, Automatic Storage Management (ASM), or RAW, and Oracle Collaboration Suite creates the tablespaces and Oracle Collaboration Suite schemas on the specified storage type during the installation process.

During the configuration phase, if not previously registered, the Oracle9*i* Database Server is registered in Oracle Internet Directory and executes component configuration assistants. The component configuration assistants create their schemas and register the information in Oracle Internet Directory which assists with the database selection during the installation of Oracle Collaboration Suite components.

Once the installation is completed, the database will only contain Oracle Collaboration Suite-specific schemas. If you require the metadata repository to reside in the same database as the Oracle Collaboration Suite-specific schemas, then you must run RepCA.

Oracle Collaboration Suite interoperability with Oracle Application Server

This section contains the following topics.

Oracle Collaboration Suite Deployment with Existing Portal Users

This section contains the following topics.

Managing Portlets within an Existing Oracle Collaboration Suite Portal

When you deploy Collaborative Portlets on any Applications tier computer, you install Oracle10*g* Application Server Portal as part of the process. If you have already deployed Oracle10*g* Application Server Portal, however, you may not wish to override it with a new Portal installation. In such cases, you can deploy Collaborative Portlets without installing Oracle10*g* Application Server Portal and must manually configure the images later.

Deploying Collaborative Portlets without Installing a New Version of Portal

When you install Oracle Collaboration Suite, the installer provides you with the option to use an existing portal or create a new one. Choose the option to use an existing portal. As a result, a new version of portal is not installed on the Applications tier. If Collaborative Portlets are configured and a new Portal is not installed, then you must fix the images. If you are setting up a high availability environment, you must then run the Configure Component option in Oracle Enterprise Manager for each additional Applications tier computer and ensure that you only do this for Collaborative Portlets.

The Effect of an Oracle Collaboration Suite Deployment on Existing Portal Users

When you install Oracle Collaboration Suite, the installer replaces the default Portal home page with the most recent version if you have not changes the default settings. If you have customized the default Portal home page then the installer does not replace it with the most recent version.

Oracle Collaboration SuiteDeployment with Existing Oracle Internet Directory Users

This section contains the following topics.

Providing Oracle Collaboration Suite Accounts for Existing Oracle Internet Directory Users

When Oracle Collaboration Suite is installed on a system with existing Oracle Internet Directory users, those users can be bootstrapped into the application and can receive create events and modify events. If you want your existing Oracle Internet Directory users to receive Oracle Collaboration Suite accounts once the product is installed then ensure that the bootstrap is turned on. If you do not want your existing Oracle Internet Directory users to receive Oracle Collaboration Suite accounts once the product is installed then ensure that the bootstrap is turned off.

Adding the orcladmin User to the User Provisioning Admin Group

Oracle Internet Directory includes a special directory administrator with full access to directory information. The default user name of the super user is `orcladmin`. If you removed `orcladmin` from your deployment then you should add at least one user that you wish to have provisioning privileges to the User Provisioning Admin group.

Note: Instructions for performing this task can be found in the Oracle Internet Directory Administrator's Guide. Please see Chapter 5, Oracle Directory Server Administration.

The orclguest User

When you install Oracle Collaboration Suite Infrastructure an account, `orclguest`, is created that provides access to Oracle Collaboration Suite applications. If you are running Oracle Application Server and you have not installed Oracle Collaboration Suite Infrastructure then you must use another account to provision your applications.

Oracle Collaboration Suite Interoperability with Oracle Enterprise Manager Grid Control

Oracle Enterprise Manager Grid Control uses a central console and management agents to an organization's grid environment including repositories and applications-tiers, as well as Web applications, hosts, and the network in between. You can choose to provide your organization with a separate Oracle Enterprise Manager Grid Control deployment for Oracle Collaboration Suite or a site-wide Grid Control deployment that manages the entire environment, including Oracle Collaboration Suite.

This section discusses various options and best practices that you should consider when deploying Oracle Enterprise Manager Grid Control to manage Oracle Collaboration Suite.

Separation of Architectures

When planning your Enterprise Manager deployment, you should keep the Enterprise Manager framework components, such as the Management Service and the Management Repository, separate from your Oracle Collaboration Suite deployment. For example, you should install the Oracle Management Server on a separate host from your Oracle Collaboration Suite Applications tiers. Similarly, you should not use the Oracle Collaboration Suite database for the Management Repository. By keeping

these components separate, you can ensure that Enterprise Manager itself will not be affected by any performance problems on aOracle Collaboration Suite or host.

Installation Sequence

This section discusses installation sequence considerations for Oracle Enterprise Manager Grid Control and Oracle Collaboration Suite. In most cases you can install either Oracle Enterprise Manager Grid Control or Oracle Collaboration Suite first. However, if you are deploying Oracle Voicemail & Fax you must install Oracle Enterprise Manager Grid Control first.

Grid Control and Application Server Control for Collaboration Suite

When you install an Oracle Collaboration Suite Applications tier, an administration console is also installed. This console is called the Oracle Application Server Control for Collaboration Suite and enables you to administer that applications tier. Similarly, when you install the infrastructure, an administration console called Application Server Control is also installed to manage that infrastructure instance.

In contrast to the Application Server Control, the Grid Control Management Console, provides complete visibility across your entire Oracle Collaboration Suite deployment. Oracle Enterprise Manager Grid Control provides links that allow you to automatically launch the Application Server Control when needed.

Installing Oracle Collaboration Suite First

You can install Oracle Collaboration Suite before installingOracle Enterprise Manager Grid Control or the Management Agents, unless you are deploying Voicemail & Fax. In this case, you will then install the Management Agent on the Collaboration Suite host. When the Management Agent is installed it starts up and discovers the Oracle Collaboration Suite components running on that host. It also automatically discovers the host itself and any other components or targets that Enterprise Manager recognizes. You will then see this host and its targets in the Grid Control Console. These targets are automatically monitored once they are discovered.

Figure 4–1 Overview of Oracle Enterprise Manager Grid Control Deployment

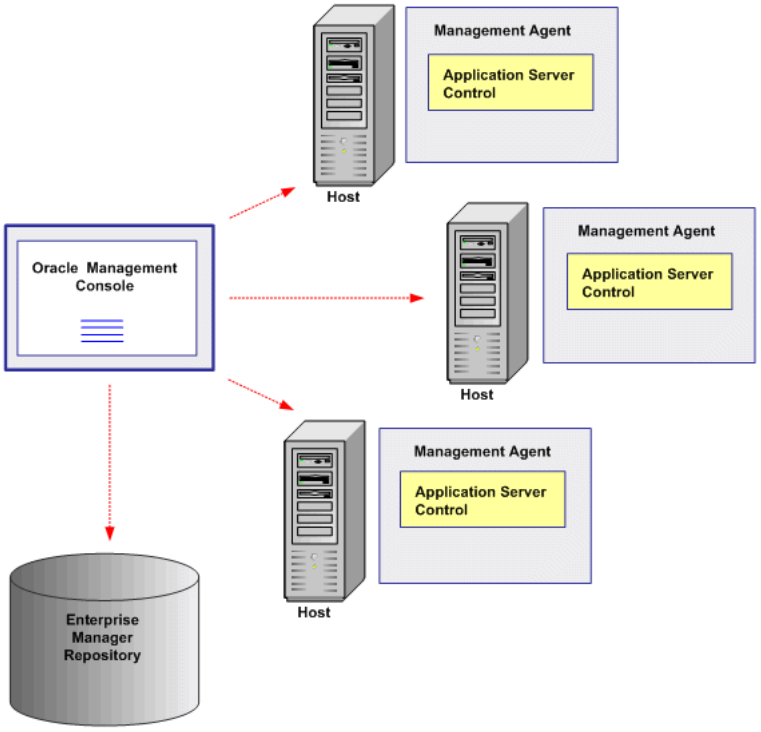


Figure 4–1 provides an overview of the Oracle Enterprise Manager Grid Control installation. In this figure there are three hosts, each of which represents an element of the organization's grid. An Oracle Enterprise Manager Grid Control management agent is installed on each host and the Oracle Management Console monitors each host through its management agent. The Oracle Management Console stores information on the Enterprise Manager repository.

Installing Oracle Enterprise Manager Grid Control First

If you are installing Oracle Collaboration Suite after Oracle Enterprise Manager Grid Control, then you must subsequently install the management agent on each Oracle Collaboration Suite host and then discover these hosts in the Oracle Management Console. You can discover the new Collaboration Suite components from either the Grid Control console or the Application Server Control for that Applications tier or infrastructure installation.

Figure 4–2 Oracle Enterprise Manager Grid Control Deployment with Oracle Collaboration Suite Components

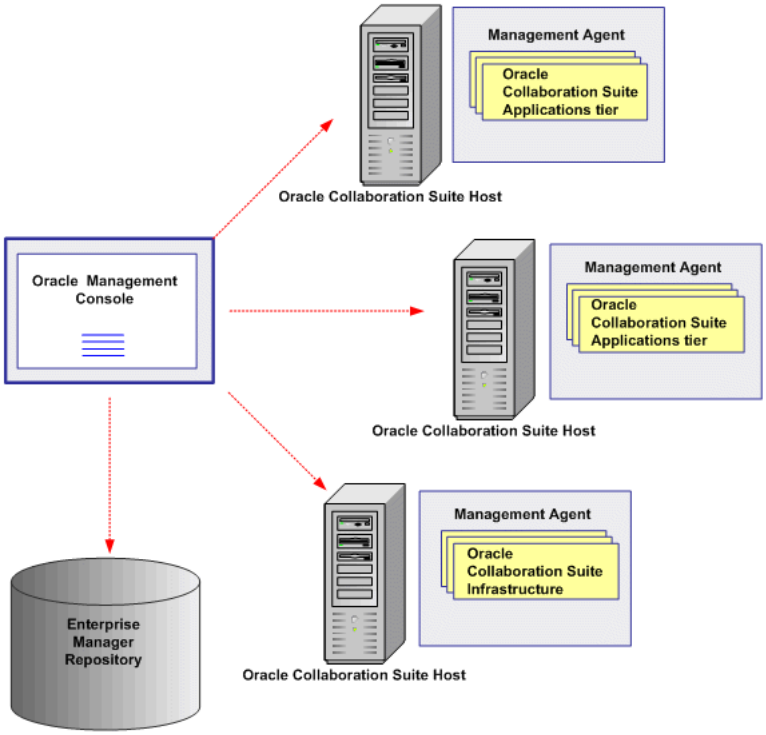


Figure 4–2 illustrates an Oracle Enterprise Manager Grid Control deployment across three Oracle Collaboration Suite hosts. The Oracle Management Console communicates with the hosts, each of which is running the Oracle Enterprise Manager Grid Control management agent. The management agent on two of the hosts is configured to run on the Oracle Collaboration Suite Applications tier while the management agent on the third host is configured to run on the Oracle Collaboration Suite Infrastructure tier. The Oracle Management Console stores relevant information in the Enterprise Manager Repository.

Grid Control Configuration for Collaboration Suite Components

Once the Oracle Collaboration Suite installation has been discovered by Grid Control, there are some additional steps to perform in the Grid Control Console. These steps are documented in *Oracle Enterprise Manager Managing Collaboration Suite*.

Using Identity Management with Oracle Enterprise Manager Grid Control

You can configure Oracle Enterprise Manager to use Oracle Identity Management. Administrators can login to Enterprise Manager using Single Sign-On and be authenticated and authorized through Oracle Internet Directory.

For information on configuring Enterprise Manager with Identity Management see the *Oracle Enterprise Manager Advanced Configuration Guide.*

Part II

Application-Level Deployment

Part II provides information to help you understand the deployment issues and available deployment options for individual Oracle Collaboration Suite components. Chapters include:

5

Deploying Oracle Calendar

This chapter contains the following topics:

Overview

Oracle Calendar is composed of the Oracle Calendar server, the Oracle Calendar application system and a variety of clients. This chapter provides conceptual and planning information for deploying the Oracle Calendar server, the Oracle Calendar application system and the various Oracle Calendar clients.

Understanding the Oracle Calendar Server and Oracle Calendar Application System Architecture and Functionality

This chapter provides conceptual and planning information for deploying the Oracle Calendar server and the Oracle Calendar application system.

Oracle Calendar Server and Oracle Calendar Application System Architecture

Oracle Calendar architecture contains two principle components, the Oracle Calendar application system and the Oracle Calendar server. Oracle Calendar is also deployed with Oracle Application Server components such as Web Cache, Oracle HTTP Server and Oracle Internet Directory. The Oracle Calendar server can be deployed with the Oracle Mail Server to support sending and receiving of calendar notifications by e-mail. However, the Oracle Calendar server can also be configured to use third-party SMTP processes to facilitate the sending of calendar information and notifications, regardless of which e-mail server is used in production.

Figure 5–1 Oracle Calendar Architecture

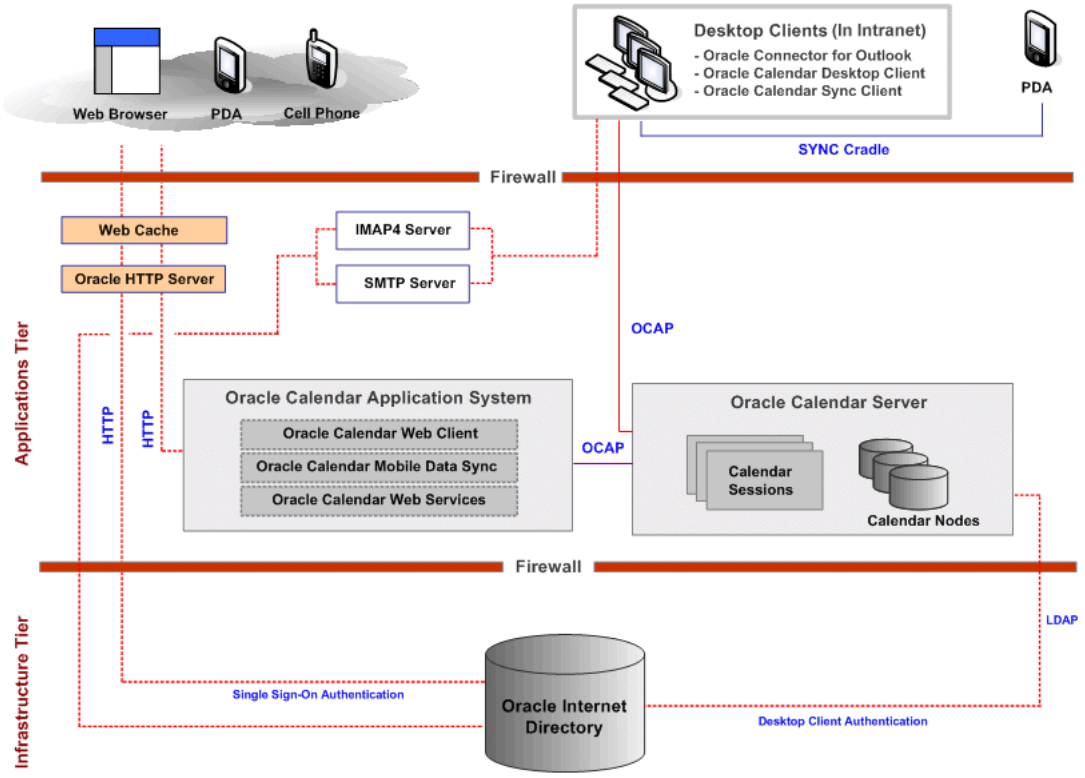


Figure 5–1 illustrates Oracle Calendar architecture. One important difference that distinguishes Oracle Calendar from other Oracle Collaboration Suite applications is that the Oracle Calendar server database is integrated into the application and therefore deployed on the Applications tier and typically not on the Infrastructure tier.

- Web Cache
- Oracle HTTP Server
- IMAP4 server
- SMTP server
- Oracle Calendar application system
- Oracle Calendar server

The Infrastructure tier contains Oracle Internet Directory.

Web-based clients such as browsers, PDAs, and cell phones connect to the Oracle Calendar server through the Web Cache and Oracle HTTP Server using the HTTP protocol. Oracle HTTP Server provides single sign-on authentication with Oracle Internet Directory and then directs the connection to the Oracle Calendar application system, which in turn connects to the Oracle Calendar server using the Oracle Calendar Access Protocol (OCAP).

Desktop clients such as Oracle Connector for Outlook, the Oracle Calendar desktop client, and the Oracle Calendar Sync client (connected to a desktop computer using a cradle) connect directly with the Oracle Calendar server using OCAP. The Oracle Calendar server authenticates desktop clients with Oracle Internet Directory using LDAP.

Note: The Oracle Calendar server and the Oracle Calendar application system have specific connection requirements that significantly impact deployment considerations. These requirements are discussed in the "Oracle Calendar Server Functionality" section.

Oracle Calendar Server

The Oracle Calendar server is the back end to an integrated suite of calendaring and scheduling products. Networked users can use a variety of desktop clients to manage their calendars. Mobile users can synchronize their agendas with a variety of PDAs or, with the addition of wireless technology of Oracle, can send and receive calendar entries using a mobile phone.

Figure 5–2 Oracle Calendar Server

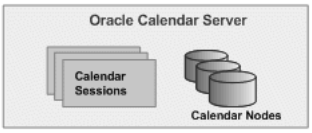


Figure 5–2 illustrates the Oracle Calendar server. In this figure, the Oracle Calendar server contains the following components:

Calendar Sessions

Calendar sessions are comprised of the listeners, processes and threads that perform specific Oracle Calendar operations. The components contained in a calendar session are described in the "Calendar server Architecture" section of Chapter 2 in the *Calendar Administrator's Guide*

Calendar Nodes

A calendar node is a calendar information database in which the server stores data such as user records, meetings, and events for a set of users. A server can host one or several nodes. Nodes may be connected into a node network, allowing users on different nodes (and servers) to schedule meetings and events transparently with one another. Each node has a specific, unique identification number called the Node-ID, which must be unique across a network of nodes.

When the Oracle Calendar server is installed, a node is automatically created and additional nodes can be added to the server. In order to group your users into nodes, logical divisions among your user base must be clearly delineated. Before making these decisions, however, the following factors must be considered:

- **Node size**

  The maximum capacity of an Oracle Calendar server node in terms of the number of users each node and the number of nodes each computer varies depending on a number of factors such as usage patterns, scheduling patterns, and regional deployment tissues. For more information see the "Planning for Oracle Calendar Server and Oracle Calendar Application System Deployment" section.

- **Network issues**

  Although server-to-server calendar communication requires low network bandwidth, in order to obtain acceptable performance for users accessing a remote server, a network bandwidth of 64 kbps or higher is suggested. If this is not possible, then you may want to consider installing a local server.

- **Scheduling between nodes**

  More server resources are required when scheduling meetings between users on different nodes in an Oracle Calendar node network. For this reason, it is a good practice to group users who work together on one node and thereby minimize the number of meetings involving users from other nodes.

- **User migration**

  Although it is possible to move individual users from node to node, the process can be lengthy and may alter or remove some information. Minimize the need to move individual users as a result of either reaching maximum node capacity, or the need to split a node according to logical divisions. For a more detailed discussion of the `unimvuser` utility, see Appendix E, "Utilities" of the *Oracle Calendar Reference Manual*.

- **Administrative considerations**

  While the bulk of the Oracle Calendar server administration can be performed remotely, there are tasks related to system maintenance that might require an on-site administrator. If you do not have personnel to manage back-up media and system problems at a branch office, then it is probably not a good idea to locate a server there.

  The time required to administer your calendar node network is also affected by the necessary repetition of some tasks. Certain features, such as holidays, are specific to each node. The tasks associated with these features, such as adding holidays, must be done separately on each node.

- **Directory System**

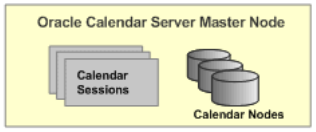
  Each node in a calendar node network that is linked to a directory server must point to the same directory server. When the Oracle Calendar server is deployed as part of Oracle Collaboration Suite, Oracle Internet Directory serves as the directory system. In a standalone deployment of the Oracle Calendar server, a directory system is optional and when present, all nodes in a network must use the same logical directory server.

Master Node

Each Oracle Calendar server deployment can contain only one master node. All clients connect to the master node on their first login. The master node then queries the directory server for identification and authentication. When the master node receives this information, it redirects the client to the appropriate server and node.

Clients use the master node to automatically route connections to the server and node that hosts the account of the user who is logging into the system. Upon connection to this centralized access point, the master node queries clients for identification. When the master node receives this information, it redirects the client to the appropriate server and a final, persistent network connection is made and maintained until the user terminates the session. You can optionally change the node that is designated as the master node and in case of large deployments, you can create an Oracle Calendar node or server dedicated exclusively to providing master node service.

Figure 5–3 Master Node



Oracle Calendar Application System

The Oracle Calendar application system is a framework for managing Oracle Calendar components or plug-ins through Web-based means. The features of Oracle Calendar are provided through Web-based applications by loading each of the components on startup.

Figure 5–4 Oracle Calendar Application System

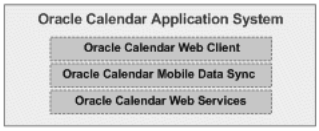


Figure 5–4 illustrates the Oracle Calendar application system. In this figure, the Oracle Calendar application system contains the following components:

- Oracle Calendar Web client
- Oracle Mobile Data Sync
- Oracle Calendar Web services

Oracle Calendar Web Client

The Oracle Calendar Web client enables users to share agendas, schedule meetings, and book resources and equipment.

Oracle Mobile Data Sync

Oracle Mobile Data Sync offers two-way direct synchronization with the Oracle Calendar server over any standard Hypertext Transfer Protocol (HTTP) connection, by opening up the calendar infrastructure to OMA-DS-compliant devices (formerly referred to as SyncML-compliant devices) or applications with Internet access. The Oracle Mobile Data Sync architecture can also be extended to support third-party standards-based or proprietary infrastructures.

Oracle Mobile Data Sync provides a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

Oracle Calendar Web Services

Oracle Calendar Web services enable applications to retrieve, through common XML queries, calendaring data for display in any portal, client application, or backend server. iCal data is coded in XML, wherein iCal becomes xCal. SOAP is used to encapsulate the messages for delivery. The calendaring data Web services SOAP is stored directly on the Calendar server store. This is in effect the CWSL, or Calendar Web Services Language.

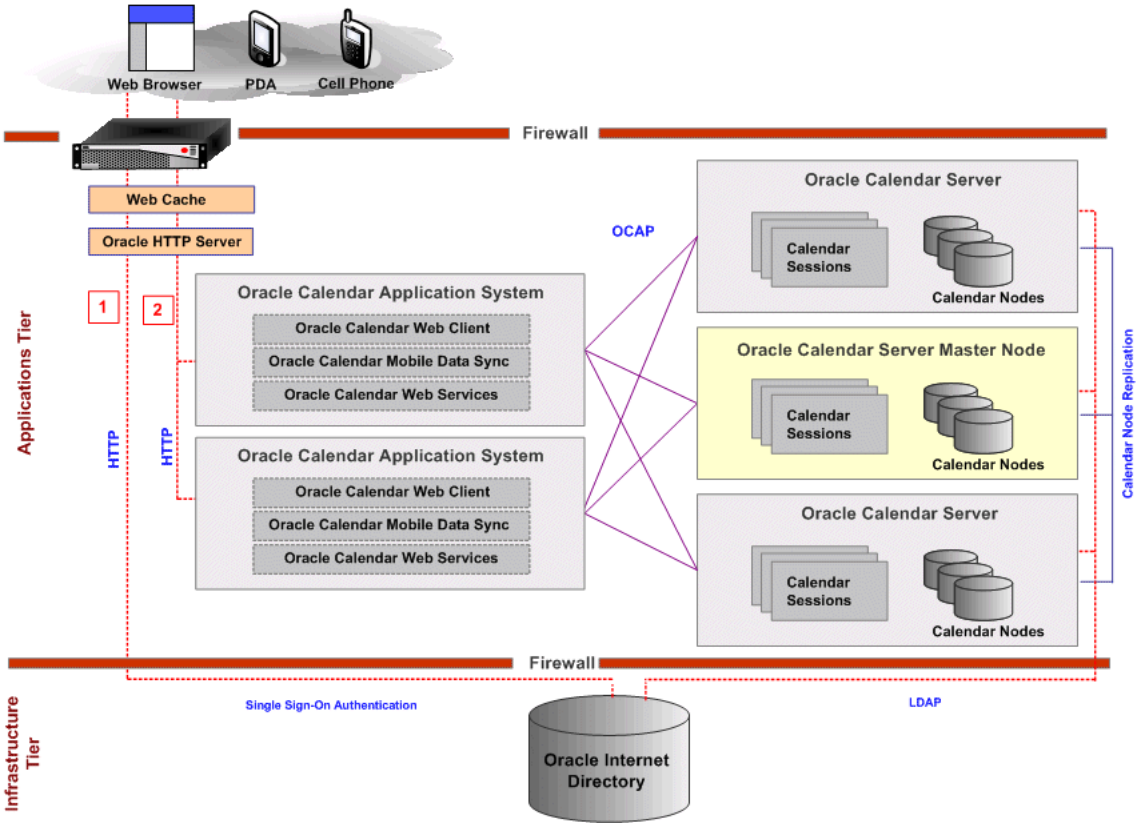
Oracle Calendar Server Functionality

This section describes Oracle Calendar server functionality with Oracle Calendar Web client and Oracle Calendar desktop client connections. The Oracle Calendar server has very specific configuration requirements to maintain successful connections with these types of connections.

Oracle Calendar Web Client Connections

Figure 5–5 illustrates how the Oracle Calendar Web client accesses the Oracle Calendar server.

Figure 5–5 Oracle Calendar Web Client Connections



In Figure 5–5, two instances of the Oracle Calendar application system and three instances of the Oracle Calendar server including a master node are deployed on the Applications tier in a DMZ and Oracle Internet Directory is deployed on the Infrastructure tier. Web browsers connects through a load balancer to the Web Cache and Oracle HTTP Server. Oracle HTTP Server first performs a single sign-on authentication against Oracle Internet Directory, and then sends an HTTP request to one of the Oracle Calendar application system instances. The Oracle Calendar application system instance sends the request to one of the Oracle Calendar server instances using OCAP.

Persistence is not required between the load balancer and the Oracle Calendar application system when a user is logging on. However, once the user has logged on, the load balancer must persistently send all user data to the appropriate Oracle Calendar application system instance. Persistence is required for single sign-on authentication, and, like all Oracle Collaboration Suite Web applications, the Oracle Calendar application system depends on single sign-on authentication. If the load balancer randomly sends information to another Applications tier, then authentication errors may occur. This is not the case for standalone Oracle Calendar installations, where single sign-on authentication is not used.

Connections Between the Oracle Calendar Application System and the Oracle Calendar Server

Each Oracle Calendar application system instance must maintain a fixed number of persistent, shared OCAP connections to each Oracle Calendar server instance. You cannot load balance the connections between the Oracle Calendar application system and the Oracle Calendar server.

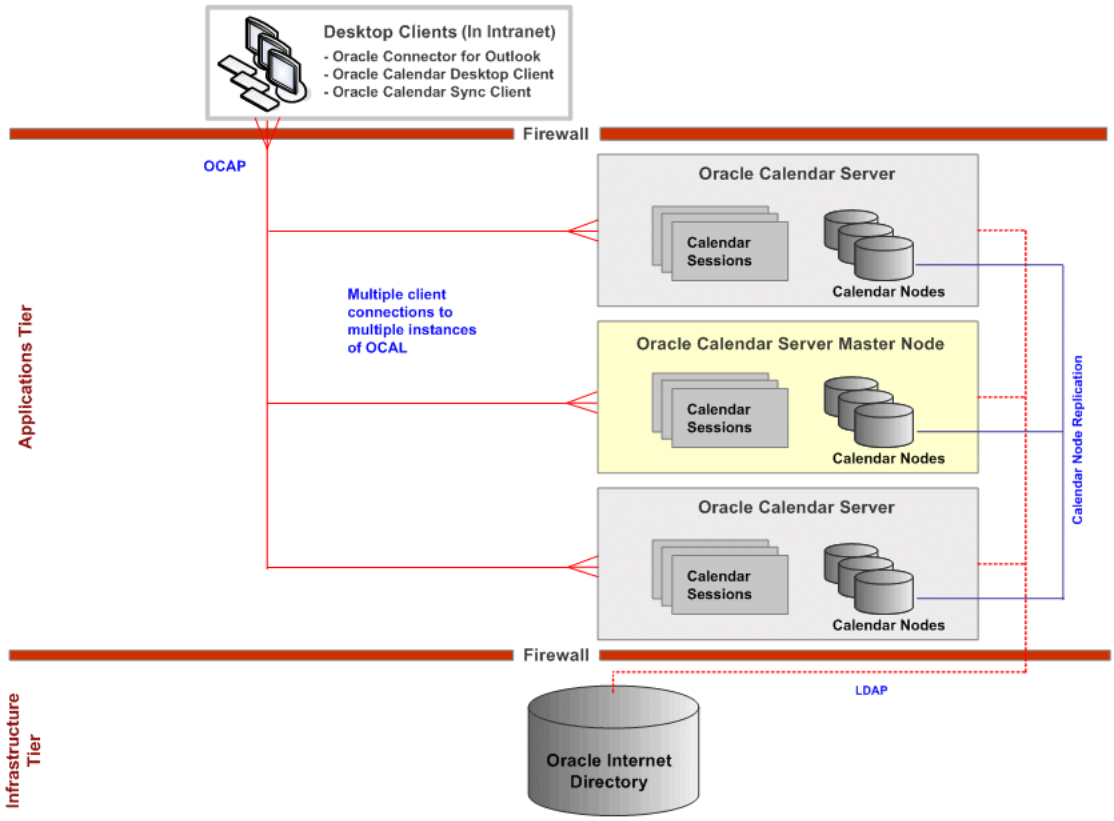
Connections Between clients and the Oracle Calendar Application System

Connections between the clients and the Oracle Calendar application system are neither a fixed number, shared, nor persistent and consequently can be load balanced.

Desktop Client Connections

Figure 5–6 illustrates how desktop clients access the Oracle Calendar server.

Figure 5–6 Oracle Calendar Server Desktop Client Connections



In Figure 5–6, multiple desktop clients connect to multiple instances of the Oracle Calendar server using fixed, persistent OCAP connections. The Oracle Calendar server updates user information by accessing Oracle Internet Directory using an LDAP connection. Data is not replicated between Oracle Calendar server instances and only information needed for a local node of a user is replicated. Because users exist on only one node and data is not replicated or shared between Oracle Calendar server instances, the connections to the Oracle Calendar server cannot be load-balanced.

Planning for Oracle Calendar Server and Oracle Calendar Application System Deployment

This section discusses issues and requirements for planning an Oracle Calendar server deployment.

Users of Oracle Calendar Server

Planning for an Oracle Calendar deployment requires an understanding of the number of Oracle Calendar users. This information varies according to different categories.

Number of Users of Oracle Calendar

The recommended capacity each node and each server is heavily dependent on hardware, the expected usage pattern of the service, and the type of clients to be used. A small, economical, or older host may only be able to functionally handle 500 or 1,000 accounts, whereas a large, enterprise class computer could easily accommodate three or four nodes each serving over 5,000 users.

For an organization that heavily uses scheduling, deployment should not exceed 10,000 users each host, whereas for an organization with a modest usage pattern over 20,000 users may be deployed on the same host. An environment deploying Oracle Calendar desktop clients (Windows, Mac, Linux, Solaris) and Oracle Connector for Outlook could provide calendar service for up to 10,000 users on a single computer, whereas an environment consisting only of the Oracle Calendar Web client would be able to host well over 20,000 users on the same resource.

Configured Users

Configured users are individuals with user accounts on an Oracle Calendar server node.

Logged-On Users

Logged-on users are user who are connected to a node but who are not actively making database requests. This figure is generally estimated to be from 33–50% of configured users. Try to forecast how your users will use the calendar application. For example, if everyone starts work at the same time, you might anticipate a period of peak usage in the morning where up to 60% of all users will be logged on at once. Also, a number of users may choose to stay logged on all day, keeping the calendaring application open in the background to permit quick and frequent access.

Active Users

Active users are logged-on users who make database access request. To estimate the number of active users at any time, take 10–15% of the total number of configured users. As with logged-on users, base this number on your highest estimate of peak usage.

Oracle Calendar Server Usage Patterns

You can optimize Oracle Calendar server performance by deploying groups of users that share complimentary usage patterns on the same calendar node. For example, an organization's Chicago office is expected to steadily decrease as its sales force is relocated to the New York office. Deploying the users from both offices on the same node reduces the administrative time required for managing two nodes. Having users

in two different time zones on the same node requires a minor configuration change for the Chicago users to enable them to set their time zone from the client.

Oracle Calendar Server Regional Deployments

Depending on the size and distribution of your organization, you may want to deploy the Oracle Calendar server according to usage patterns based on geography and time zones. You may want to have users of one geographic region share the same nodes as users of another geographic region if time differences ensure that neither group of users will be active at the same time.

Oracle Calendar Server Client Access Considerations

Because Oracle Calendar has a large number of clients, the type of clients accessing the Oracle Calendar server can significantly impact your deployment. If most of the connections are through the Oracle Calendar Web client, then most of the stress will take place on the tier that contains Web Cache, Oracle HTTP Server, and the Oracle Calendar application system. Consequently this is the portion of your deployment that you may need to scale first. If the majority of your connections are through Oracle Calendar desktop clients, then most of the stress will be on Oracle Calendar servers because these clients establish and maintain connections to (and persistent sessions on) the Oracle Calendar servers. So as your user base grows, you may need to scale the Oracle Calendar server portion of your deployment to accommodate an increased number of direct client connections to the Oracle Calendar server.

Oracle Calendar Server Scheduling Patterns

You can optimize your Oracle Calendar server deployment users based on geographic location or by functional groups. By grouping users that often schedule each other onto the same node, you will both reduce the network traffic between servers and also the data replicated between nodes.

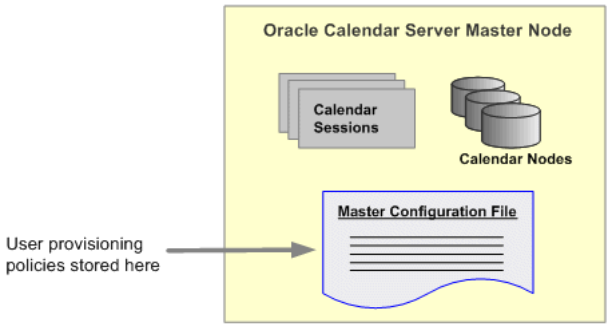
For example, while an organization's Sales and Financing departments have completely different functional areas, they may collaborate on numerous projects for which they share the same scheduling. For example, the Sales department may work with the Financing department to produce attractive new financing packages that they can offer to customers when selling their products. If the calendaring information for each department is stored on the same node, then there will be no need for frequent data replication between them.

Oracle Calendar Server Provisioning Policies

The Oracle Calendar server stores user provisioning policies in the master configuration file on the master node. In the default Oracle Calendar server installation, all user provisioning is handled by the master node. The first and most important step in a large deployment is to change your provisioning policies as required by making any necessary changes in the master configuration file.

> **See Also:** "Calendar User Account Provisioning" in Chapter 7 of *Oracle Calendar Administrator's Guide*

Figure 5–7 Master Configuration File



Oracle Calendar Installation Notes

Ensure that you complete all of the instructions in the *Oracle Collaboration Suite Installation Guide*.

> **See Also:** For information on installing Oracle Calendar, see the following guides:
>
> - *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
> - *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

Distributed Installations

Multiple instances of Oracle Calendar can be installed on the same Unix or Linux host (not on Windows). By default, each instance of Oracle Calendar is installed with all its components on the same host. This includes the following components:

- Oracle Calendar server
- Oracle Calendar Administrator
- Oracle Mobile Data Sync
- Oracle Calendar Web client
- Oracle Calendar Web services
- Oracle Calendar SDK

If you wish to run different components on different hosts (for example, to run the Oracle Calendar application system on a different host than the Oracle Calendar server), then you must keep the following in mind.

- When the Oracle Calendar server is installed in a standalone mode, Oracle Calendar Web clients identify themselves to the Oracle Calendar server using a shared key stored in both the Oracle Calendar application system and server configuration files. This shared key must match exactly across all Oracle Calendar application system and server instances. As this key is generated automatically by the installation procedure, and is different for each install, you will have to perform this configuration manually.
- If you wish to spread the user base of a deployment across multiple calendar server nodes on the same host or distributed across multiple hosts, then you must connect the nodes into a network.

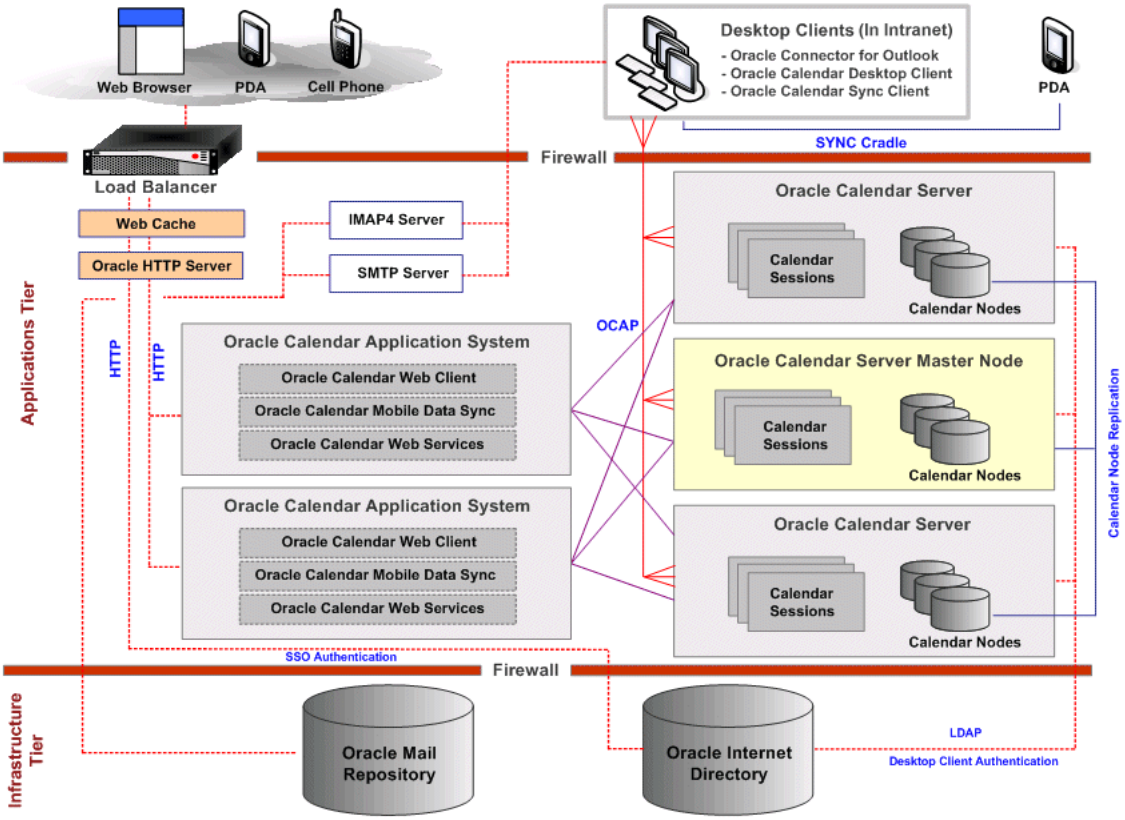
Oracle Calendar Server and Oracle Calendar Application System Deployment Configurations

This section describes available Oracle Calendar server deployment configurations and explains the advantages and disadvantages of each one.

Oracle Calendar Server Deployed in the Applications tier

Unlike other Oracle Collaboration Suite applications, the Oracle Calendar server database is deployed on the Applications tier by default. Figure 5–8 illustrates a typical Oracle Calendar server deployment with multiple Oracle Calendar application system and Oracle Calendar server hosts.

Figure 5–8 Deploying Oracle Calendar Server in the Applications Tier



Applications Tier

In Figure 5–8, the Applications tier is located in a DMZ with a load balancer for Web clients. The following components are deployed on the Applications tier:

- Web Cache
- Oracle HTTP Server
- Two Oracle Calendar application system hosts
- Three Oracle Calendar application system hosts
- IMAP4 Server
- SMTP Server

Infrastructure Tier

In Figure 5–8, the Infrastructure tier contains the Oracle Mail repository and Oracle Internet Directory.

HTTP Connections

In Figure 5–8, clients such as browsers, PDAs (using OMA-DS), and mobile devices connect to the Oracle Calendar server through Web Cache and Oracle HTTP Server using the HTTP protocol. Oracle HTTP Server provides single sign-on authentication with Oracle Internet Directory and then directs the connection to the Oracle Calendar application system, which in turn connects to the Oracle Calendar server using OCAP.

Each Oracle Calendar application system instance must maintain a fixed number of persistent, shared OCAP connections to each Oracle Calendar server instance. Connections between clients and the Oracle Calendar application system are neither a fixed number, shared, nor persistent, and consequently can be load balanced.

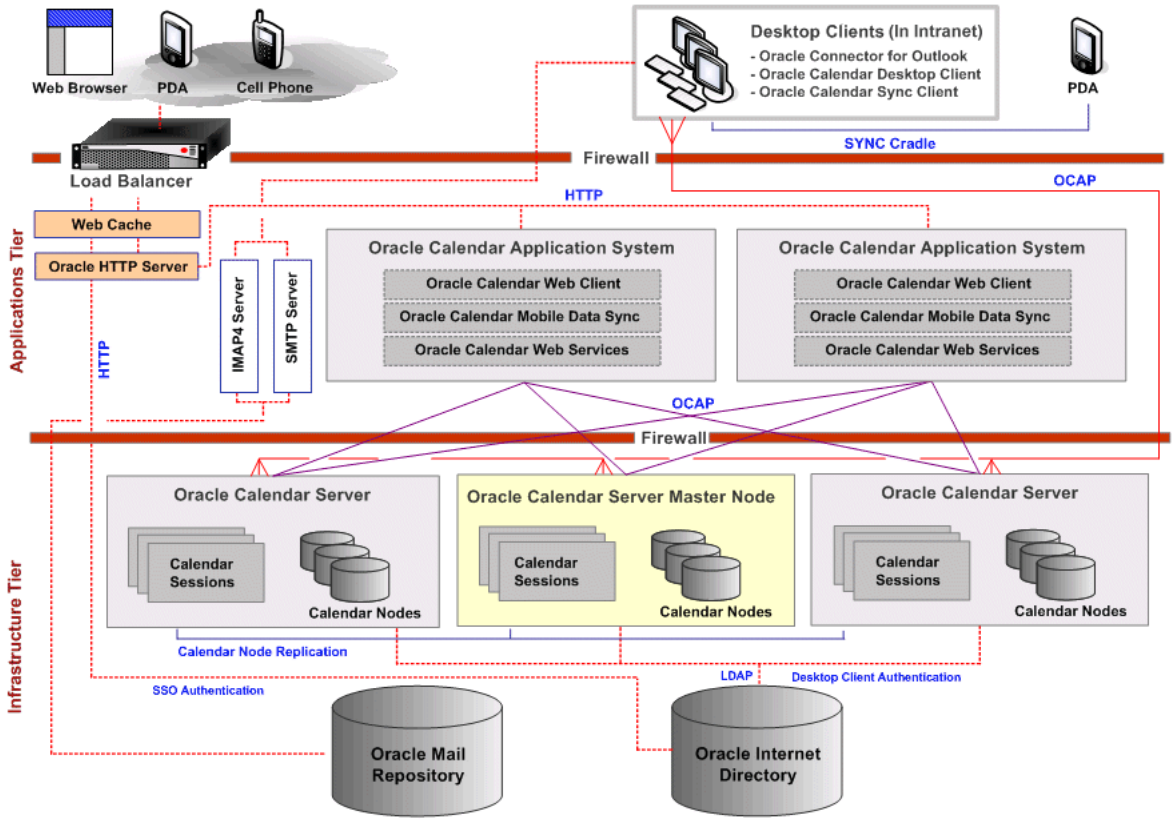
Desktop Client Connections

Desktop clients such as Oracle Connector for Outlook, the Oracle Calendar desktop client, and the Oracle Calendar sync client (connected to a desktop computer through cradle) connect directly with the Oracle Calendar server using OCAP. The Oracle Calendar server authenticates desktop clients with Oracle Internet Directory using LDAP.

Oracle Calendar Deployed in the Infrastructure tier

You can optionally deploy the Oracle Calendar server on the Infrastructure tier. Regardless of where the Oracle Calendar server is installed, attention should be given to RAID options to achieve reliable storage and performance. Figure 5–9 illustrates this deployment configuration.

Figure 5–9 Deploying Oracle Calendar Server in the Infrastructure Tier



Applications Tier

In Figure 5–9, the Applications tier is located in a DMZ with a load balancer for the Oracle Calendar Web client but not for Oracle Calendar desktop clients. The following components are deployed on the Applications tier:

- Web Cache
- Oracle HTTP Server
- Two Oracle Calendar application system hosts
- IMAP4 Server
- SMTP Server

Infrastructure Tier

In Figure 5–9, the following components are deployed on the Infrastructure tier:

- Three Oracle Calendar server hosts
- Oracle Mail repository
- Oracle Internet Directory

In this configuration, firewall ports must be open to enable OCAP connections from the Applications tier to the Infrastructure tier. If a load balancer is being used on the Infrastructure tier firewall, make sure that it does not load balance calendar connections (i.e. connections to the Oracle Calendar server DNS host name or port numbers) because it will disrupt the persistent shared OCAP connections, causing calendar operations to fail. Note that the only advantage of having the calendar

database on the infrastructure is to take advantage of storage configurations and failover configurations.

HTTP Connections

In Figure 5–9, HTTP or HTTPS-based clients such as browsers, PDAs (using OMA-DS, formerly known as SyncML), and mobile devices connect to the Oracle Calendar server through Web Cache and Oracle HTTP Server using the HTTP protocol. Oracle HTTP Server provides single sign-on authentication with the Oracle Internet Directory and then directs the connection to the Oracle Calendar application system, which in turn connects to the Oracle Calendar server using OCAP.

Each Oracle Calendar application system instance must maintain a fixed number of persistent, shared OCAP connections to each Oracle Calendar server instance. Connections between clients and the Oracle Calendar application system are neither a fixed number, shared, nor persistent and consequently can be load balanced.

Desktop Client Connections

Desktop clients such as Oracle Connector for Outlook, the Oracle Calendar desktop client, and the Oracle Calendar Sync client (connected to a desktop computer through a cradle) connect directly with the Oracle Calendar server using OCAP. The Oracle Calendar server authenticates desktop clients with Oracle Internet Directory using LDAP.

Deploying the Oracle Calendar Web Client and Oracle Calendar Web services

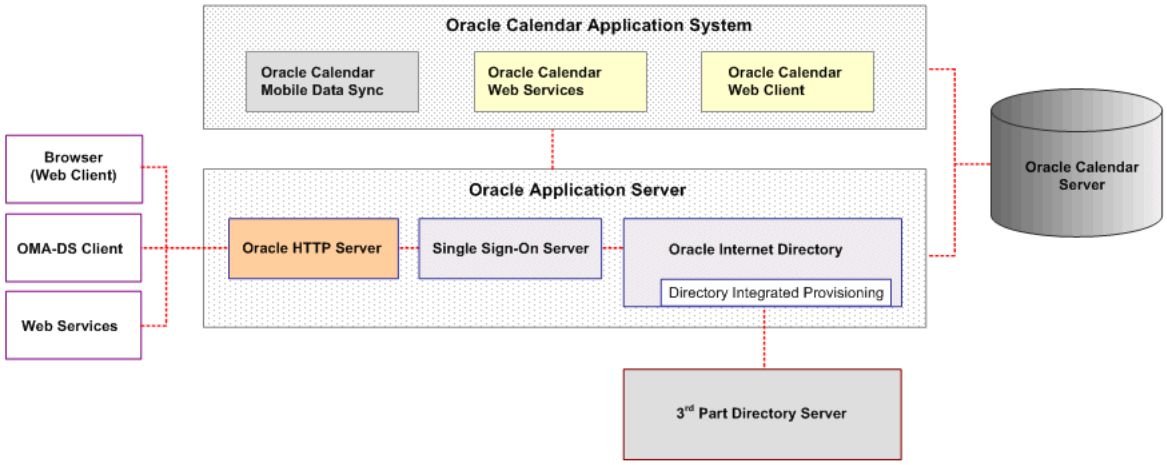
This section contains the following topics:

- Oracle Calendar Web Client and Oracle Calendar Web Services Architecture
- Oracle Calendar Web Client and Oracle Calendar Web Services Standalone Installation Notes
- Oracle Calendar Web Client and Oracle Calendar Web Services Sizing and Memory Use
- Oracle Calendar Web Client and Oracle Calendar Web Services Deployment and Maintenance

Oracle Calendar Web Client and Oracle Calendar Web Services Architecture

The Oracle Calendar Web client and Oracle Calendar Web services are both part of the Oracle Calendar application system, as illustrated by the following diagram.

Figure 5–10 Oracle Calendar Web client and Oracle Calendar Web services



Notes:

This section describes Oracle Calendar Web client and Oracle Calendar Web services deployment, rather than Oracle Calendar application system deployment as a whole. The deployment of the other component of the Oracle Calendar application system (Oracle Mobile Data Sync) is described separately in "Deploying Oracle Mobile Data Sync".

For more information on Oracle Calendar application system architecture, see the following sections:

- "Understanding the Oracle Calendar Server and Oracle Calendar Application System Architecture and Functionality"
- "Planning for Oracle Calendar Server and Oracle Calendar Application System Deployment"
- "Oracle Calendar Server and Oracle Calendar Application System Deployment Configurations"

Oracle Calendar application system components are FastCGI-based. The Oracle Calendar application system connects to the back-end datastore, the Oracle Calendar server.

When you deploy an instance of the Oracle Calendar application system on an Applications tier, all three of its components are included. You may want to disable certain components, depending on how the Applications tier is positioned in your architecture, and whether or not you want certain components to be accessible externally. (For details on disabling components of the Oracle Calendar application system, see Customizing OCAS Components in Chapter 3 of *Oracle Calendar Administrator's Guide*.)

For example, the Oracle Calendar Web client and Oracle Calendar Web services could be enabled only on Applications tiers behind the DMZ for internal use by your organization. In such a setup, external access would require users to tunnel through to these tiers using a VPN client.

Alternatively, you could enable the Oracle Calendar Web client on Applications tiers within the DMZ while making sure it is adequately protected with SSL and a firewall. In such a setup, you may choose to disable access to Oracle Calendar Web services on these tiers if there is no need for external access.

> **Note:** In order for the Oracle Collaboration Suite Portal Calendar portlet to function properly, the Portal must have access to Oracle Calendar Web services.

If you have a large number of users, you will likely be deploying two to four Applications tiers with a load balancer. When load balancing, ensure that alternate domains such as *webclient*`1.oracle.com` and *webclient*`2.oracle.com` are not used, as the Oracle Calendar application system does not support this. The domain name must remain consistent.

Oracle Calendar Web Client and Oracle Calendar Web Services Standalone Installation Notes

Standalone installations of Oracle Calendar support the following versions of Apache with `mod_fastcgi`.

- Apache 1.3.26 and later with `mod_fastcgi 2.2.12`
- Apache 2.0.53 and later with `mod_fastcgi 2.4.2`

While the preceding versions of `mod_fastcgi` have been tested and are known to work with their associated Apache version, newer versions of `mod_fastcgi` versions will also likely work as they are developed.

Download the appropriate software from `http://www.apache.org/` and `http://www.fastcgi.com/`.

Oracle Calendar Web Client and Oracle Calendar Web Services Sizing and Memory Use

An Oracle Calendar application system instance that does not include Oracle Mobile Data Sync has no permanent memory requirements, as data is stored on the backend Calendar server. For Oracle Calendar application system instances that do include Oracle Mobile Data Sync, see Oracle Mobile Data Sync Sizing and Memory Use.

The main requirements to consider when planning a deployment of the Oracle Calendar Web client and Oracle Calendar Web services are the number of FastCGI processes to run, the amount of RAM needed to run them, and the number of Applications tiers available to run them on. These factors are interrelated and are described in the following sections.

- RAM, FastCGI Processes and Concurrency
- Example
- Determining the Best Setup for Your Organization

RAM, FastCGI Processes and Concurrency

The amount of RAM required by the Oracle Calendar Web client or Oracle Calendar Web services is directly connected to the number of FastCGI processes running on an Applications tier. Each FastCGI process requires approximately 20 to 30 MB of RAM. The number of FastCGI processes you need depends on how many users you have,

and, more specifically, how many of those concurrently use the Oracle Calendar Web client or Oracle Calendar Web services.

Each FastCGI process can handle three to four requests each second (numbers will vary depending on hardware and load). In other words, you need one FastCGI process for every three to four concurrent connections. The total number of FastCGI processes can be spread across multiple Applications tiers running the Oracle Calendar Web client or Oracle Calendar Web services. These processes must be considered in addition to the number allocated for Oracle Mobile Data Sync, as described in Oracle Mobile Data Sync Sizing and Memory Use.

Example

Imagine that Vision Corporation has 50,000 users, and that number is broken down as follows:

- **Total Users (including desktop client, Oracle Connector for Outlook and Oracle Calendar Web client users)**: 50,000
- **Expected Oracle Calendar Web client users**: 10,000

Vision Corporation's users must adhere to a defined 9:00 a.m. to 5:00 p.m. schedule, so almost all of these 10,000 Oracle Calendar Web client users will sign in and access their calendar within the first thirty minutes of the work day. On a busy day, this could occur during the first ten minutes.

- **Peak concurrency (users each second)**: (10,000 requests) / (10 minutes) = 1000 requests each minute, or 16.67 requests each second.
- **Number of FastCGI processes needed**: (16.67 requests each second) / (3.5 requests each second each FastCGI process) = 4.76

If Vision Corporation is running Oracle Collaboration Suite on two Applications tiers for load balancing and redundancy, then the default of five FastCGIs on each tier should be more than enough to handle any extreme peak periods.

Because a FastCGI process requires 20 to 30 MB of RAM, each tier would require about 125 MB of RAM for the Web client.

Determining the Best Setup for Your Organization

In the preceding section, the example and its calculations are provided as a guideline for you to determine the needs of your own organization. You may have many more Oracle Calendar users, but less chance of concurrent use, especially if members of your organization are working in different time zones.

The number of FastCGIs required for your organization depends on Oracle Calendar Web client use patterns. Also, you should only run as many FastCGI processes as are necessary, so as not to impact other applications running on the tiers.

A general starting point is to assume that at peak, 0.5% to 5.0% of Calendar users will concurrently use the Oracle Calendar Web client at any given time. In environments where only the Oracle Calendar Web client is available and users are active within the same time period, concurrency will be near the top of the range. In a geographically dispersed environment where all the desktop clients are available, concurrency will be near the bottom of the range.

Experiment with your architecture to determine the optimum settings for your needs. Check the Oracle HTTP Server `error.log` for messages indicating FastCGI overload, such as:

- `Resource temporarily unavailable: FastCGI: failed to connect to server`
- `FastCGI: comm with server "server_path" aborted`

You should only run as many FastCGI processes as are necessary, in case there are other applications sharing tiers with the Oracle Calendar Web client and Oracle Calendar Web services. For information on setting the number of FastCGI processes, see *Oracle Calendar Administrator's Guide*.

Oracle Calendar Web Client and Oracle Calendar Web Services Deployment and Maintenance

This section only provides a high-level overview of some post-installation tasks for the Oracle Calendar Web client and Oracle Calendar Web services. Consult *Oracle Calendar Administrator's Guide* for detailed instructions on managing, configuring and maintaining all components of Oracle Calendar.

By default, Oracle Calendar Web client and Oracle Calendar Web services are enabled on an installation of the Oracle Calendar application system. To disable them, comment out the appropriate sections of `ocas.conf`, as described in Customizing Oracle Calendar application system Components in Chapter 3 of *Oracle Calendar Administrator's Guide*.

Use Oracle Enterprise Manager to stop and start the Oracle Calendar Web client and Oracle Calendar Web services.

You can also manage the Oracle Calendar Web client and Oracle Calendar Web services using the following commands in `$ORACLE_HOME/ocas/bin/`.

- To start the Oracle Calendar Web client and Oracle Calendar Web services (if they are enabled on an Applications tier) enter the following command:

  ```
  ocasctl -start -n FastCGI_processes
  ```

  Where *`FastCGI_processes`* is the number of FastCGI processes you want to run on that tier.

- To stop the Oracle Calendar Web client and Oracle Calendar Web services enter the following command:

  ```
  ocasctl -stopall
  ```

Deploying Oracle Mobile Data Sync

This section contains the following topics:

- Oracle Mobile Data Sync Devices
- Oracle Mobile Data Sync Architecture
- Oracle Mobile Data Sync Sizing and Memory Use
- Oracle Mobile Data Sync Deployment and Maintenance

Oracle Mobile Data Sync Devices

One of the keys to planning a successful Oracle Mobile Data Sync deployment is to make sure that members of your organization use supported mobile devices. Oracle Mobile Data Sync is built around the OMA-DS (Open Mobile Alliance Data Synchronization, formerly known as SyncML) standard, and while any device built to

this standard should work with Oracle Mobile Data Sync, it is best to use devices tested and certified by Oracle. A list of such devices, along with configuration instructions, is published on the Oracle Technology Network site here:

http://www.oracle.com/technology/products/cs/user_info/omobile_collaboration/html/mobile_data_sync_get_started.html

Ensure that users in your organization have access to this site, as it contains important information and is updated regularly.

Another important site for Oracle Mobile Data Sync users is the Troubleshooting and FAQ page, located at the following URL:

http://www.oracle.com/technology/products/cs/user_info/omobile_collaboration/mobile_data_sync_index.html

This site provides answers to commonly asked questions about synchronization technology and how it is implemented in Oracle Mobile Data Sync.

If secure synchronization of data is a high priority for your organization, then use devices that support SSL synchronization. The list of devices on the Oracle Technology Network site specifies which support SSL synchronization. Oracle Mobile Data Sync supports SSL connections that are properly configured on the appropriate port during Oracle Collaboration Suite installation and configuration.

Another issue to consider when choosing devices is that they have varying degrees of support for traveling through different time zones. This is important for members of your organization who might be traveling a great deal. Information on this is also available on the Oracle Technology Network site.

By default, Oracle Mobile Data Sync will allow any OMA-DS-compliant device to connect to it and synchronize. However, you can configure the server to only accept connections from supported devices of your choice. For more information, see Oracle Mobile Data Sync Administrative Tasks in Chapter 3 of *Oracle Calendar Administrator's Guide*.

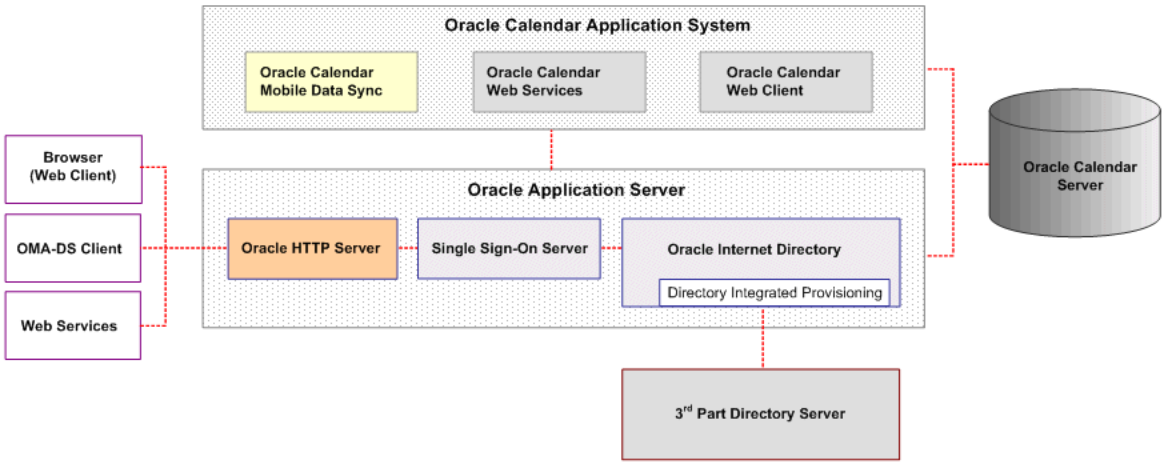
Oracle Mobile Data Sync Architecture

This section contains the following topics:

Oracle Mobile Data Sync and the Oracle Calendar Application System

Oracle Mobile Data Sync is deployed as part of the Oracle Calendar application system, as illustrated in the following diagram.

Figure 5–11 The Oracle Calendar Application System and Oracle Mobile Data Sync



Notes:

This section describes Oracle Mobile Data Sync deployment, rather than Oracle Calendar application system deployment as a whole. The deployment of the other components of the Oracle Calendar application system (the Oracle Calendar Web client and Oracle Calendar Web services) is described separately in "Deploying the Oracle Calendar Web Client and Oracle Calendar Web services".

For more information on Oracle Calendar application system architecture, see the following sections:

- "Understanding the Oracle Calendar Server and Oracle Calendar Application System Architecture and Functionality"
- "Planning for Oracle Calendar Server and Oracle Calendar Application System Deployment"
- "Oracle Calendar Server and Oracle Calendar Application System Deployment Configurations"

Like the other two Oracle Calendar application system components, Oracle Mobile Data Sync is FastCGI-based and connects to the backend datastore, the Oracle Calendar server.

When you deploy an Oracle Calendar application system instance, all three of its components are included. If you do not plan on making the Oracle Calendar Web client and Oracle Calendar Web services available externally, then you should consider dedicating an Oracle Calendar application system tier to Oracle Mobile Data Sync, with the other components disabled, and placing this tier inside the DMZ so that it is accessible by external devices. The Oracle Calendar Web client and Oracle Calendar Web services components can be deployed on other Oracle Calendar application system instances behind, or inside the DMZ.

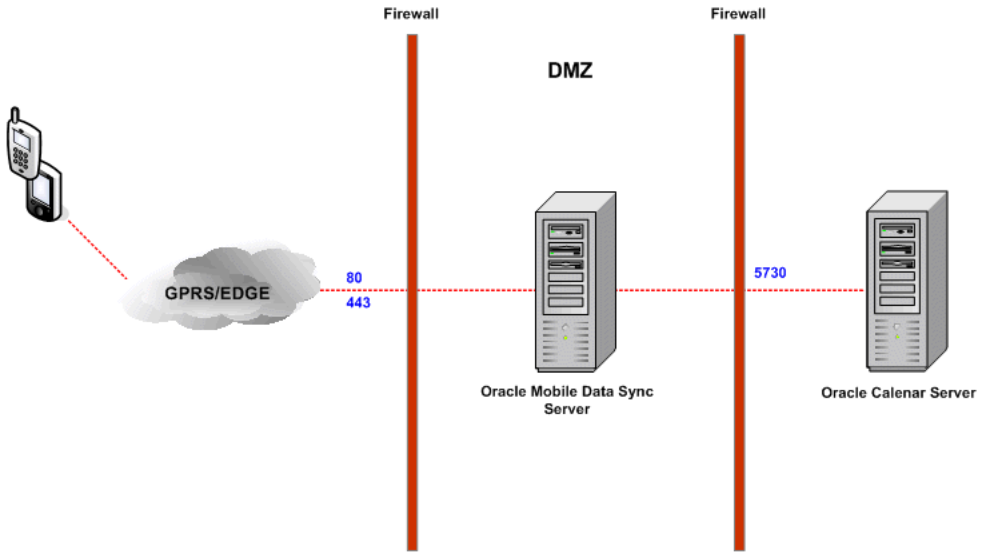
Oracle Mobile Data Sync must be directly accessible by devices and not through Oracle Application Server Single Sign-On. The Oracle Collaboration Suite installation program provides a Oracle Mobile Data Sync access point that is not protected by Oracle Application Server Single Sign-On, so no extra configuration is required for

this. The default URL for Oracle Mobile Data Sync is `http://your-domain.com/ocst-bin/ocas.fcgi`. Check `ocal.conf` to confirm the actual address for your organization.

Oracle Mobile Data Sync Ports and Connections

As it is best to make Oracle Mobile Data Sync externally accessible, and as Applications tiers are usually installed inside a corporate network behind a firewall, the Applications tier containing the Oracle Calendar server port (OCAL port) must be open to the Oracle Mobile Data Sync server. The default is port 5730, but the port number can be obtained from the ports list Web page in Oracle Collaboration Suite Control For more information, see "Checking Oracle Collaboration Suite Port Numbers" in Chapter 1 of *Oracle Collaboration Suite Administrator's Guide*.

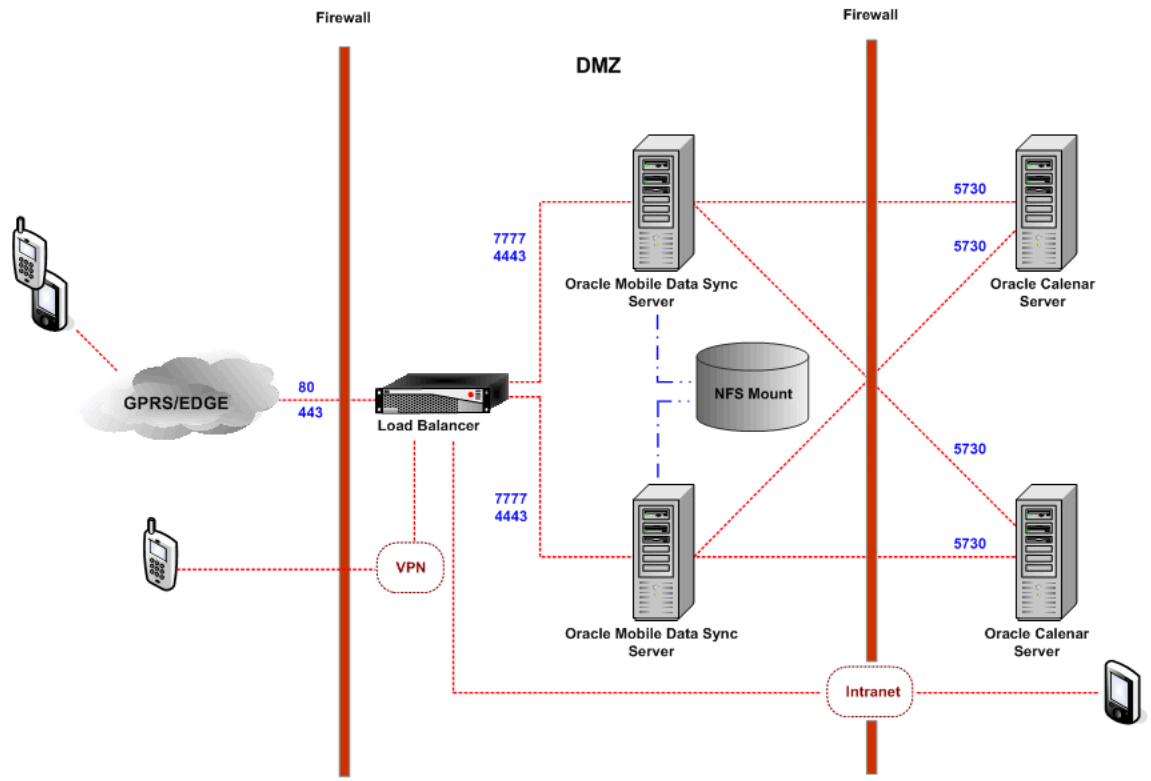
Figure 5–12 Oracle Mobile Data Sync ports and connections



In the preceding diagram, the Oracle Mobile Data Sync server resides in the DMZ and accepts SSL and non-SSL connections over ports 443 and 80, respectively. The Oracle Mobile Data Sync server connects to the Oracle Calendar server, which is behind the DMZ. The Oracle Calendar server listens for Oracle Mobile Data Sync requests on port 5730.

A more complex, but real-world deployment of Oracle Mobile Data Sync would look similar to the following illustration.

Figure 5–13 Oracle Mobile Data Sync common deployment



In the preceding illustration, all sync clients connect to a load balancer in the DMZ. The load balancer accepts SSL and non-SSL connections, then redirects these connections to ports 4443 and 7777, respectively, as non-SSL data (protected in the DMZ) on the Oracle Mobile Data Sync servers. These share a common NFS mount for storage of synchronization information (as described in the next section), and connect to Oracle Calendar servers behind the DMZ. The Oracle Calendar servers listen for Oracle Mobile Data Sync requests on port 5730.

Internal users of PDAs connect to the load balancer through the intranet, while external users of mobile devices can tunnel in to the network using VPN. External users of PDAs and mobile devices can also connect through GPRS or EDGE protocols to the URL of the load balancer.

Oracle Mobile Data Sync Tiers and Storage of Synchronization Information

By default, each Oracle Mobile Data Sync Applications tier stores the following information in its own respective internal location:

- **Session database**: This contains the information used during a synchronization session. In other words, it is a location to store messages that are passed between the device and server during a device synchronization.
- **Links database**: This contains the information maintained for all synchronizations, such as device time zones, last recorded synchronizations, device-ID to server-ID mappings, and so on.

If you have multiple Oracle Mobile Data Sync tiers, then you must point them all to a central, unified location to store this information, such as an NFS mount or a datastore (network appliance). Failure to do this can result in many unnecessary slow (full)

synchronizations. See Oracle Mobile Data Sync Administrative Tasks in Chapter 3 of *Oracle Calendar Administrator's Guide* to find out how to modify `ocas.conf` to do this.

Oracle Mobile Data Sync Sizing and Memory Use

The following sections describe Oracle Mobile Data Sync sizing and memory use:

- RAM and FastCGI Processes
- Hard Disk Space
- Determining the Best Setup for Your Organization

RAM and FastCGI Processes

Like the Oracle Calendar Web client and Oracle Calendar Web services, Oracle Mobile Data Sync RAM requirements are directly connected to the number of FastCGI processes running on an Applications tier. Each FastCGI process requires approximately 20 to 30 MB of RAM. The number of FastCGI processes you need for Oracle Mobile Data Sync depends on how many daily synchronizations occur in your organization. These processes must be considered in addition to the number allocated for the Oracle Calendar Web client and Oracle Calendar Web services, as described in Oracle Calendar Web Client and Oracle Calendar Web Services Sizing and Memory Use.

One FastCGI process is required for every synchronization that occurs. The length of each synchronization varies greatly, from two to three seconds for most synchronizations, to over a minute for full, but less common synchronizations. A safe assumption is that the average synchronization time is 20 seconds. In other words, assume that one FastCGI process can handle three synchronizations each minute.

You must run enough FastCGI processes to handle the number of synchronizations you expect to occur in your organization during peak hours. The total number of FastCGI processes can be spread across multiple Applications tiers running Oracle Mobile Data Sync. Make sure you run enough FastCGI processes to handle spikes in Oracle Mobile Data Sync use (such as after a new deployment).

Example

The following example illustrates how to prepare for peak Oracle Mobile Data Sync use. Under normal circumstances, your organization probably would not experience the kind of intense use described here.

Imagine that Vision Corporation has 50,000 users, and the number is broken down as follows:

- **Total Users**: 50,000
- **Expected Oracle Mobile Data Sync users**: 1,000

Vision Corporation's users must adhere to a defined 9:00 a.m. to 5:00 p.m. schedule, so almost all of these 1,000 Oracle Mobile Data Sync users will probably synchronize during the first hour of the work day. Because it is difficult to judge when exactly these synchronizations will occur — there could be a peak point during the hour — let us do the calculations as if there are 2,000 Oracle Mobile Data Sync users.

- **Exaggerated total Oracle Mobile Data Sync users**: 2,000
- **Peak concurrency (synchronizations each minute)**: (2,000 synchronizations) / (60 minutes) = 33.33 synchronizations each minute.

- **Number of FastCGI processes needed**: (33.33 synchronizations each minute) / (3 synchronizations each minute each FastCGI process) = 11.11

For the sake of simplicity, and as this example uses exaggerated numbers to account for peak, if not extraordinary circumstances, let us round off that number down to ten FastCGI processes.

If Vision Corporation is running Oracle Collaboration Suite on two Applications tiers for load balancing and redundancy, then the default of five FastCGIs on each tier should be more than enough to handle extreme peak synchronization periods (Oracle Calendar Web client use aside).

Because a FastCGI process requires 20 to 30 MB of RAM, each tier would require about 125 MB of RAM for Oracle Mobile Data Sync.

Based on this example, and allowing for variance in synchronization times and lengths, the following table lists ranges of Oracle Mobile Data Sync users, suggested FastCGI numbers, and the amount of memory needed.

Table 5–1 Oracle Mobile Data Sync FastCGI and Memory requirements for peak use

Range of Oracle Mobile Data Sync users	Suggested FastCGI Processes	Total RAM Required
500 - 1000	5	125 MB
1000 - 2000	10	250 MB
1500 - 3000	15	375 MB
2000 - 4000	20	500 MB

Hard Disk Space

Plan on allocating about 100 KB of permanent hard disk space each Oracle Mobile Data Sync user to store mapping tables and device information (links database). Two MB of temporary hard disk space each concurrent user should be allocated to maintain information used across synchronization messages during a synchronization session (session database).

A standalone Oracle Mobile Data Sync instance, composed of a standalone Oracle HTTP Server and standalone Oracle Calendar application system, with only the Oracle Mobile Data Sync request handler enabled (not Oracle Calendar Web client or Oracle Calendar Web services) requires about 500 MB.

Determining the Best Setup for Your Organization

After consulting the table in the preceding section, experiment with your FastCGI numbers and architecture to determine the optimum settings for your needs. Do surveys of your employees to determine how many people are synchronizing, and when. Try and establish patterns for use — perhaps more people synchronize on Monday mornings, or perhaps you have workers in different time zones who synchronize at various times of day.

Check the Oracle HTTP Server `error.log` for messages indicating FastCGI overload, shown as follows:

- `Resource temporarily unavailable: FastCGI: failed to connect to server`
- `FastCGI: comm with server "`*`server_path`*`" aborted`

You should only run as many FastCGI processes as are necessary, in case there are other applications sharing tiers with Oracle Mobile Data Sync. For information on setting the number of FastCGI processes, see *Oracle Calendar Administrator's Guide*.

Oracle Mobile Data Sync Deployment and Maintenance

This section only provides a high-level overview of some post-installation tasks for Oracle Mobile Data Sync. Consult *Oracle Calendar Administrator's Guide* for detailed instructions on managing, configuring and maintaining all components of Oracle Calendar.

By default, Oracle Mobile Data Sync is enabled on an installation of the Oracle Calendar application system. To disable it, comment out the appropriate section of `ocas.conf`, as described in Customizing OCAS Components in Chapter 3 of *Oracle Calendar Administrator's Guide*.

Deploying Oracle Connector for Outlook

This section contains the following topics:

Check for Supported Versions of Microsoft Outlook

The first thing to do when planning an Oracle Connector for Outlook deployment is to make sure you have access to supported version of Microsoft Outlook. These are listed in Appendix D, "Installing Oracle Collaboration Suite Clients" of the *Oracle Collaboration Suite Installation Guide*. Ensure that you also install the latest patches and service packs, as applicable. Microsoft Outlook 2000 must be used in Corporate Workgroup mode.

Note: Third-party Outlook add-ons can cause unexpected behavior in Oracle Connector for Outlook. If your organization uses and depends on third-party add-ons, then check with Oracle support to see if there are any known issues with them.

Deploying Oracle Connector for Outlook with Roaming Profiles and Terminal Services

Oracle Connector for Outlook supports Windows Roaming Profiles and Windows Server 2003 Terminal Services. Think about if you want to use these technologies before you start deploying and installing Oracle Connector for Outlook.

This section contains the following topics:

Windows Roaming Profiles

As of 10*g* Release 1 (10.1.1), Oracle Connector for Outlook is certified to work with Microsoft Windows Roaming Profiles. Windows Roaming Profiles is the mechanism whereby a user's profile — including startup applications, shortcuts, desktop settings, and registry settings — are stored on and retrieved from a central network server. With Windows Roaming Profiles, a user can have access to their data from any network-enabled computer. Oracle Connector for Outlook must be installed on the local computers, but can be configured on login from startup scripts. Data is stored in specific folders that are mapped to the server, while registry information for users is retrieved from the server and set up locally on first login.

When using Windows Roaming Profiles, ensure the following:

- All workstations use the same versions and patches of Windows, Outlook and Oracle Connector for Outlook.
- Oracle Connector for Outlook is deployed on all workstations using the same installation and configuration options.
- Oracle Connector for Outlook offline folders are mapped to a location on the home drive. For example, `Z:\profile_name\`.
- The default path for archiving should be mapped to a location on the home drive so that PST archives are available on every workstation. For example, `Z:\profile_name\archive\`.

Avoid accessing the same roaming profile from different workstations simultaneously, because this can lead to unexpected behavior.

Windows Server 2003 Terminal Services

As of 10*g* Release 1 (10.1.1), Oracle Connector for Outlook is certified to work with Windows Server 2003 Terminal Services. Terminal Services were conceived to provide organizations with a secure and cost-effective means of hosting Windows desktop sessions on a remote server. Remote users connect to a server through a desktop or Web interface and benefit from the full Windows experience without the overhead of running applications locally. Windows Server 2003 Terminal Services requires greater than normal bandwidth, and you must ensure that all drives are mapped correctly.

Consider using Terminal Services in combination with Roaming Profiles, such as when you have several Terminal Services servers running behind a load balancer. Without roaming profiles, when each time a client is directed to a different server, a profile will have to be re-created for that client. With a roaming profile stored on the backend, this will not be necessary — the client will have access to its profile no matter what server it is directed to.

Character Set Considerations with Terminal Services

Not all fields of Oracle Connector for Outlook support the Unicode character set. This means that if clients of several different language sets are connecting to the same terminal server, unexpected behavior may result. Ideally, you should configure separate servers with different character sets as follows:

- Western (English, French, Italian, Spanish, German)
- Cyrillic (Russian, Hungarian)
- Asian (Chinese, Japanese)
- Greek
- Arabic

Clients can be configured to connect to the server of the appropriate language.

Deploying Oracle Connector for Outlook to Local Computers

There are three common methods for deploying Oracle Connector for Outlook across an organization. For details on installation steps, see Appendix D, "Installing Oracle Collaboration Suite Clients" of the *Oracle Collaboration Suite Installation Guide*.

This section contains the following topics:

- Using Software Delivery Tools and Performing Silent Installations
- Using a Base Image
- Using a Shared Executable

Using Software Delivery Tools and Performing Silent Installations

This is the simplest method for end-users and the recommended choice for deploying Oracle Connector for Outlook. It requires using the Microsoft MSI installer with Microsoft Active Directory to deploy Oracle Connector for Outlook to workstations without requiring the user to log on with administrative rights. Each instance is deployed with the information logon of the user and server information extracted through Active Directory. MSI, which is extracted from the Oracle Connector for Outlook installation executable, can be used to copy over the binary files, install, reboot and execute a PRF file to configure a user's profile. This can be done as a "silent install," where the user does not need to be involved in, or even be aware of, the installation process.

Software delivery tool technology enables administrators to then automatically upgrade users when needed, and even uninstall unauthorized (such as Beta) versions. Licenses must be acquired for whatever software delivery tool is used.

For details on performing silent installations, enabling elevated privileges for users without administrative rights, and using Microsoft MSI, see Appendix D of the *Oracle Collaboration Suite Installation Guide*.

Using a Base Image

This method involves creating a base image that includes Oracle Connector for Outlook and installing it on all computers in your organization. The drawbacks to this method include:

- It is not practical to reimage all computers in an organization.
- User-side configuration is required, including entering passwords and specifying server names.

Using a Shared Executable

This method involves sharing an installation executable on a network that users run to install Oracle Connector for Outlook. This can cause a drain on bandwidth and, like with the Base Image method, requires user-side configuration after installation. Users must have administrative rights to their computers to use this method.

Configuring Oracle Connector for Outlook using PRF Files

Consider using PRF files to configure profiles for your users. In addition to allowing you to pre-configure parameters such as server names and ports, PRF files provide a convenient way of implementing organizational policy for all users. For example, you may want to ensure the following things about the user profiles:

- They preclude users from changing their passwords
- They are populated with organizational information not modifiable by users

Sample PRF content is included in see Appendix D of the *Oracle Collaboration Suite Installation Guide*. Ensure that you customize the top part of this content appropriately.

> **Note:** Users of `Modprof.exe` can still use this tool to create and modify Outlook 2000 profiles. However, Oracle strongly recommends using the Configuration Wizard that comes with Oracle Connector for Outlook.

Other characteristics to plan on configuring in a deployment, whether through PRFs, `Modprof.exe`, or manually, include the following:

- IMAP4 settings
- POP3 settings
- PST mail archive files
- Enabling or disabling of e-mail virus scans
- Backup software
- Synchronization protocols (older synchronization tools require you to specify which protocol to use)
- Third-party service provider settings

Ensure DNS is set up correctly and that the proper ports are used for mail, calendar and contacts, namely:

- IMAP: 143
- SMTP: 25
- Calendar: 5730
- LDAP: 389

Oracle Connector for Outlook also supports SSL or TLS secure protocols on the appropriate ports.

To deploy using PRFs, you may want to write a script that does the following:

- Prompts the user for a user name and password, then uses that information to run a PRF file to set up a profile for that user.
- Runs a PRF file that not only sets up a profile but is also configured to acquire credentials from the system, though this is more difficult.
- Have the user run the PRF to create the profile, after which the user will have to enter a login user name and password.

Automating deployment can be highly desirable, and you may want to combine some of the strategies mentioned here into one executable that, for example, silently installs Oracle Connector for Outlook then runs a script that configures profiles of users using PRF files.

Oracle Connector for Outlook includes a Configuration Wizard for configuring and creating PRF files and profiles. For information on the Configuration Wizard, working with PRF files, and configuring Oracle Connector for Outlook, see Appendix D,

"Installing Oracle Collaboration Suite Clients" of the *Oracle Collaboration Suite Installation Guide*.

Oracle Connector for Outlook Maintenance

After installation, Oracle Connector for Outlook can further be configured using settings defined in the `[OUTLOOK_CONNECTOR]` section of the `unison.ini` file on the Oracle Calendar server. For example, use `unison.ini` to control how often the Global Address Book is downloaded to users' workstations. For further information, see "Controlling Client Behavior" in Chapter 3 of *Oracle Calendar Reference Manual*.

Oracle Connector for Outlook includes built-in logging functionality. Log information is stored on workstations of users. Users can set preferences for this by selecting **Oracle Connector Troubleshooting** from the Oracle Connector for Outlook **Help** menu. Oracle recommends that at minimum, the default log settings be used.

Deploying Oracle Calendar Clients

The Oracle Calendar desktop client can be deployed in similar ways to Oracle Connector for Outlook, such as by using software delivery tools, base images or shared executables. For example, you may want to deploy the Oracle Calendar desktop client for Macintosh using a base image shared by Macintosh users in your organization.

Oracle Calendar Sync is a simple application that can easily be installed by end-users.

The following topics describe deployment strategies for Oracle Calendar clients:

- Deploying the Oracle Calendar Desktop Client with Windows Server 2003 Terminal Services
- Deploying the Oracle Calendar Desktop Client to Local Computers
- Deploying the Oracle Calendar Desktop Client on Shared Workstations
- Deploying Oracle Calendar Sync

> **Note:** Before undertaking any Oracle Calendar client deployment, check for supported platforms in Appendix D of the *Oracle Collaboration Suite Installation Guide*.

Deploying the Oracle Calendar Desktop Client with Windows Server 2003 Terminal Services

The Oracle Calendar desktop client supports Windows Server 2003 Terminal Services with Citrix Metaframe XP Version 1.00. The advantage of deploying the Oracle Calendar desktop client in this way is that installation only has to be done once, and it is easy to control which versions have been deployed to users.

If you have remote users connecting to the server, then you may find that they experience slow performance, depending on the network capacity.

Deploying the Oracle Calendar Desktop Client to Local Computers

The Oracle Calendar desktop client supports silent installation. The advantage of this is that no interaction is required from users. For Windows platforms, you can perform customized silent installations by extracting the files from the Oracle Calendar desktop client installation executable and modifying `unison.ini`. For details on silent

installations, see "Installing Calendar Clients" in Appendix D of the *Oracle Collaboration Suite Installation Guide*.

> **Note:** Silent installation is only supported for the Windows and Linux/Solaris versions of the Oracle Calendar desktop client.

Alternatively, you may choose to create a base image that includes the Oracle Calendar desktop client and is installed on all computers in your organization. This is easier than asking users to find a copy of the installation executable on the network. However some drawbacks to this method are as follows:

- It is not practical to reimage all computers in an organization.
- User-side configuration is required, including entering passwords and specifying server names.

Linux and Solaris installations of the Oracle Calendar desktop client place all required files within a single directory hierarchy without dependencies on the name or IP address of the host. This makes these two clients ideal candidates for a base image deployment.

Finally, you may choose to simply share an installation executable on a network. Users run the executable to install the Oracle Calendar desktop client. While this is a simple way to make the installation program available to users, it can cause a drain on bandwidth and, such as that with the base image method, requires user-side configuration after installation. Windows and Macintosh users must have administrative rights to their computers to use this method. The installation steps are simple and can be performed using a full graphical interface or a text mode interface.

Deploying the Oracle Calendar Desktop Client on Shared Workstations

One final issue to consider when deploying the Oracle Calendar desktop client is the use of shared workstations, such as in a library or on a public computer.

The Oracle Calendar desktop client stores user preferences and, optionally, local copies of agendas and address books on the computer on which it is installed. If various users log on to a computer using the same credentials and open their respective Calendar accounts using the Oracle Calendar desktop client, they must share the same Preferences. Also, each Calendar user will be prompted to locate their own database files (offline agendas and address books). The number of sets of database files is unlimited, so a periodic cleanup of the computer may be necessary.

Most users in these circumstances will not need offline access to their information and would probably be better off simply using the Oracle Calendar Web client. If this is not possible or practical, Oracle recommends that you disable Oracle Calendar desktop client offline address book functionality as follows:

- **For all users**: Set `offlineab` to `FALSE` in the `[LIMITS]` section of the Calendar server's `unison.ini` file.
- **For all users on a specific computer**: Set `offlineab` to `FALSE` in the local `UNISON.INI` file (not `unison.ini`). Do this in the following section of the file, according to your platform:
  - On Windows and Macintosh: `[GENPREFS]`
  - On Linux and Solaris: `[LIMITS]`

For further information, see "Controlling Client Behavior" in Chapter 3 of *Oracle Calendar Reference Manual*.

Deploying Oracle Calendar Sync

Installing Oracle Calendar Sync is a simple procedure and is described in "Installing Calendar Clients" in Appendix D of the *Oracle Collaboration Suite Installation Guide*. You can choose to share the installation executable on the network, or make it a part of your organization's base image so that users can install it as needed. Ensure that users already have their device and its accompanying software installed before installing Oracle Calendar Sync.

Oracle recommends that devices only be synchronized with one computer. Synchronizing a device with multiple computers can lead to unexpected behavior.

6

Deploying Oracle Content Services

This chapter discusses planning information designed to help you make important decisions about how to configure and deploy Oracle Content Services.

The following sections are included in the chapter:

- Understanding the Oracle Content Services Architecture and Functionality
- Planning for Oracle Content Services Deployment

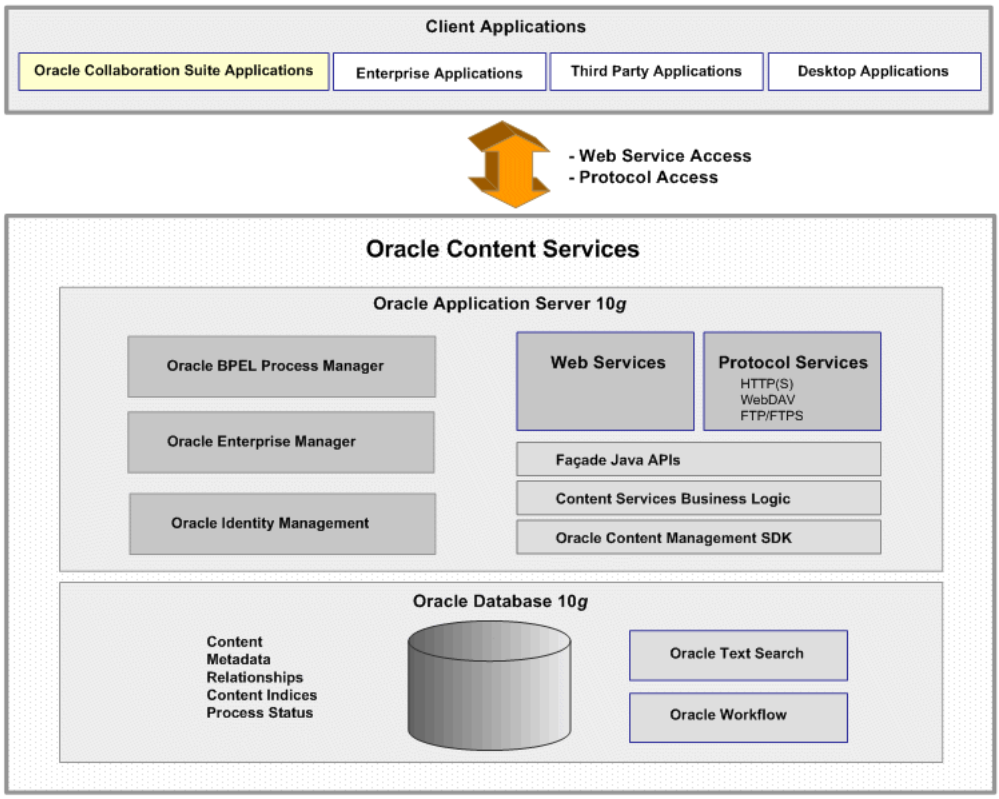
See Chapter 1, "Oracle Content Services Administration Concepts", in *Oracle Content Services Administrator's Guide* for detailed information on Oracle Content Services architecture and integration with key Oracle technologies.

Understanding the Oracle Content Services Architecture and Functionality

The following sections describe the technology underlying Oracle Content Services, as well as how the nodes and other processes interact. It also provides information about the Oracle Content Services Site model and Oracle Internet Directory.

For more detailed information about the Oracle Content Services architecture, see the *Oracle Content Services Administrator's Guide*.

Figure 6–1 Oracle Content Services Architecture



The Oracle Content Services application is built using Oracle Content Management SDK (Oracle CM SDK) Java APIs. This low-level API provides much of the required functionality, infrastructure, and runtime environment for content management, but does not dictate the business rules governing that content. These business rules and policies are implemented in a separate business logic layer.

A façade layer then provides a uniform Java interface that encompasses both Oracle CM SDK and application business logic. This layer is the foundation for the Oracle Content Services Web application, protocol servers, and Web services. The façade ensures that all components interfacing with Oracle Content Services do so at an abstraction level that respects the application business logic.

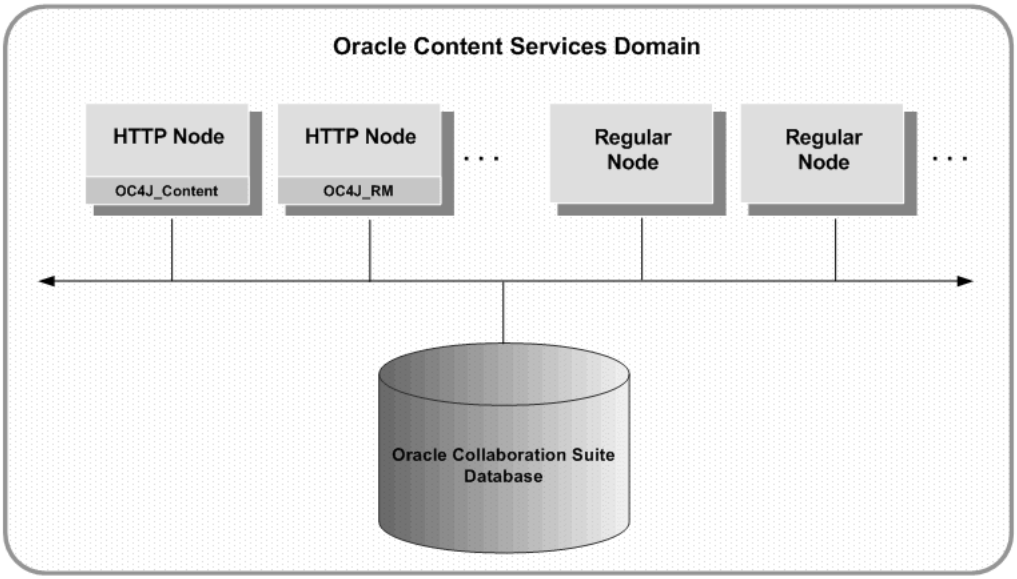
The Oracle Content Services Domain

An Oracle Content Services *domain* is a logical grouping of Oracle Content Services nodes and an Oracle database instance (called the Collaboration Suite Database) that contains the Oracle Content Services data. The nodes run on Oracle Application Server.

Oracle Content Services Schema

A *schema* is a group of related objects in a database. The Oracle Content Services schema is created in an Oracle database during the configuration process. The schema owns all database objects, including metadata about Oracle Content Services and configuration information (see Figure 6–2).

Figure 6–2 The Oracle Content Services Domain



Oracle Content Services Nodes

An Oracle Content Services *node* is the application that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the application at runtime.

The Oracle Content Services node processes and the database itself can be physically configured on a single host, or across several, separate hosts.

By default, an Oracle Content Services domain includes two nodes:

- regular node
- HTTP node

You can configure additional HTTP or regular nodes on the same computer or on additional computers.

The regular node supports protocol servers, such as FTP, as well as agents, such as the Garbage Collection Agent. The HTTP node supports the Oracle Content Services application, portlet, and WebDAV by means of servlets that are configured to work with the Oracle Application Server Containers for J2EE (OC4J).

Services, Servers, and Agents

Each node supports a *service* with specific configuration parameters, such as language, default character set, connections to the database, and cache sizes.

The service, in turn, supports the *servers*. Each server is either a protocol server or an agent. The protocol servers listen for requests from clients on a specific Internet Protocol (IP) port and respond to requests according to the rules of the protocol specification.

Agents perform operations periodically (time-based) or in response to events generated by other Oracle Content Services servers or processes (event-based). Although different agents can run in different nodes, each agent must run only on a single node. Typically, all the shipped agents must be run to ensure a stable system.

Oracle Internet Directory

Oracle Content Services uses Oracle Internet Directory for its identity management directory (list of user names and passwords). During configuration of Oracle Collaboration Suite, you select an Oracle Internet Directory server to be used with Oracle Content Services.

The Site Model

In Oracle Content Services, a *Site* is an organizational entity whose users can collaborate on files and folders. Oracle Content Services sites are based on Identity Management Realms.

See Chapter 1, "Oracle Content Services Administration Concepts", in *Oracle Content Services Administrator's Guide* for detailed information on Sites.

Planning for Oracle Content Services Deployment

This section provides information for planning an Oracle Content Services deployment.

- Choice of Protocols
- Oracle Content Services Sizing Guidelines
- Tablespaces
- Oracle Content Services Backup and Recovery

Choice of Protocols

The most important decision regarding performance and scalability is the choice of which protocols to use to access Oracle Content Services.

See Chapter 4, "Oracle Content Services Protocol Support", in *Oracle Content Services Administrator's Guide* for detailed information on protocol servers supported by Oracle Content Services, along with the client access paths and software for the supported protocols.

Oracle Content Services Sizing Guidelines

This section describes hardware requirements for a sample deployment of Oracle Content Services and formula that allow you to determine the hardware configuration required to deploy Oracle Content Services in your organization.

This section includes the following topics:

- Sizing Formulas for Each Applications Tier Computer
- Sizing Formulas for the Database Computer
- Memory Requirements: Sample Deployment

Hardware requirements for Oracle Content Services are primarily determined by the factors described in Table 6–1:

Table 6–1 Primary Factors Determining Oracle Content Services Hardware Requirements

Hardware Resource	Applications tier computer requirement variables	Database computer requirement variables
CPU	▪ Peak number of operations performed each second	▪ Peak number of operations performed each second ▪ Whether using Oracle Text indexing
Memory	▪ Peak number of operations performed each second ▪ Peak number of concurrent connected users ▪ Average number of protocols used each concurrent connected user ▪ Average number of sessions used each concurrent connected user ▪ Number of users accessing Oracle Content Services through FTP ▪ Number of files each folder	▪ Peak number of operations performed each second ▪ Number of files
Disk Size	N/A	▪ Number of files ▪ Average content size of files, whether they can be indexed or not
Disk Throughput (not discussed in this file)	N/A	▪ Peak number of files read and written each second ▪ Average content size of files

In order to determine hardware requirements, assumptions must be made about the type of work that users are performing. The following measurements are averages extrapolated from deployment of Oracle Content Services within Oracle Corporation (40,000+ users), and are generally applicable for projecting Oracle Content Services usage.

Table 6–2 User Profiles

User Task	Number of Operations each Connected User each Hour
Folder opens	8
Files read / written	10
Queries	0.1

Note: These sizing guidelines may be inaccurate if the desired user profile is significantly larger than the average measurements detailed in Table 6–2.

These sizing guidelines are based on benchmarks of 10,000 concurrent connected users on Sun Microsystems hardware. The guidelines have been validated against

measurements taken from internal Oracle Corporation production usage of Oracle Content Services by 40,000 Oracle employees, with 20 million files and 6.5TB of content. This system uses Intel Linux hardware for the Applications tier computers, and Sun hardware for the database.

Sizing Formulas for Each Applications Tier Computer

This section provides formulas that you can use to determine specific hardware sizing for each Applications tier computer.

- Number of CPUs
- Required Usable Disk Space
- Total Computer Memory, HTTP as the Primary Protocol
- Total Computer Memory, Primary Protocol Other Than HTTP

The following table summarizes the sizing formulas:

Table 6–3 General Oracle Content Services Sizing Recommendations for Each Applications Tier Computer

Component	Sizing Recommendations
Number of CPUs	`roundup(`*`peak concurrent connected users`*`/ 250 + 33% headroom)`
Required usable disk space	At least 500MB for Oracle Content Services
Total computer memory	If HTTP is the primary protocol: `480MB + (3.6 MB *` *`peak concurrent connected users`*`)` If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in Table 6–2: `480MB + (1MB * peak concurrent connected users * average number of sessions in use by each concurrent connected user) + (3KB * number of objects desired in the java object cache) + (8MB * number of connections to the database)`

Number of CPUs Use the following formula to determine the number of CPUs required:

`roundup(`*`peak concurrent connected users`*` / 250 + 33% `*`headroom`*`)`

The *`peak concurrent connected users`* parameter is the number of users who are signed in to Oracle Content Services and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content Services named user population.

The *`headroom`* parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should be allocated.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.

- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space Allocate at least 500MB for Oracle Content Services.

Total Computer Memory, HTTP as the Primary Protocol If HTTP is the primary protocol, then use the following formula to determine the total computer memory required:

```
480MB + (3.6MB * peak concurrent connected users)
```

The 480MB is for the first Oracle Content Services Applications tier computer. The value of 3.6MB is calculated from the following assumptions:

- **1.6 sessions each concurrent connected user**: This assumes that the primary interface for Oracle Content Services is through the HTTP node. The additional 0.6 sessions are HTTP sessions which are started whenever a user of the Oracle Content Services Web interface starts another Oracle Content Services Web interface or if the user accesses Web Folders or Oracle Drive.
- **0.1 connection pool connections each concurrent connected users**: This assumes the stated user profile.
- **400 objects in the Java data cache each concurrent connected user**: This assumes 50 files each folder and 8 folders opened each hour, assuming the stated user profile.

Total Computer Memory, Primary Protocol Other Than HTTP If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in Table 6–2, use the following formula to determine the total computer memory required:

```
480MB + (1MB * peak concurrent connected users * average number of sessions in use
by each concurrent connected user) + (3KB * number of objects desired in the Java
object cache) + (8MB * number of connections to the database)
```

The 480MB is for the first Oracle Content Services Applications tier computer. The other values are calculated from the following assumptions:

- The value of 1MB is high by design. Oracle Content Services has been optimized to reduce database CPU load by using Applications tier memory to cache items. This ensures a more scalable and less expensive system, because the database computer is less of a scalability bottleneck, and because memory on one- or two-processor Applications tier computers is typically less expensive than memory or CPU on high-end database computers (computers with large amounts of attached storage or with many processors).
- Oracle recommends limiting the number of peak concurrent user sessions through the `IFS.SERVICE.MaximumConcurrentSessions` parameter in the service configuration. Oracle has tested with Java heaps up to 2GB. With this constraint, this implies up to approximately 700 concurrent connected users each node and a total of 1986MB in size, if the following are true:
  - Each user uses 1.6 sessions
  - Each session is 1MB (700 * 1.6 * 1MB = 1,120MB)
  - Each user needs 400 Java data cache objects
  - Each object is 3KB in size (700 * 400 * 3KB = 866MB)

For each additional node on the same computer, you must include the node overhead in the sizing. See Table 6–5 for more information.

The HTTP/WebDAV memory overhead includes memory for 10 simultaneous guest user requests. Because of this, guest users should not be counted as connected users for HTTP/WebDAV access.

- For the average number of sessions in use by each concurrent connected user, use the value 1.6 for the HTTP node.
- Calculate the number of objects desired in the Java object cache by using the following formula:

  (*number of folder opens in the peak hour*) * (*number of objects each folder*) * (*number peak concurrent connected users*)

  Use the result to set the value of the `IFS.SERVICE.DATACACHE.Size` parameter.
- The number of connections to the database depends on the number of simultaneous read or write operations being performed. Assume 0.1 database connections each user if using a standard user profile. This is a sum of the parameters `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize` and `IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize` for each service.

Sizing Formulas for the Database Computer

This section provides formula that you can use to determine specific hardware sizing for each database computer to be used for Oracle Content Services users.

- Number of CPUs
- Required Usable Disk Space
- Total Computer Memory

The following table summarizes the sizing formulas:

Table 6–4 General Oracle Content Services Sizing Recommendations for the Database Computer

Component	Sizing Recommendations
Number of CPUs	roundup(*peak concurrent connected users* / 250 + 33% headroom)
Required usable disk space	4.5GB + *total raw file size* + (*total raw files size* * 20%)
Total computer memory	64MB + 128MB + *database buffer cache* + (1MB * *number of connections to the database*) + (500 bytes * *number of files*) + (100KB * *peak concurrent connected users*)

Number of CPUs Use the following formula to determine the number of CPUs required:

roundup(*peak concurrent connected users* / 250 + 33% headroom)

The *peak concurrent connected users* parameter is the number of users who are signed in to Oracle Content Services and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content Services named user population.

The *headroom* parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should

be allocated. One additional CPU is used for the background Oracle Text indexing of new file content, if you are using Oracle Text indexing.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.
- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space Use the following formula to determine the usable disk space required:

```
4.5GB + total raw file size + (total raw file size * 20%)
```

The 4.5GB represents the space required for Oracle software and the initial database configuration. If you are not using Oracle Text to index the content, multiply the total raw file size by 15% instead of 20%.

The following considerations can increase the amount of usable disk space required for the database computer:

- Mirroring for backup and reliability
- Redo log size, which should be determined by how many files are inserted and their size
- Unused portion of the last extent in each database, which occurs with pre-created database files or which can be large if the next extent setting is large

Total Computer Memory Use the following formula to determine the total computer memory required:

```
64MB + 128MB + database buffer cache + (1MB * number of connections
to the database) + (500 bytes * number of files) + (100KB * peak concurrent
connected users)
```

This formula is based on the following assumptions:

- 128MB is the minimum amount of memory required to run a small Oracle Server.
- Number of files: The database buffer cache in the default Oracle database configuration is sufficient for approximately 50,000 files. For deployments with more than 50,000 files, allocate 500 bytes each file for optimal performance, including wildcard filename searches. Reduce this number if users do not perform wildcard filename searches.
- 100KB is calculated by assuming that 0.1 database connections are needed each concurrent connected user as in the stated user profile. Each database connection takes approximately 1MB of database memory.

Memory Requirements: Sample Deployment

Table 6–5 describes approximate minimum memory overhead on the Applications tier computers for each component.

Table 6–5 Memory Overhead by Component

Description	Approximate. minimum memory (MB) for Applications tier computer running a regular node and HTTP node	Approximate minimum memory (MB) for Applications tier computer running an additional HTTP node	Approximate minimum memory (MB) for Applications tier computer running an additional regular node
Memory used by the operating system upon booting the computer.	60	60	60
Overhead for first Java Virtual Computer (JVM).	30	30	30
Domain controller JVM. Only needs to be run once for a single Oracle Content Services schema, regardless of how many Applications tier computers are running Oracle Content Services protocols.	20	0	0
Oracle Enterprise Manager Web site. Must run on every node to allow managing the node through Oracle Enterprise Manager.	150	150	150
Regular Oracle Content Services node JVM. By default, runs the FTP server and the Oracle Content Services agents.	50	0	50
Oracle Content Services Node guardian JVM, which monitors the Oracle Content Services regular node and recovers from node failures.	10	0	10
Oracle HTTP Server, including the default HTTP daemons. Only needs to run where HTTP access is required.	30	30	0
Oracle Content Services OC4J process. Only needs to run where Oracle Content Services HTTP/WebDAV/ Oracle Drive access is required. Must be paired with Oracle HTTP Server.	130	130	0
Total	**480**	**400**	**300**

Tablespaces

This section provides information about the Oracle Content Services tablespaces.

This section includes the following topics:

Data Types and Storage Requirements

Table 6–6 shows the different types of data stored in Oracle Content Services and describes the purpose of each tablespace. Each of these tablespaces will be discussed in further detail in subsequent sections of this file.

Table 6–6 Tablespace Definitions

Tablespace Type	Name (in Oracle Files Configuration Assistant)	Tablespace Name	Description
File Storage	Indexed Media	`IFS_LOB_I`	Stores the Large Object (LOB) data for files that are indexed by Oracle Text, such as text and word processing files.
File Storage	Non-Indexed Media	`IFS_LOB_N`	Stores the LOB data for files that are not indexed by Oracle Text, such as zip files.
File Storage	interMedia Media	`IFS_LOB_M`	Stores the LOB data for files that are indexed by Oracle *inter*Media, such as image, audio, and video files.
Oracle Text	Oracle Text Data	`IFS_CTX_I`	Stores words (tokens) extracted by Oracle Text from Oracle Content Services files (the Oracle table `DR$IFS_TEXT$I`).
Oracle Text	Oracle Text Index	`IFS_CTX_X`	Stores the Oracle B*tree index on the Oracle Text tokens (the Oracle index `DR$IFS_TEXT$X`).
Oracle Text	Oracle Text Keymap	`IFS_CTX_K`	Stores miscellaneous Oracle Text tables (the Oracle tables `DR$IFS_TEXT$K`, `DR$IFS_TEXT$N`, `DR$IFS_TEXT$R`).
Metadata	Primary	`IFS_MAIN`	Stores metadata for files, information about users and groups, and other Oracle Content Services object data.
General Oracle Storage	N/A	Various	`SYSTEM`, `ROLLBACK`, `TEMP`, and other tablespaces that store the Oracle data dictionary, temporary data during transactions, and so on.

Typical tablespace storage space and disk I/O are detailed in Table 6–7:

Table 6–7 Tablespace Storage Requirements and Disk I/O

Tablespace	% of Total I/O Throughput Requirements	% of Disk Space Requirements
IFS_MAIN	50%	2%
IFS_CTX_X	20%	1%
IFS_CTX_I	10%	1%
IFS_LOB_I	8%	35%
IFS_LOB_N	5%	55%
Various	5%	1%
IFS_LOB_M	1%	4%
IFS_CTX_K	1%	1%
Total	**100%**	**100**

Note the following issues regarding the information in Table 6–7:

- I/O rates are highly dependent on the size of the db_cache_size. These measurements were taken on the Oracle-internal Oracle Content Services implementation, with 8GB db_cache_size, 17 million files, and 40,000 named users.
- The IFS_MAIN tablespace is the most important tablespace to spread across disks for maximum I/O capacity.
- Disk I/O for the IFS_CTX_I, IFS_CTX_X and IFS_CTX_K tablespaces is largely generated from Oracle Text batch processes (ctx_ddl.sync_index, and ctx_ddl.optimize_index), which are not critical to end-user performance. Therefore, these tablespaces can be on disks with lower I/O capacity, if necessary.

Storing Files in an Oracle Database

The largest consumption of disk space will occur on the disks that actually contain the files that reside within Oracle Content Services, namely the Indexed Media tablespaces, Non-Indexed Media tablespaces, and *inter*Media tablespaces. This section explains how the files are stored and how to calculate the amount of space those files will require.

As previously mentioned, files stored in Oracle Content Services are actually stored in database tablespaces. Oracle Content Services makes use of the Large Object (LOB) facility of the Oracle Database. All files are stored as Binary Large Objects (BLOBs), which is one type of LOB provided by the database. LOBs provide for transactional semantics much like the normal data stored in a database. In order to accomplish these semantics, LOBs must be broken down into smaller pieces which are individually modifiable and recoverable. These smaller pieces are referred to as chunks. Chunks are a group of one or more sequential database blocks from a tablespace that contains a LOB column.

Both database blocks and chunk information within those blocks (BlockOverhead) impose some amount of overhead for the stored data. BlockOverhead is presently 60 bytes each block, which consists of the block header, the LOB header, and the block checksum. Oracle Content Services configures its LOBs to have a 32K chunk size.

As an example, assume that the DB_BLOCK_SIZE parameter of the database is set to 8192(8K). A chunk would require four contiguous blocks and impose an overhead of 240 bytes. The usable space within a chunk would be 32768-240=32528 bytes.

Each file stored in Oracle Content Services consists of an integral number of chunks. Using the previous example, for instance, a 500K file will actually use 512000/32528=15.74=16 chunks. Sixteen chunks will take up 16*32K = 524288 bytes. The chunking overhead for storing this file would then be 524288-512000=12288 bytes which is 2.4% of the original file's size.

The chunk size used by Oracle Content Services is set to optimize access times for files. Note that small files, files less than one chunk, will incur a greater disk space percentage overhead since they must use at least a single chunk.

Another structure required for transactional semantics on LOBs is the LOB Index. Each LOB index entry can point to 8 chunks of a specific LOB object (`NumLobPerIndexEntry = 8`). In our continuing example, where a 500K file takes up 16 chunks, two index entries would be required for that object. Each entry takes 46 bytes (`LobIndexEntryOverhead`) and is then stored in an Oracle B*tree index, which in turn has its own overhead depending upon how fragmented that index becomes.

The last factor affecting LOB space utilization is the `PCTVERSION` parameter used when creating the LOB column. For information about how `PCTVERSION` works, please consult the *Oracle Database SQL Reference*.

Oracle Content Services uses the default `PCTVERSION` of 10% for the LOB columns it creates. This reduces the possibility of "ORA-22924 snapshot too old" errors occurring in read consistent views. So by default, a minimum of a 10 percent increase in chunking space must be added in to the expected disk usage to allow for persistent `PCTVERSION` chunks.

For large systems where disk space is an issue, Oracle recommends reducing `PCTVERSION` to 1, in order to reduce disk storage requirements. This may be done at any time in a running system using the following SQL commands:

```
alter table odmm_contentstore modify lob (globalindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob_t) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob_t) (pctversion 1);
alter table odmm_nonindexedstore modify lob (nonindexedblob2) (pctversion 1);
```

The steps for calculating LOB tablespace usage are as follows:

1. Calculate the number of chunks a file will use by figuring the number of blocks each chunk, then subtracting the `BlockOverhead` (60 bytes) from the chunk size to get the available space each chunk.
2. Divide the file size by the available space each chunk to get the number of chunks, each the following formula:

   ```
   chunks = roundup(FileSize / ChunkSize=((ChunkSize/BlockSize) * BlockOverhead)))
   ```

   For example, if *`FileSize`* = 100,000, *`ChunkSize`* = 32768, *`Blocksize`* = 8192, and *`BlockOverhead`* = 60, then the number of chunks is as follows:

   ```
   roundup(100000 / (32768 - ((32768 / 8192) * 60))) = 4 chunks
   ```

3. Calculate the amount of disk space for a file by multiplying the number of chunks times the chunk size, multiplying that result by the `PCTVERSION` factor, and then adding the space for `NumLobPerIndexEntry` (8) and `LobIndexEntryOverhead` (46 bytes).

   ```
   FileDiskSpaceInBytes = roundup(chunks * ChunkSize * PCTVERSIONFactor) +
   roundup(chunks / NumLobPerIndexEntry * LobIndexEntryOverhead)
   ```

Hence, if *chunks* = 4, *ChunkSize* = 32768, *PCTVERSIONFactor* = 1.1, *NumLobPerIndexEntry* = 8, and *LobIndexEntryOverhead* = 46:

```
roundup(4 * 32768 * 1.1) + (roundup(4 / 8) * 46)= 144226 FileDiskSpaceInBytes
```

4. Calculate the total disk space used for file storage by summing up the application of the preceding formulas for each file to be stored in the LOB, using the following formula:

   ```
   TableSpaceUsage = sum(FileDiskSpaceInBytes)
   ```

   This is for all files stored.

Oracle Content Services creates multiple LOB columns. The space calculation must be made for each tablespace based upon the amount of content that will qualify for storage in that tablespace.

Oracle Content Services Metadata and Infrastructure

The Oracle Content Services server keeps persistent information about the file system and the contents of that file system in database tables. These tables and their associated structures are stored in the Oracle Content Services Primary tablespace. This tablespace contains approximately 300 tables and 500 indexes. These structures are required to support both the file system and the various protocols and user interfaces that make use of that file system.

The administration and planning tasks of this space should be very similar to operations on a normal Oracle database installation. The administrator of the system should plan for approximately 6K of overhead each file to be used from this tablespace, or about 2% of the overall content. If there is a significant amount of custom metadata, such as categories, this overhead will be larger.

The initial disk space allocated for this tablespace is approximately 50MB for a default install. Of this 50MB, 16MB is actually used at the completion of installation. This includes instantiations for all required tables and indexes and the metadata required for the approximately 700 files that are loaded into Oracle Content Services as part of the install. Different tables and indexes within this tablespace will grow at different rates depending on which features of Oracle Content Services are used in a particular installation.

Oracle Text

When Oracle Content Services works in conjunction with Oracle Text, it enables users to access powerful search capabilities on the files stored within Oracle Content Services. Disk space for these capabilities is divided among three distinct tablespaces for optimal performance.

The Oracle Text Data tablespace contains tables which hold the text tokens (separate words) that exist within the various indexed files. The storage for these text tokens is roughly proportional to the ASCII content of the file.

The ASCII content percentage varies depending on the format of the original file. Text files only have white space as their non-ASCII content and therefore incur a greater each file percentage overhead. File types such as Microsoft Word or PowerPoint contain large amounts of data required for formatting that does not qualify as text tokens. The each file percentage on these types of files is therefore lower. On a system with diverse content types the expected overhead is approximately 8% of the sum of the original sizes of the indexed files.

Table 6–8 offers general guidelines for the amount of ASCII text in a file for several popular formats:

Table 6–8 Average ASCII Content each File Type

Format	Plain ASCII Content as Percentage of File Size	Typical Percentage of all File Content[1]
Microsoft Excel[2]	250%	4%
ASCII	100%	2%
HTML	90%	10%
Rich Text Format	80%	2
Microsoft Word	70%	13%
Acrobat PDF	10%	18%
Microsoft PowerPoint	1%	3%
Images (JPEG, BMP), Compressed files (Zip, TAR), Binary files, and so on.	0%	50%
Total		**100%**

1 From statistics of Oracle Corporation's internal usage of Oracle Content Services.

2 By default, Oracle Text indexes each number in an Excel file as a separate word. Excel stores a number more efficiently than its ASCII equivalent, which is why the ASCII content as a percentage of the file size is greater than 100%.

The Oracle Text Keymap tablespace contains the tables and indexes required to translate from the Oracle Content Services locator of a file (the Oracle Content Services DocID) to the Oracle Text locator of that same file (the Oracle Text DocID). The expected space utilization for this tablespace is approximately 70 bytes each indexed file.

The Oracle Text Index tablespace contains the B*tree database index that is used against the text token information stored in the Oracle Text Data tablespace. This will grow as a function of the ASCII content just as the Oracle Text Data tablespace does. On a system with diverse content types the expected overhead is approximately 4% of the sum of the ASCII content of the files, or approximately 1% of the sum of the total sizes of the indexed files.

Disk Space Requirements: Sample Deployment

This section details various requirements for disk space, and offers guidance as to how necessary disk space will expand with the addition of files to the server.

Based on experience running Oracle Content Services for Oracle Corporation's internal usage, the disk overhead of Oracle Content Services for a large system (hundreds of gigabytes of file content) is approximately as detailed in Table 6–9.

Table 6–9 Disk Space Requirements Summary

Tablespace Overhead Type	Overhead Versus Total Raw File Content[1]	Primarily Determined By
File Storage	12%	Size of files relative to chunk size (32KB by default)
Oracle Text	5%	Amount of ASCII content in all files

Table 6–9 (Cont.) Disk Space Requirements Summary

Tablespace Overhead Type	Overhead Versus Total Raw File Content[1]	Primarily Determined By
Metadata	2%	Number of folders, files, and so on.
General Oracle Storage	1%	Fixed, not configurable, database settings for `TEMP`, `UNDO`, and other tablespaces
Total	**20%**	

[1] This does not include: Mirroring for backup and reliability; Redo log size, which should be determined by how many files are inserted and their size; Unused portion of the last extent in each database file (which will occur with pre-created database files or which may be large if the next extent setting is large).

See *Oracle Database Concepts* for explanations of the terms Large Object, tablespace, chunk size, and extents.

Note: Given that a large percentage of the overhead is in LOB overhead, the overhead for your Oracle Content Services instance may vary depending on the average and median sizes of files.

Oracle Content Services Backup and Recovery

Planning for failures is one of the most important jobs of any system administrator or database administrator (DBA). Be sure to implement a daily or weekly backup plan that meets the needs of your business and operations environment. Take advantage of the Oracle database backup capabilities, that are built in the database.

Always back up the system before upgrading, migrating new data, or making other major changes. See *Oracle Database Backup and Recovery Basics* for additional information.

Note: In addition to the Oracle Content Services schema, there are three special schemas that ensure secure connectivity to other systems. When you back up your system, make sure to include these schemas.

The special schema names are derived from the Oracle Content Services schema name. For example, if the Oracle Content Services schema name is `CONTSRV`, the additional schemas are `CONTSRV$CM`, `CONTSRV$DR`, and `CONTSRV$ID`.

7

Deploying Oracle Discusssions

This chapter contains the following topics:

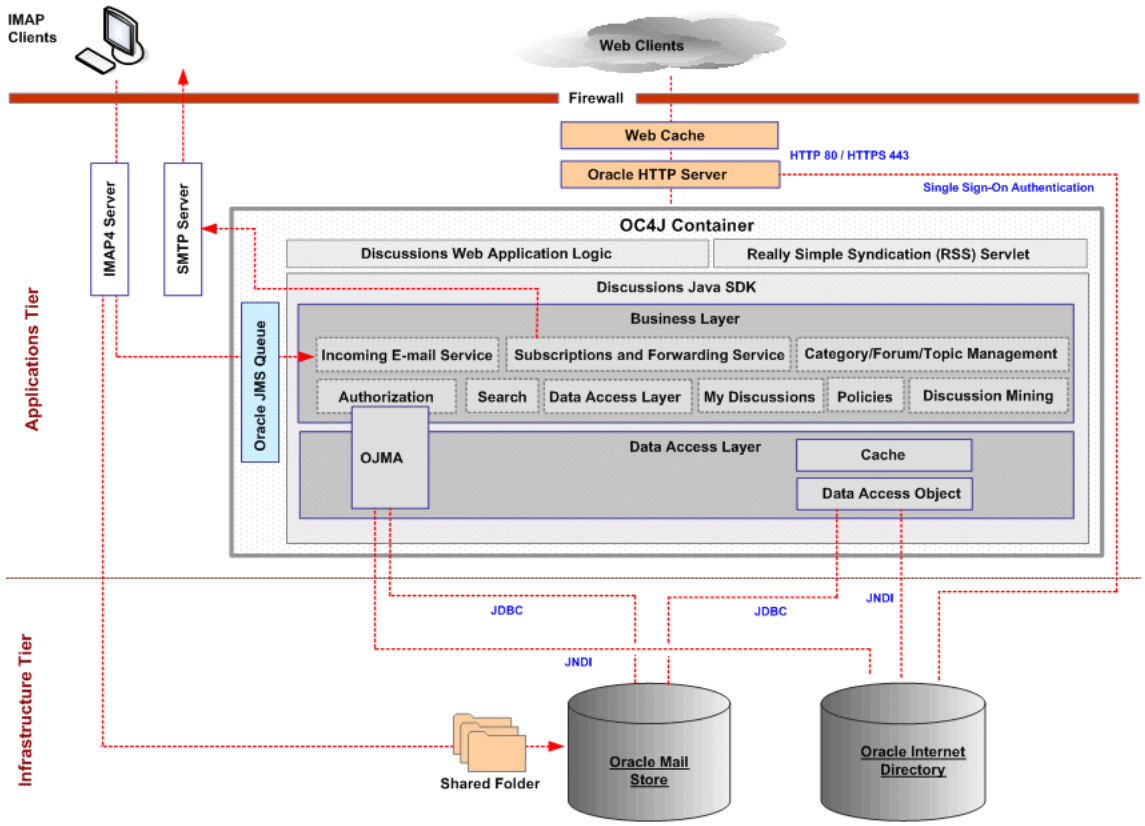
Understanding the Oracle Discusssions Architecture and Functionality

This chapter provides the conceptual background required to deploy Oracle Discusssions. It provides an overview of the Oracle Discusssions components and deployment configurations.

Oracle Discusssions Architecture

Oracle Discusssions is built upon the Oracle Mail architecture and is comprised of a shared folder in the Oracle Mail schema. Figure 7–1 illustrates the Oracle Discusssions architecture and functionality:

Figure 7–1 Oracle Discusssions Architecture



Applications Tier

In Figure 7–1, the Applications tier contains the following components:

- **IMAP4 Server**: It sends incoming mail from IMAP clients. This mail is processed by Advanced Queue and then by the Incoming E-mail Service. IMAP clients can access Oracle Discusssions forums as Mail Shared Folders. When posting messages to an Oracle Discusssions forum through E-mail, the Oracle IMAP4 Server receives a new message for Discussions and notifies the Oracle Discusssions application that a new message is ready to be processed through an Oracle JMS Queue.
- **SMTP Server**: It handles outgoing mail from the Subscription and Forwarding Service.
- **Web Cache:** Web client requests are processed through Web Cache and then forwarded to the Oracle HTTP Server.
- **Oracle HTTP Server**: It first sends an HTTP or HTTPS request to Oracle Internet Directory to perform single sign-on authentication, and then sends an HTTP or HTTPS request to the OC4J container.
- **OC4J Container**: Oracle Discusssions is deployed as a J2EE application in an OC4J container. The application is comprised of the following:
  - **Discussions Web Application Logic**. The Discussions Web Application Logic contains the web application with which users interact with Oracle Discusssions. The Web application enables users to browse forums, post new

messages and moderate forum content. The Oracle Discusssions Web Application is built on the Oracle Discusssions Java SDK APIs.

- **Really Simple Syndication Servlet (RSS)**. RSS is a web module that builds and returns several feeds for Discussions. For example, users can access RSS feeds for all topics of a forum, all messages of a topic, or their favorite topics.
- **Oracle JMS Queue.** The Oracle JMS Queue is used by the IMAP4 Server to notify the Oracle Discusssions application that a new e-mail message has been received which is addressed to a Discussions forum.
- **Discussions Java SDK**. The Oracle Discusssions Java SDK APIs are designed following the Java Mail SDK APIs in an Object Oriented model. They expose APIs for interacting with the Oracle Discusssions system. The Oracle Discusssions Web Application is built on top of the same Java SDK.

OC4J Container Business Layer

The OC4J container business layer is comprised of the following:

Table 7–1 Oracle Discusssions Java SDK Business Layer

Business Layer Component	Definition
Incoming E-Mail Service	Handles incoming e-mail messages to the discussion.
Subscription and Forwarding Service	Forwards relevant discussion information to specified recipients.
Category Forum Topic Management	Handles category and topic management in the discussion.
Authorization	Handles authorization of discussion participants by authenticating them with the Oracle Internet Directory. The authorization service uses OJMA to establish a JNDI connection with Oracle Internet Directory.
Search	Enables participants to search the discussion.
Data Access Layer	The data access layer accesses Oracle Mail repository to fetch information as list of topics in a forum or messages in a topic.
My Discussions	Enables participants to organize discussions in a UI category called "My Discussions".
Policies	Controls Discussions behavior based on policies set by forum moderators.
Discussion Mining	Computes which topics and message are most popular or most interesting based on time and other criteria.

Table 7–2 Oracle Discusssions Java SDK Data Access Layer

Business Layer Component	Definition
OJMA	Discussions uses Oracle Java Mail APIs (OJMA) for managing Mail Shared Folders and the access control policies.
Cache	Caches most frequently accessed information in memory.
Data Access Object	Accesses data in the Oracle Mail store andOracle Internet Directory.

Infrastructure Tier

Oracle Discusssions leverages the Oracle Mail store and Oracle Internet Directory in the Infrastructure tier.

Oracle Mail Store

Oracle Discusssions leverages existing Oracle infrastructure provided by Oracle Mail SharedFolders for its message storage. A category can be mapped to a SharedFolder holding other folders. A forum can be mapped to a SharedFolder holding all the topics posted to that forum. When creating a new category, Oracle Discusssions interacts with Oracle Mail to create a new SharedFolder defined to contain other folders. When creating a new forum, Oracle Discusssions interacts with Oracle Mail and creates a corresponding new SharedFolder to contain messages. Oracle Mail enables for a deployment scenario in which e-mail data is stored in different Oracle Mail stores and each Oracle Mail store is associated with a database instance.

Oracle Internet Directory

Oracle Discusssions authorization information, including all SharedFolder definition and permission information is stored in the Oracle Internet Directory. As a result of the Oracle Discusssions Web Application design, permissions are checked through an Oracle Internet Directory lookup before performing any write operation, such as appending new messages or creating a new forum.

Oracle Discussions Functionality

Oracle Discusssions functionality is illustrated in Figure 7–1. In this figure, Web clients and IMAP clients perform functions with Oracle Discusssions.

Web Clients

Oracle Discusssions is a Web-based application for on-line bulletin boards. Consequently Oracle Discusssions can be accessed through Web browsers. Web clients connect to Oracle Discussions through Web Cache and the Oracle HTTP Server. The Oracle HTTP Server first performs a single sign-on authentication on the Oracle Internet Directory, and then makes an HTTP or HTTPS request to the OC4J container where the Oracle Discusssions J2EE application is deployed. In a typical request processing flow, Oracle Discusssions first verifies the permissions of the requesting user in the Oracle Internet Directory using OJMA APIs and then looks up the required data in the in memory cache. If the required data is not present, it proceeds through the Data Access Layer to fetch it from the Oracle Mail store using JDBC and PL/SQL procedures.

IMAP Clients

IMAP clients send e-mail messages to and receive e-mail messages from Oracle Discusssions. Incoming messages are sent to the Oracle Discusssions forum e-mail address. The IMAP4 server notifies the Oracle Discusssions application of the incoming message through an Oracle JMA Queue. Outgoing messages are forwarded as specified by forum moderators or are sent to users subscribed to Oracle Discusssions content by the Subscription and Forwarding Service and through the SMTP server.

Planning for Oracle Discusssions Deployment

This section provides information for planning an Oracle Discusssions deployment.

Determining the Number of Database Connection Pools in a Shared OJMA

The Oracle Java Mail API (OJMA) has a limited number of available database connection pools. Because Oracle Discusssions shares the same OC4J container as

other applications including Oracle Mail, the default number of connection pools (typically set at three hundred) may be exceeded. If the number of combined concurrent user from Oracle Discusssions and other Oracle Collaboration Suite applications exceeds or is likely to exceed the existing number of OJMA connection pools then you can increase the number of available connection pools in the OC4J_ Properties file and the process parameter in the Oracle Collaboration Suite database used for Discussions.

> **See Also:** "Managing Oracle Workspaces " in Chapter 5 of *Oracle Collaboration Suite Administrator's Guide*.

Reducing the Delay for Posting Data Cached in an OC4J Container

Oracle Discusssions caches most frequently accessed information in memory. When deployed in a multiple OC4J containers scenario, each container has its own cache. As a result, a user accessing Oracle Discusssions from one OC4J container may not immediately see information posted by a user accessing Oracle Discusssions from another OC4J container. If the delay between these events is excessive, then you can shorten it by modifying the TTL (Time to Leave) attribute for the OC4J container cache.

Determining When to Increase the OC4J Cache Size

In some cases, you may want to increase the size of the OC4J cache. You can use Oracle Enterprise Manager Configuration for Oracle Collaboration Suite to detect the number of hits and misses for the Oracle Discusssions application. A significant number of misses may indicate that the cache is to small to handle the current workload and must be increased.

Oracle Discussions Deployment Configurations

This section discusses available deployment configurations for Oracle Discusssions. Because Oracle Discusssions leverages the Oracle Mail schema, most deployment configurations are based on available deployment configurations for Oracle Mail.

> **See Also:** For information about available deployment configurations, see "Oracle Mail Deployment Configurations" in Chapter 8, "Deploying Oracle Mail".

Oracle Discussions Deployment with the Oracle Mail Store

Each instance of Oracle Discusssions on the Applications tier can only be associated with one mail store. The Oracle Discusssions application is associated with the corresponding mail store through a single Oracle Discusssions administrative user. When you install Oracle Discusssions, you choose a mail store and an e-mail domain. The installer then creates an internal mail user that is associated with the specified mail store, and provisions the administrative user for the specified e-mail domain. The administrative user is the owner of all shared folders used by Oracle Discusssions. The following guidelines apply to the Oracle Discusssions administrative user:

- All Oracle Discusssions folders within the Oracle Mail store are created by the administrative user.
- Only the owner of a shared folder can create sub-shared folders within the shared folder.

- Because only the shared folder creator can delete boards, when a shared folder associated with a board is exposed to native e-mail clients, it cannot be deleted by board member accessing it from those clients.

Figure 7–2 Oracle Discusssions Deployment with Oracle Mail Store

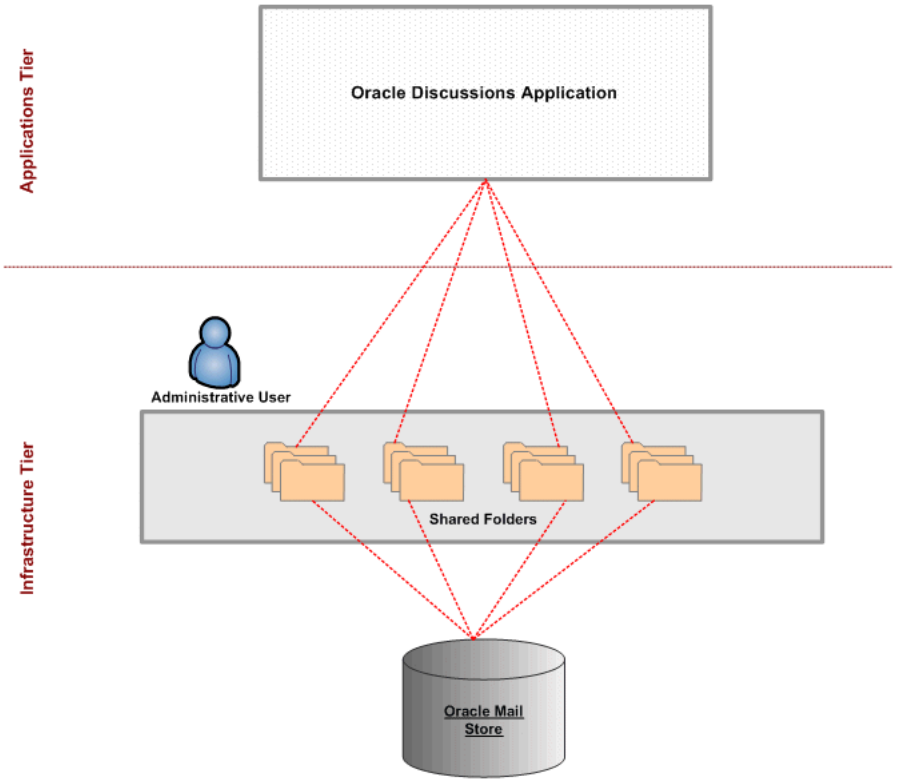


Figure 7–2, illustrates how an individual Oracle Discusssions application on the Applications tier can only be mapped to one Oracle Mail store. In addition, the Oracle Mail store can only have a single Oracle Discusssions administrative user that creates and administers the SharedFolders on the mail store. This figure contains a single Oracle Discusssions application on the Applications tier that connects to the shared folders of a single Oracle Mail store on the Infrastructure tier. The shared folders are created and administered by a single Oracle Discusssions administrative user.

8

Deploying Oracle Mail

This chapter contains the following topics:

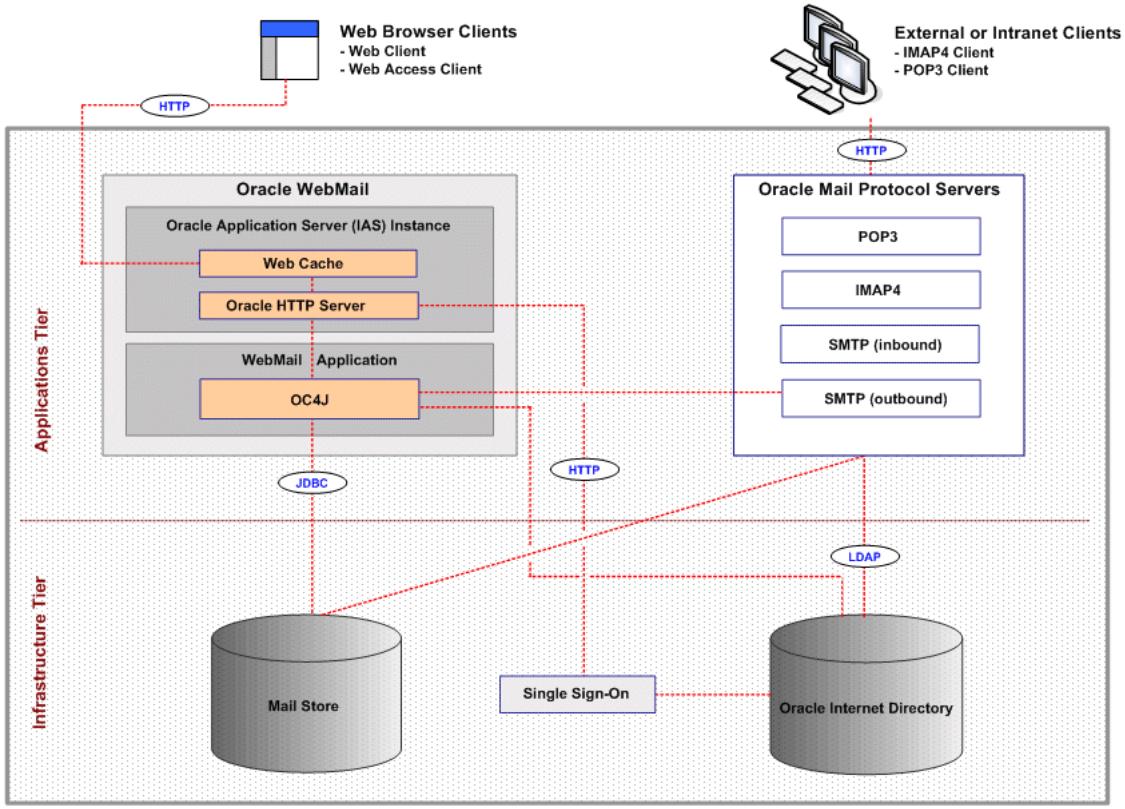
Understanding the Oracle Mail Architecture and Functionality

This chapter provides the conceptual background required to deploy Oracle Mail. It provides an overview of the Oracle Mail architecture, a discussion of deployment planning issues and deployment configurations.

Oracle Mail Architecture

This section provides an overview of the Oracle Mail architecture. Subsequent sections of this chapter discuss the available deployment configurations for the Oracle Mail architecture.

Figure 8–1 Oracle Mail Architecture



Infrastructure Tier

In Figure 8–1, the Infrastructure tier contains the following components:

- **Mail store** is the repository that stores Oracle Mail messages.
- **Oracle Internet Directory** stores user identity information.

Applications Tier

In , the Applications tier contains the Oracle Mail application which is comprised of the Oracle Mail protocol servers and Oracle WebMail.

Oracle WebMail

Oracle WebMail is comprised of an Oracle Application Server instance and the WebMail application. The Oracle Application Server instance contains the Web Cache and the Oracle HTTP Server. The WebMail application is an OC4J container. Oracle WebMail also uses the outbound SMTP protocol server for sending mail. Oracle WebMail functionality is described in the "Oracle Mail Functionality" section.

Oracle Mail Protocol Servers

Oracle Mail contains the following protocol servers:

- **POP3** for accessing mail that is downloaded to a local mail client
- **IMAP4** for accessing mail that remains stored on the server
- **SMTP (inbound)** for processing mail sent from outside the organization

- **SMTP (outbound)** for sending mail within the organization.

The function and purpose of the Oracle Mail protocol servers is further discussed in the "Oracle Mail Functionality" section.

Clients

Oracle Mail supports a variety of desktop mail clients. Oracle WebMail supports both a browser-based thin client and the Oracle Collaboration Suite Integrated Client. Both the Web client and the Web Access client are deployed as servlet-based applications in the same OC4J container. The thin client is a traditional page-to-page application and most of its application logic is located in the Applications tier. Much of the application logic for the Web Access Client, however, is in located in the JavaScript libraries loaded into the browser.

Oracle Mail Functionality

This section describes the functionality of the Oracle Mail architectural components. Oracle Mail performs different functions such as sending mail from inside or outside an organization and retrieving mail from inside an organization.

Outbound Mail

This section describes how Oracle Mail processes outbound mail.

Figure 8–2 Oracle Mail Processing Outbound Mail

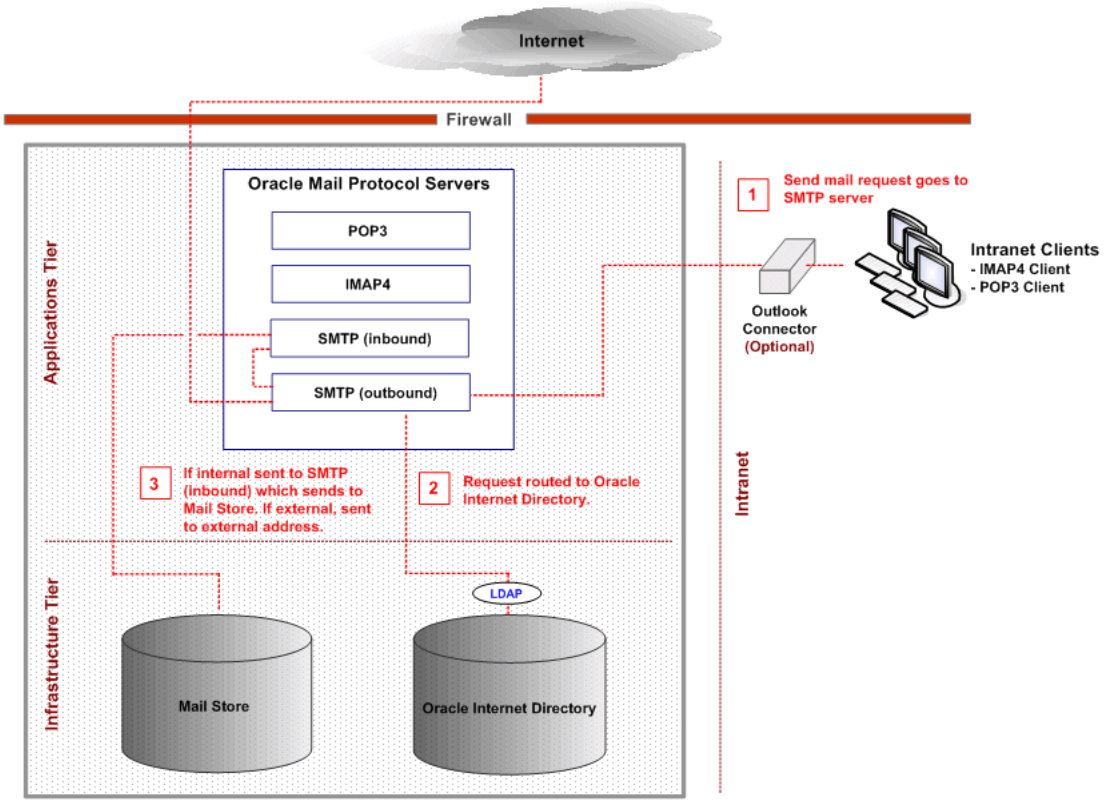


Figure 8–2 illustrates how Oracle Mail processes outbound mail:

1. A client on the organization's Intranet delivers a send mail request to the SMTP server on the application tier. Clients can include a desktop clients (POP3 or IMAP4), and Microsoft Outlook using the Outlook Connector.
2. The SMTP server routes the send mail request to Oracle Internet Directory which verifies and authenticates the recipient's address and then returns the send mail request to the SMTP server.
3. If the message recipient is internal, then the SMTP server sends the message to the SMTP (inbound) server, which delivers it to the mail store. If the recipient is external, then the SMTP server delivers the message to this individual.

Inbound Mail

This section describes how Oracle Mail processes inbound mail.

Figure 8–3 Oracle Mail Processing Inbound Mail

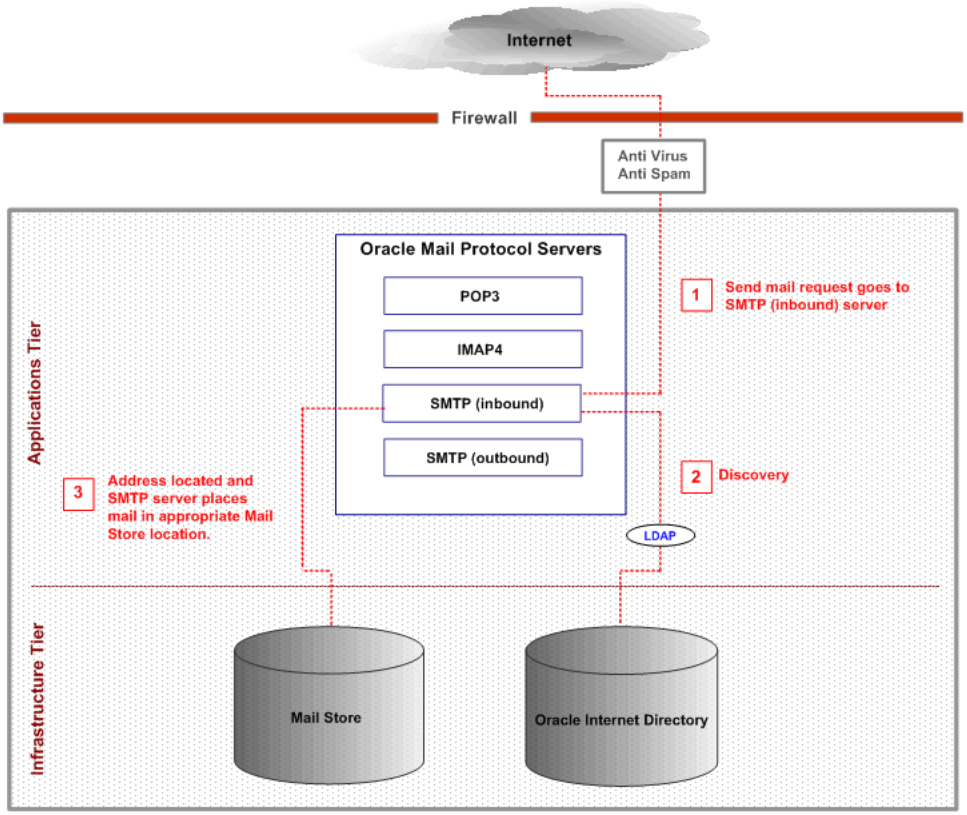


Figure 8–3 illustrates how Oracle Mail processes inbound mail:

1. A send mail request from outside the organization is delivered to the SMTP server.
2. The SMTP server uses Oracle Internet Directory for address verification and authentication.
3. Oracle Mail returns the request back to the SMTP server, which then delivers it to the mail store for user pickup or further routing and delivery.

Outbound Web Mail

This section describes how Oracle WebMail processes outbound mail.

Figure 8–4 Oracle WebMail Processing Outbound Mail

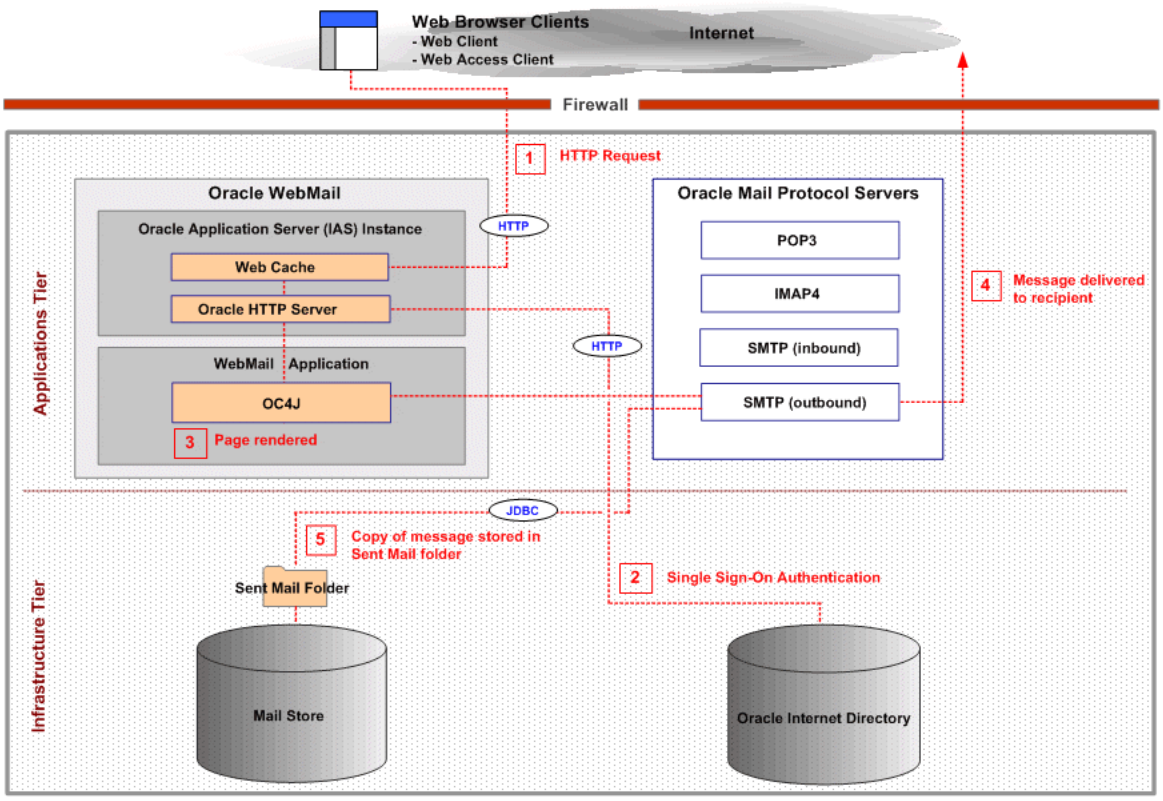


Figure 8–4 illustrates how Oracle WebMail processes outbound mail:

1. A Web client sends an HTTP request to the Web cache, which then sends the request to the Oracle HTTP Server.
2. The Oracle HTTP Server performs single sign-on authentication against Oracle Internet Directory and then forwards the request to the WebMail components in the OC4J container.
3. The OC4J container renders the page for the Oracle WebMail application. The outbound message is composed on this page and then sent to the SMTP (outbound) server.
4. The SMPT (outbound) server delivers the message to the recipient.
5. The SMTP (outbound server delivers a copy of the message to the Sent Mail folder in the mail store.

Inbound Web Mail

This section describes how Oracle WebMail processes inbound mail.

Inbound WebMail

This section describes how Oracle WebMail processes inbound mail.

Figure 8–5 Oracle WebMail Processing Inbound Mail

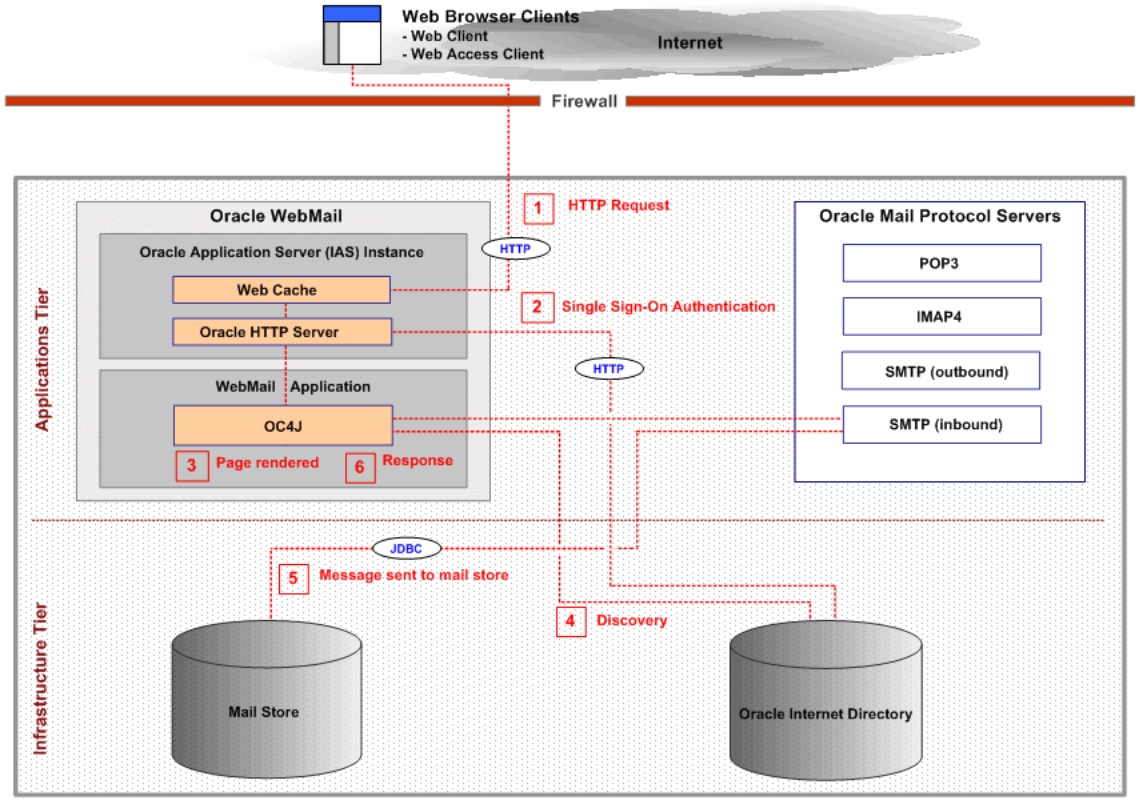


Figure 8–5 illustrates how Oracle WebMail processes inbound mail:

1. A Web client sends an HTTP request to the Web cache, which then sends the request to the Oracle HTTP Server.
2. The Oracle HTTP Server performs single sign-on authentication against Oracle Internet Directory and then forwards the request to the WebMail components in the OC4J container.
3. The OC4J container renders the page for the Oracle WebMail application. The outbound message is composed on this page and then sent to the SMTP (inbound) server.
4. Oracle WebMail performs discovery by verifying and authenticating the recipient's address, against Oracle Internet Directory and returning the request back to the SMTP (inbound) server.
5. The SMTP (inbound) server stores the message in the mail store.
6. The OC4J container renders a response page and sends it to the Web client.

Oracle Mail Retrieving E-mail Messages

This section discusses how Oracle Mail retrieves e-mail messages.

Figure 8–6 Oracle Mail Retrieving E-mail Messages

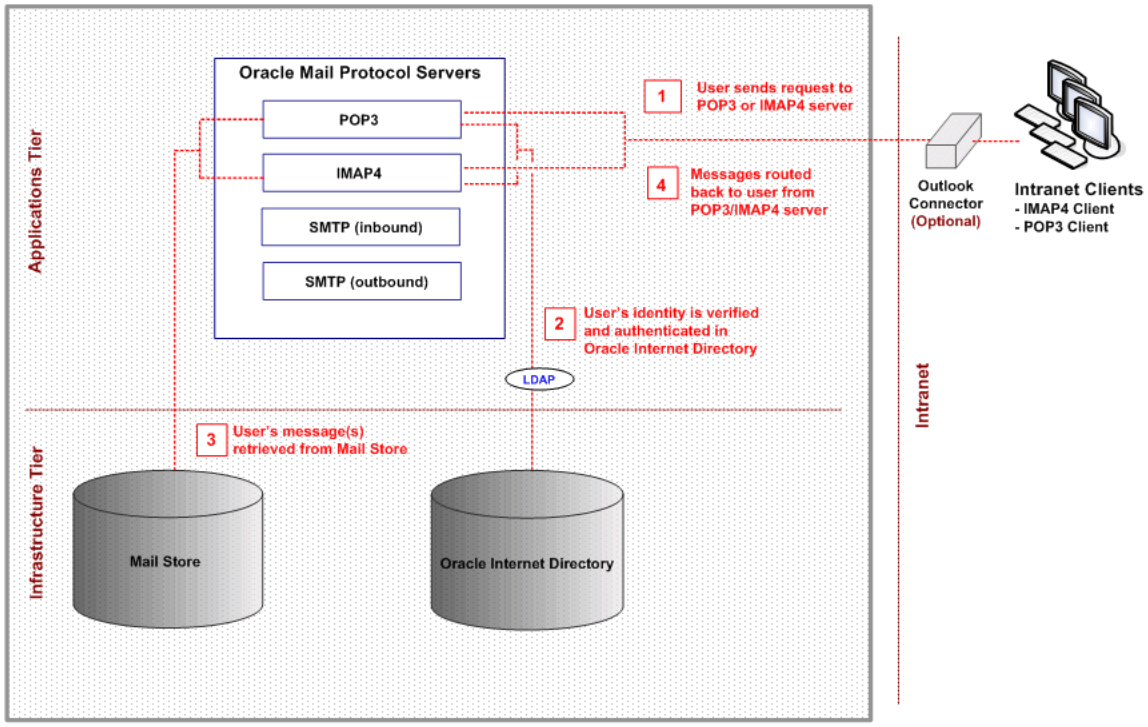


Figure 8–6 illustrates how Oracle Mail retrieves e-mail messages:

1. IMAP4 and POP3 clients send requests to their respective servers. The Oracle Connector for Outlook is optionally deployed for Microsoft Outlook clients.
2. The user's identity is verified and authenticated against Oracle Internet Directory.
3. The IMAP4 or POP3 server retrieves the user's message(s) from the mail store.
4. The IMAP4 or POP3 server routes the message(s) to the IMAP4 or POP3 client.

Oracle WebMail Retrieving E-mail Messages

This section discusses how Oracle WebMail retrieves e-mail messages.

Figure 8–7 Oracle WebMail Retrieving E-Mail Messages

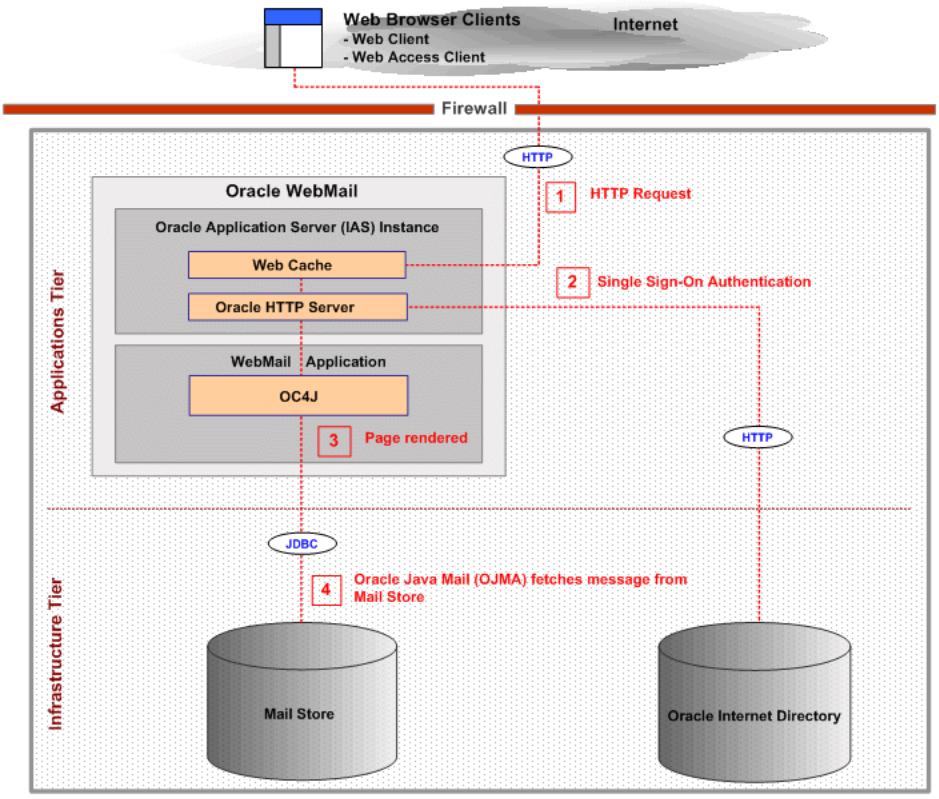


Figure 8–7 illustrates how Oracle WebMail retrieves e-mail messages:

1. A Web client sends an HTTP request to the Web cache, which then sends the request to the Oracle HTTP Server.
2. The Oracle HTTP Server performs single sign-on authentication against Oracle Internet Directory and then forwards the request to the WebMail components in the OC4J container.
3. The OC4J container renders the page for the Oracle WebMail application.
4. Oracle WebMail retrieves the message(s) from the mail store using Oracle Java Mail (OJMA), and displays the message(s) on the page rendered in the preceding step.

Planning for Oracle Mail Deployment

This section discusses issues that you must consider when planning your Oracle Mail deployment. Because deployment requirements vary among different organizations, this guide provides general guidelines and not specific instructions for deploying Oracle Mail.

Number of Users

How many users are on the existing system? The new mail system must be able to handle at least those existing users, preferably with some room to grow. Also consider the number of concurrent users on your system at peak load.

Expected Growth

How many users do you expect to add in the next 5 years? Expect your mail system to be around for several years, so rather than adding servers every time a certain number of new users are added to the system, plan your system to grow with the user population.

Anticipated Mail System Usage

Is mail central to your business or is it a relatively lightly used means of communication? How many messages do you expect to transmit and receive each day? What is the average size of these messages? If mail is heavily used or if users tend to send mails with large attachments (such as presentations or formatted papers), you may need to use larger servers to deal with the increased load. This is also important for evaluating your network bandwidth requirements, discussed later in this section.

Mail Clients

Which mail client(s) do you plan to use in your system? Oracle Mail supports IMAP4, POP3, and provides thin, web-based clients that are accessible through a standard web browser. You may choose to let users access their mail through all three protocols, or two, or just one. A POP3 system may permit a smaller back end configuration since messages are downloaded to the client machines. IMAP4 systems require more back end support because all messages are stored on the server rather than downloaded. The Oracle WebMail thin client also can use IMAP4 or can connect directly to the mail store using OJMA. Because the Oracle WebMail thin client is browser-based, it requires a Web server that accommodates the peak number of concurrent users. If Oracle WebMail uses IMAP4, then stress is placed on the Applications tier. If OJMA is used, then stress is placed on the mail store and performance is faster.

Oracle Mail enables you to separate these protocol servers into tiers apart from the message store to enabling you to distribute the load as required among Applications tier computers that can process lighter loads.

System Configuration

The size and configuration of the servers required for the new mail system depend on the preceding requirements. If your site already has available systems on hand to use for installing Oracle Mail, the diagram of available systems you created earlier will help during the planning stages. For every server in the diagram you create of your new system (every computer, dedicated protocol server, LDAP server, test system), you must determine the hardware requirements such as CPU, memory, disk, and networking requirements.

To make support easier, it is often best to chose a single hardware provider for all of your hardware. Remember that Oracle Mail does allow configurations containing different platforms. Keeping the same or similar hardware configurations as the legacy system, if appropriate, also makes migration easier.

CPU Usage

Sizing requirements for a site depends heavily on the preceding factors, and are unique for every installation, but it is important to select hardware that will provide reasonable performance. Contact your local Oracle representative to assist with analyzing your requirements for proper system configuration if needed.

Hardware Consolidation

If you plan to consolidate the number of mail servers in the system, utilize servers that can handle the peak number of concurrent users that will be on the system at the same time. Servers can be used 24x7, so the same servers can be used for users across many time zones.

N-Tiered Configuration

Oracle Mail enables you to configure your mail system to have message store, protocol servers and clients on the same machine, or on separate machines. Having larger back-end messaging servers with several commodity protocol servers may be more cost efficient for certain installations. Oracle Mail is architected so that a site can scale components as required.

Scaling Oracle Mail

This section discusses strategies for scaling Oracle Mail.

Figure 8–8 Scaling Oracle Mail Components

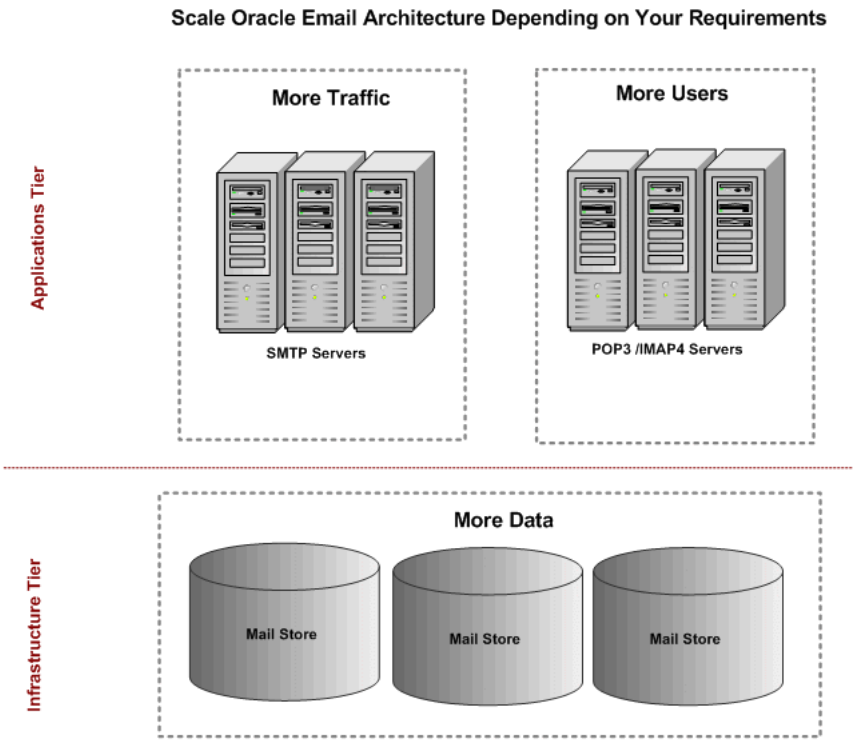


Figure 8–8 illustrates the different strategies for scaling Oracle Mail. You can add more SMTP servers to meet increasing incoming and outgoing mail requirements. You can add more POP3 and IMAP4 servers to handle an increasing number of users attempting to access their messages at the same time. You can add more mail stores if you want to store more e-mail messages, however this should not be used for archiving purposes. The "Oracle Mail Deployment Configurations" section contains additional tiering options.

Disk Configuration

How much mail do you expect to store? Looking at the size of the legacy mail system should give you an idea of the disk storage required for your system. Imposing quotas on users is one way to limit growth of the message store, but remember that quotas that are too small or are too sharply reduced from previous limitations (if any) will result in a user population that constantly clamors for increased storage space. Messages will still be received into the application, but users who are over their quota will not be able to retrieve their new message until they have cleaned up their accounts.

Knowing the size of the user accounts will also help you determine the size of each batch of users to migrate.

The Oracle Mail application should also have a disk configuration that meets other critical requirements such disk mirroring, stripping, and disk partitioning, all of which will help in redundancy solution of your installation.

Network Topology and Bandwidth

Oracle Mail requires that there be good network connectivity between all sites involved. During the migration process, it is essential for all remote and local sites to have good throughput to an Oracle Mail installation in order to move legacy information to the new system in a timely manner.

mail clients access messages in Oracle Mail by sending requests to Oracle Mail's IMAP4 or POP3 protocol servers. Oracle Mail'S. IMAP4 and POP3 protocol servers use shared server processes (SPS) to service multiple clients with fewer database connections. SPS provides load balancing by using an Oracle Mail listener to distribute the client load equally across multiple instances of the protocol server processes. Therefore, an analysis of network bandwidth and connectivity is necessary and the network re-configured if necessary to provide reasonable performance to access messages.

Generally, mail size varies too much to be used as an accurate measurement for bandwidth needs. However, if your mail traffic tends to include large attachments such as graphics this should be taken into consideration. Another method to check network usage is to measure peak day and hour mail traffic load at several representative locations, for two or more weeks, then divide the peak hour traffic by the total number of users. Knowing the number of incoming and outgoing messages helps gauge the load capacity required of the SMTP server. (It also helps in the decision of the Applications tier solution.) The following numbers are rough estimates for average network bandwidth requirements for 100 concurrent users. These numbers should be added to the values for the existing network usage.

Table 8–1 average network bandwidth requirements for 100 concurrent users

User Profile	Bandwidth on Application Tier	Bandwidth on Infrastructure Tier
ISP	2.9 Mbps	1.2 Mbps
Corporate	4 Mbps	1.8 Mbps

Note: The application tier is composed of the IMAP4, POP3, and SMTP processes.

Security

How much security is needed by your site? Firewalls are helpful in preventing unauthorized access to internal systems that may contain sensitive information. Anti-virus programs may help prevent or limit electronic viruses spread through mail. Third party anti-virus programs that work with MTAs can be used with Oracle Mail. Oracle Mail also provides server side rules that administrators (or end users) can use to screen out suspicious mails. Oracle Mail is shipped with a virus cleanup tool that cleanses the message store of viruses that have already entered the system.

DNS Evaluation

Since Oracle Mail and the Internet utilize domain name servers (DNS) for host and domain resolution it is always a good practice to evaluate the DNS entries for your site. Every host in your e-mail system involved in determining where to direct a piece of e-mail has a Mail Exchanger (MX) record in the DNS so that external as well as internal servers know where to direct messages. Make sure that all hosts involved can be seen through the DNS. In the event that you choose to run sendmail from a UNIX computer and run Oracle Mail on NT, you can configure the UNIX version of sendmail to connect and deliver mail remotely to your installation.

Directory Services Information

Oracle Mail makes use of Oracle Internet Directory during a migration to map attributes and objects directly into Oracle Internet Directory.

All information is transferred to Oracle Internet Directory. If you choose to maintain a separate human resources (HR) directory as the source of truth for directory information, then you can redirect information from your HR installation to automatically update Oracle Mail for synchronized, up-to-date directory information using the Oracle Software Developers Kit (SDK).

Oracle Mail is LDAP-compliant so you can maintain your old LDAP installation for legacy purpose.

Determine user Naming Conventions

It is important to determine the naming convention of your users. Your organization may already be an internal standard such as `user_x` or `user_name`. Oracle Mail enables for the standard name convention of `Firstname.Lastname`, which means that account names can have meaningful, rather than cryptic, names.

Oracle WebMail Planning Issues

This section describes planning issues for deploying Oracle WebMail.

Scaling Oracle WebMail

The single-computer install is recommended only for a small numbers of concurrent users, since CPU and disk I/O are shared with the Infrastructure tier components including Oracle Internet Directory and the mail store. To scale for larger numbers of concurrent users, Oracle recommends placing multiple Applications tier computers hosting Oracle WebMail behind a load-balancer. illustrates scaling Oracle WebMail Applications tier computers.

Figure 8–9 Scaling Oracle WebMail Applications Tier Components

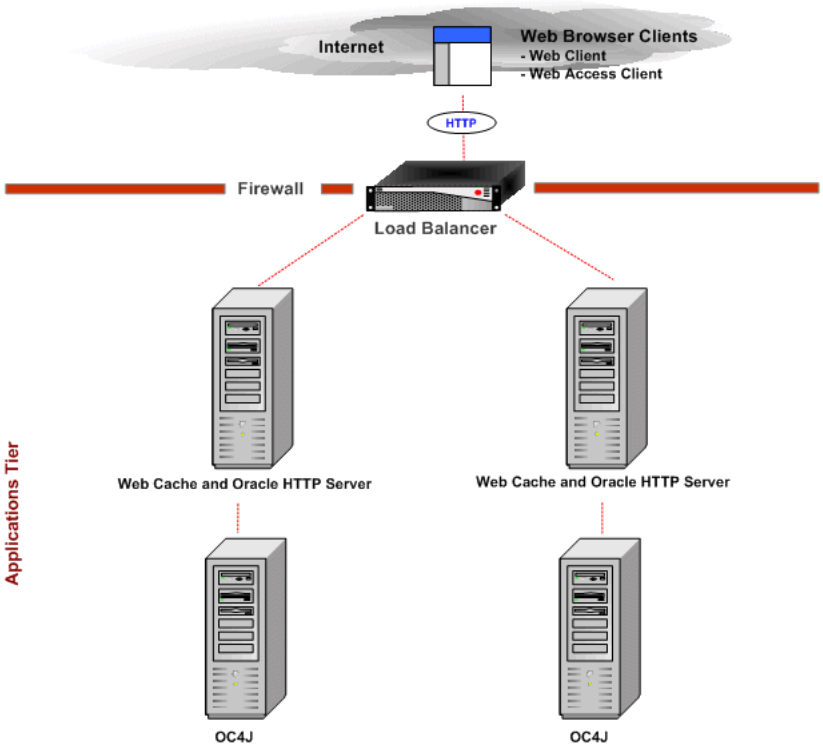


Figure 8–9 illustrates a common method for scaling Oracle WebMail Applications tier components. In this figure a load balancer distributes traffic between two computers that each contain the Web cache and Oracle HTTP server. Each of these computers sends traffic to one of two computers that contain the Oracle WebMail OC4J container. If one Oracle computer containing either the Web cache and Oracle HTTP Server or the OC4J container experiences failure, the load balancer routes traffic to the remaining computer with the Web cache and Oracle HTTP server. Oracle WebMail uses Web Cache clustering and must have session binding turned on when using this feature.

Sizing the JVM Heap

Typically, Oracle WebMail requires 2-3MB each concurrent user in sizing the JVM heap. You should also be aware of any operating system-specific limitations on memory addressing that may be present on your hardware.

Connection Pools

The sizing of the connection pools used by Oracle WebMail vary depending on usage requirements and resources. Too few connection pools will result in poor performance and limited scalability, but too many can unnecessarily use up database resources.

Sending Messages

Oracle WebMail supports the ability to send messages either to the SMTP server(s) or directly into the mail store using a database connection. The first method requires two network hops but takes advantage of very efficient SMTP connection pooling to the database. The second method shares database connections with the same ones used for retrieving data from the mail store, but supports authenticated sending.

Oracle Mail Deployment Configurations

Oracle Mail deployment configurations follow the same guidelines as those for Oracle Collaboration Suite. For information on deploying Oracle Mail in a single-computer, multiple-computer, or high availability environment, please refer to Chapter 3, "Deploying Oracle Collaboration Suite".

Oracle Connector for Outlook

Oracle Connector for Outlook enables Microsoft Outlook users to access Oracle Mail. For information on deploying Oracle Connector for Outlook, please refer to the "Deploying Oracle Connector for Outlook" section of Chapter 5, "Deploying Oracle Calendar".

9

Deploying Oracle Mobile Collaboration

This chapter contains the following topics:

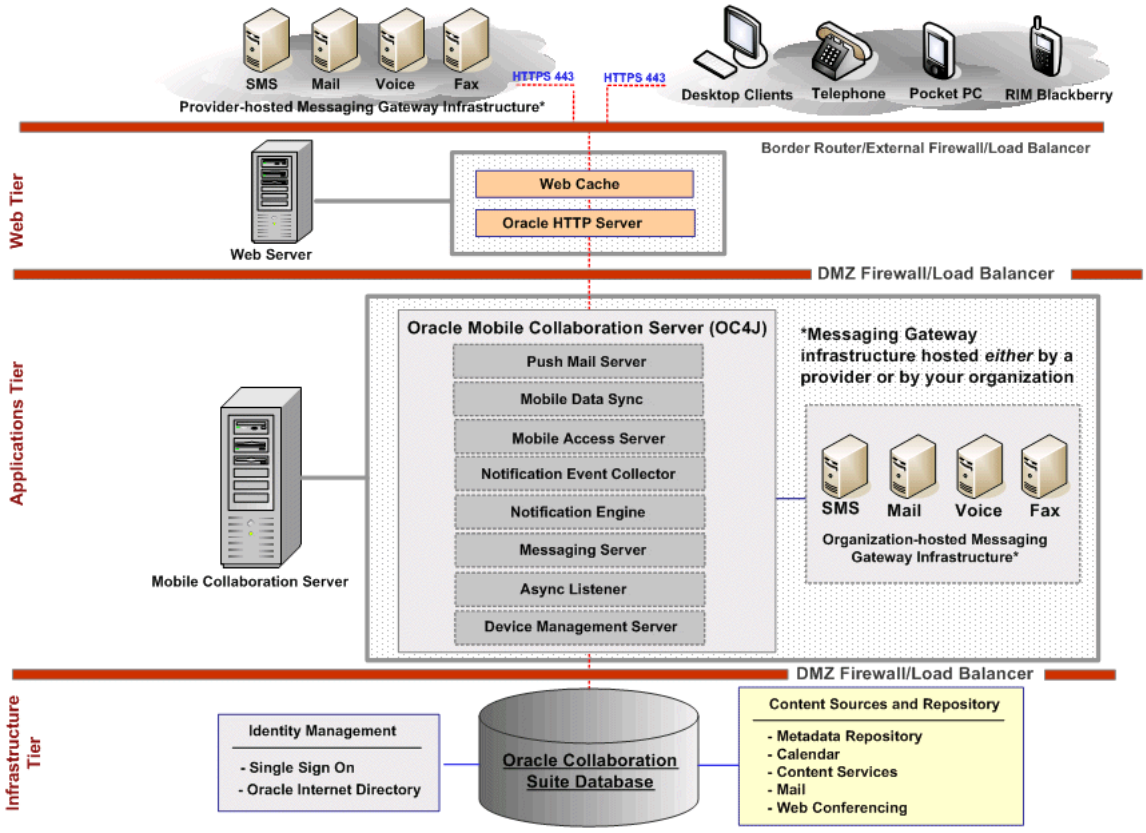
Understanding the Oracle Mobile Collaboration Architecture and Functionality

This section discusses the architecture and functionality of Oracle Mobile Collaboration.

Oracle Mobile Collaboration Architecture

Oracle Mobile Collaboration provides users with continuous access to enterprise collaboration data such as e-mail, voice mail, calendar data, address book information, online files, and employee directories, from any location, using any mobile device. Consequently Oracle Mobile Collaboration is deployed on the Applications tier to access other Oracle Collaboration Suite data on the Infrastructure tier. Figure 9–2 illustrates the Oracle Mobile Collaboration architecture.

Figure 9–1 Oracle Mobile Collaboration Architecture



In Figure 9–1 Oracle Mobile Collaboration is deployed across three tiers, the Infrastructure tier, Applications tier and the Web tier.

Infrastructure Tier

The Infrastructure tier is deployed behind a DMZ firewall with an optional load balancer.It contains an Oracle Database 10*g* with Identity Management components, as well as the content sources and repository.

Identity Management

Identity management is comprised of OracleAS Single Sign-On and Oracle Internet Directory.

Content Sources and Repository

The contents sources and repository comprise content from the various Oracle Collaboration Suite Applications accessed by Oracle Mobile Collaboration clients as well as the metadata repository. Content sources include Oracle Calendar, Oracle Content Services, and Oracle Mail.

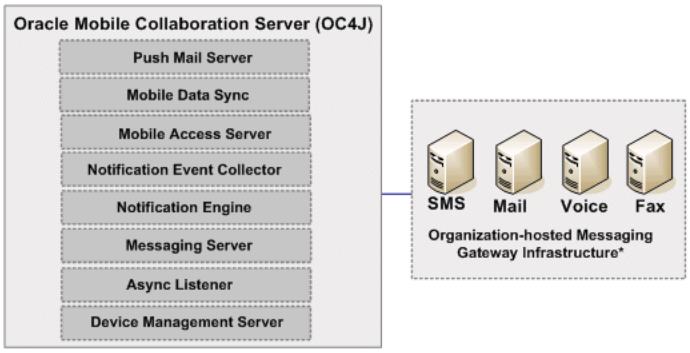
Applications Tier

The Applications tier is deployed in a DMZ with optional load balancers. It contains the Oracle Mobile Collaboration server and the messaging gateway infrastructure. The messaging gateway infrastructure can optionally be hosted by your organization on the Applications tier, or by a provider.

Oracle Mobile Collaboration Server

 illustrates the Oracle Mobile Collaboration Server with the messaging gateway infrastructure.

Figure 9–2 Oracle Mobile Collaboration Server with Messaging Gateway Infrastructure



- **Mobile Access Server**:Provides the wireless browsing feature.
- **Push Mail Server**: Provides the push mail feature.
- **Device Management Server**: Provides the over-the-air installation, update, and install of push mail and SyncML client programs on the devices of the user.
- **Notification Engine**: Communicates with the devices and sends UDP or SMS notification messages to the devices.
- **Notification Event Collector**: Collects the following events.
  - Unified Messaging (UM) events de-queued from the e-mail server
  - Events for which the Calendar Server listens
  - UDP events for which various Push Mail devices listen.
- **Mobile Data Sync**: Delivers remote synchronization of data stored in Oracle Collaboration Suite, including Calendar events, tasks and contacts, with any OMA-DS-enabled (formerly SyncML) device. See "Deploying Oracle Mobile Data Sync" in Chapter 5, "Deploying Oracle Calendar".
- **Messenging Server**: Delivers all Oracle Mobile Collaboration message types including messages and notifications.
- **Async Listener**: Processes all asynchronous requests for Oracle Collaboration Suite data. It currently supports e-mail and SMS channels.

Messaging Gateway Infrastructure

In , the messaging gateway infrastructure is a hosted messaging gateway that is actually a collection of transport gateways, each catering to a particular delivery method or channel. Oracle Application Server provides the platform to combine these various transport gateways in a single environment. The messaging gateway infrastructure is optionally deployed on the Applications tier, or is hosted by a third party. The messaging gateway infrastructure contains the following components:

- **SMS (Short Message Service)**: Retrieves text messages from the Oracle Mobile Collaboration server and delivers them to end-user devices.

- **Mail**: Retrieves e-mail messages from the Oracle Mobile Collaboration server and delivers them to end-user devices.
- **Voice**: Retrieves voice messages from the Oracle Mobile Collaboration server and delivers them to end-user devices.
- **Fax**: Retrieves fax messages from the Oracle Mobile Collaboration server and delivers them to end-user devices.

Web Tier

The Web tier is deployed between two firewalls, with an optional border router or load balancer. It contains the Web server, which runs Web cache and the Oracle HTTP Server. You can optionally deploy the Web server in a Web tier configuration, or you can deploy it on the Applications tier, effectively clubbing the Web tier and Applications tier.

Clients and Messaging Gateway Infrastructure

The Oracle Mobile Collaboration server is accessed from a variety of clients including, desktop clients, telephones, pocket PCs, or RIM Blackberry devices. Clients access the Oracle Mobile Collaboration server using one of the following gateways, on the Messaging Gateway Infrastructure.

Note: All Oracle Mobile Collaboration components except for P-IMAP are able to operate with Web Cache.

Oracle Mobile Collaboration Functionality

This section describes the functionality of the Oracle Mobile Collaboration architectural components. Oracle Mobile Collaboration performs different functions such as:

- Unified Messaging
- Calendar Notifications
- Ask E-mail
- Ask SMS
- Voice Requests for Oracle Collaboration Suite Data

Unified Messaging

Users can receive notifications about Unified Messaging events such as the arrival of new e-mail from specific individuals, or new fax or messages marked urgent, through various delivery channels such as SMS, e-mail, voice, or fax.

Figure 9–3 Unified Messaging Flow

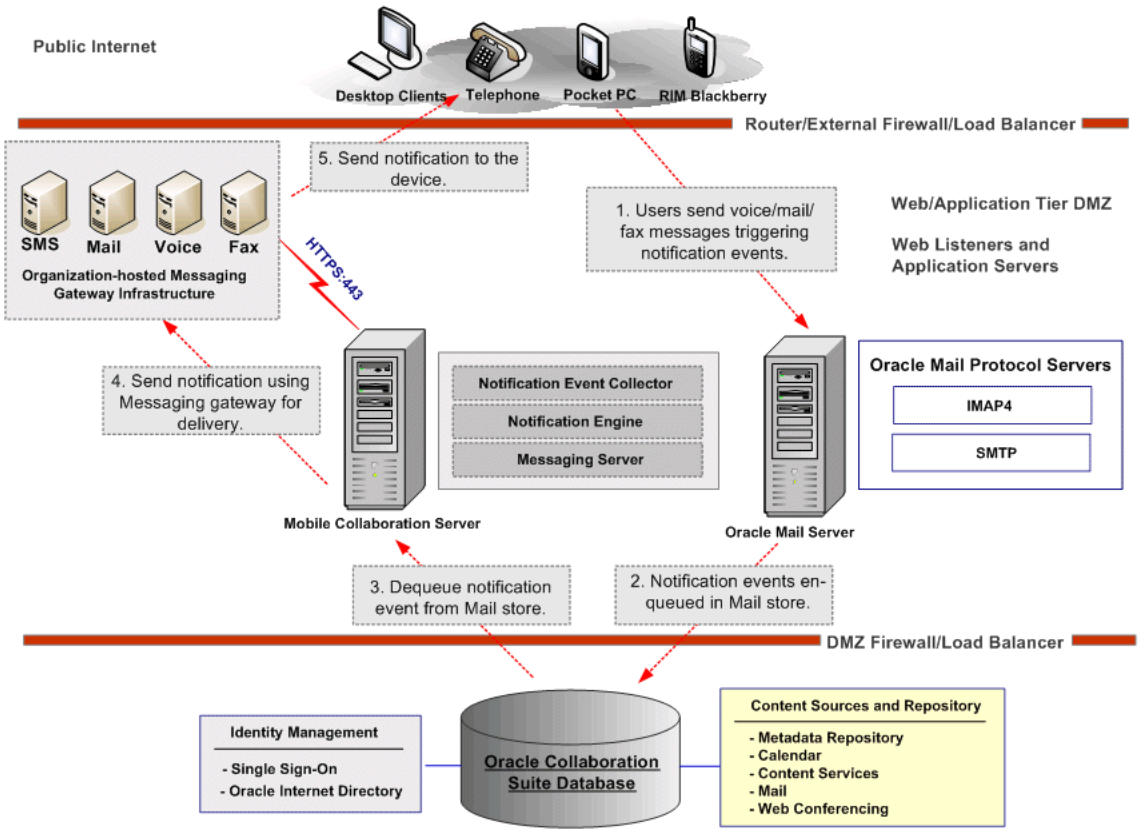


Figure 9–3 illustrates the following flow for delivering unified messages to end-users with Oracle Mobile Collaboration:

1. Users send voice, e-mail, or fax messages that trigger notification events.
2. Notification events are enqueued in the mail store which in this example is one of the repositories in the Oracle Collaboration Suite database.
3. The mail store sends a dequeue notification.
4. The notification is sent using the messaging gateway for delivery.
5. The notification is sent to the device.

Calendar Notifications

Users can receive notifications about calendar events like new meetings, updated meetings, or cancelled or deleted meetings from various delivery channels including SMS, E-mail, voice or fax.

Figure 9–4 Calendar Events Flow

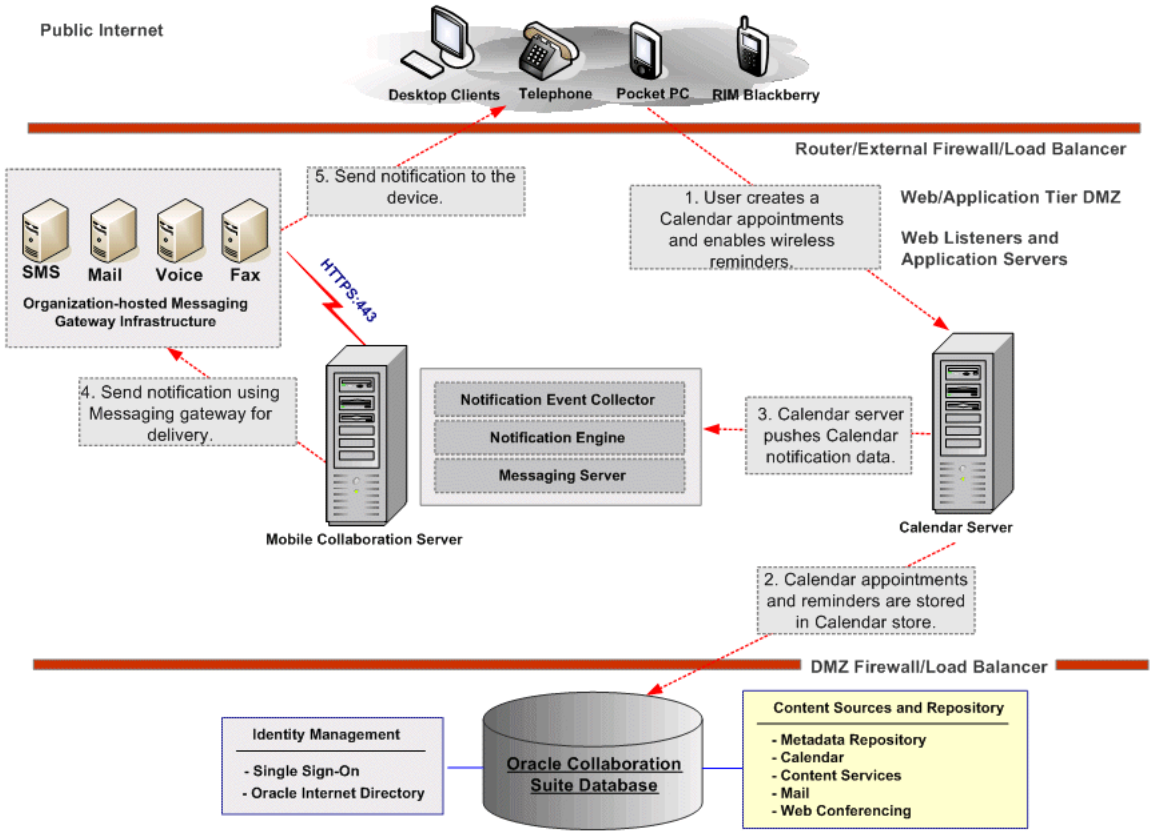


Figure 9–4 illustrates the following flow for delivering calendar events to end-users with Oracle Mobile Collaboration:

1. Users create Calendar appointments and enable wireless reminders.
2. Calendar appointments and reminders are stored in the calendar database. The calendar database is deployed on the Applications tier as part of the calendar server. Information is also written to the Oracle Collaboration Suite database which contains the Oracle Calendar metadata.
3. The calendar server pushes the calendar notification data to the Oracle Mobile Collaboration server.
4. The notification is sent using the messaging gateway for delivery.
5. The notification is sent to the device.

Ask E-mail

With the Ask E-mail feature, users can retrieve corporate collaboration data by sending an e-mail message to the Oracle Mobile Collaboration server. The Oracle Mobile Collaboration server sends a text response that contains the requested data.

Figure 9–5 Ask E-mail Flow

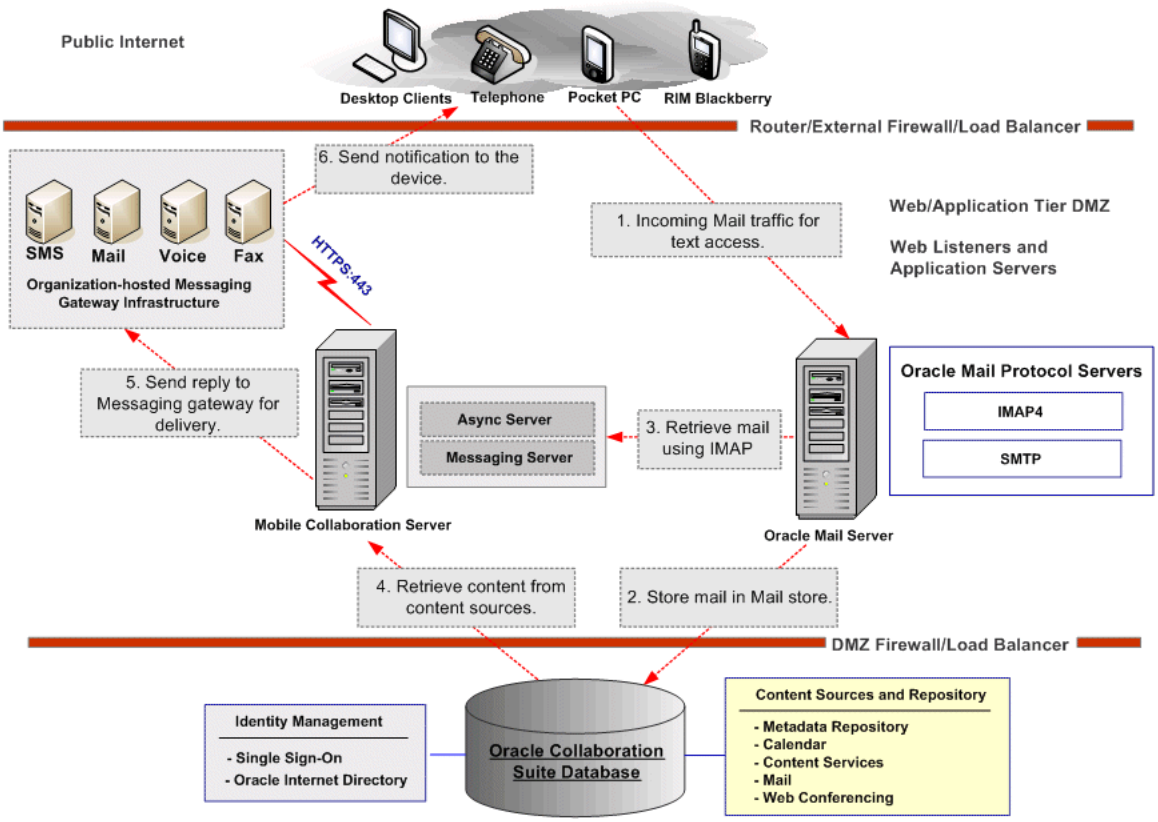


Figure 9–5 illustrates the following flow for send e-mail messages to request corporate data and to receive the requested data on a wireless device:

1. Users send e-mail messages requesting text access to corporate data.
2. The e-mail message is sent to the mail store which in this example is one of the repositories in the Oracle Collaboration Suite database.
3. The Oracle Mobile Collaboration server retrieves the e-mail request using the IMAP protocol.
4. The Oracle Mobile Collaboration server retrieves content from the appropriate repository in the Oracle Collaboration Suite database. If The Oracle Mobile Collaboration server is retrieving calendar data, then it does so from the calendar server which is deployed on the Applications tier.
5. The notification is sent using the messaging gateway for delivery.
6. The notification is sent to the device.

Ask SMS

Users can retrieve corporate collaboration data by sending a short message (SMS) to the Oracle Mobile Collaboration server and which replies with a text response that contains the requested data.

Figure 9–6 Ask SMS Flow

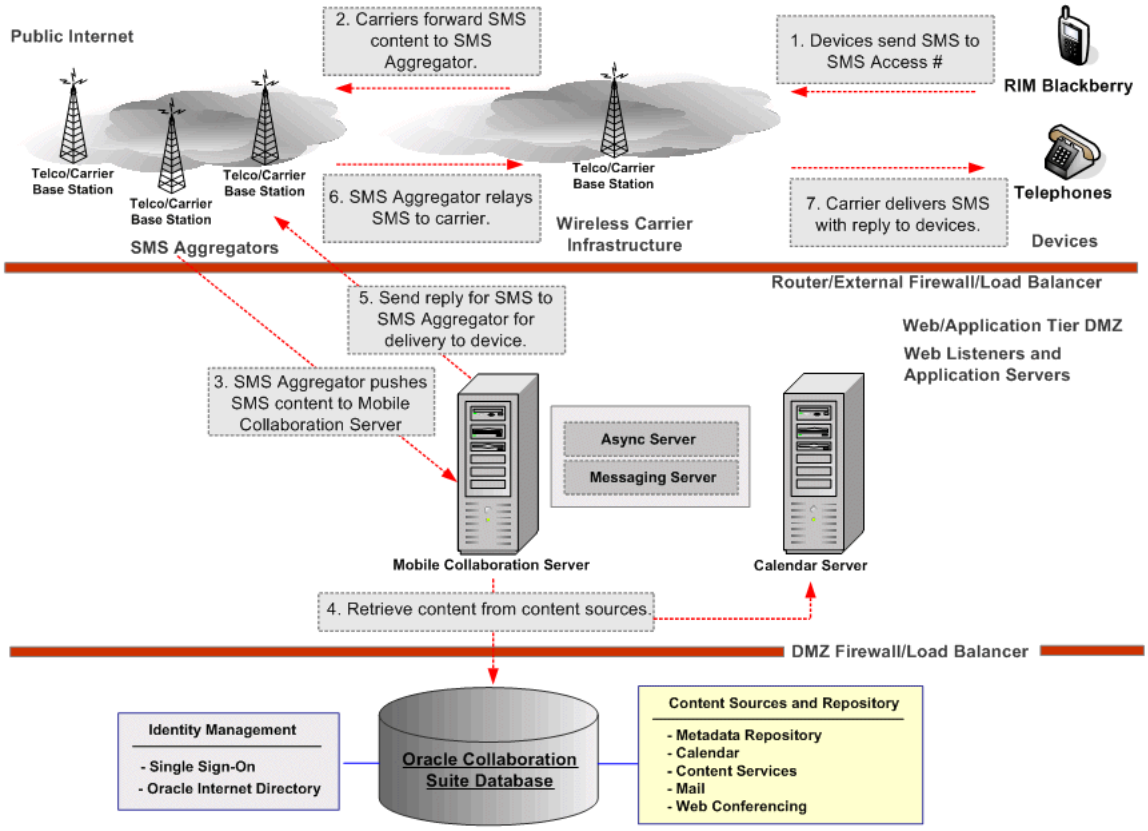


Figure 9–6 illustrates the following flow for delivering unified messages to end-users with Oracle Mobile Collaboration:

1. Devices send SMS to SMS Access #
2. Carriers forward SMS content to SMS Aggregators.
3. SMS Aggregators push SMS content to the Oracle Mobile Collaboration server.
4. The Oracle Mobile Collaboration server retrieves content from the appropriate repository in the Oracle Collaboration Suite database. If The Oracle Mobile Collaboration server is retrieving calendar data, then it does so from the calendar server which is deployed on the Applications tier.
5. SMS sends a reply to the SMS Aggregator for delivery to the requesting devices.
6. The SMS Aggregator relays the request to the SMS to carrier.
7. The carrier delivers SMS with reply to the requesting devices.

Voice Requests for Oracle Collaboration Suite Data

Users can make voice requests for Oracle Collaboration Suite data and receive these requests from the target applications through the Voice XML Gateway and the Oracle Mobile Collaboration server.

Figure 9–7 Voice XML Gateway

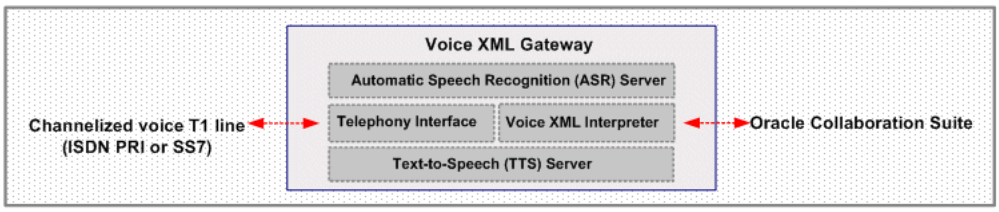


Figure 9–7 illustrates the Voice XML Gateway. The Voice XML Gateway is comprised of the following:

- **Automatic Speech Recognition (ASR) server**: Performs speech recognition.
- **Telephony Interfaces**: Communicates with end-user devices.
- **Voice XML Interpreter**: Interprets VoiceXML language generated by Oracle Mobile Collaboration server.
- **Text-to-Speech (TTS) server**: Performs text-to-speech conversion.

Voice Requests for Oracle Collaboration Suite Data Process Flow

illustrates the process flow for making voice requests for Oracle Collaboration Suite data.

Figure 9–8 Voice Request for Oracle Collaboration Suite Data Process Flow

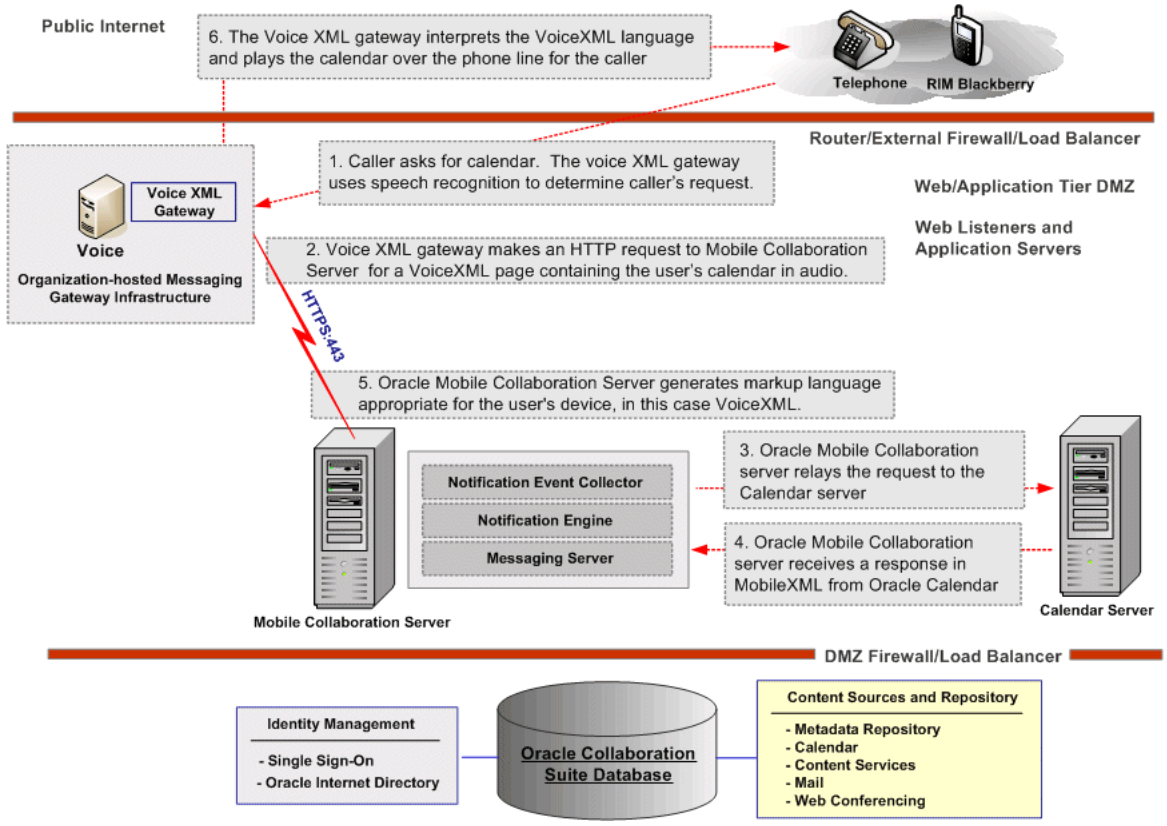


Figure 9–8 illustrates the following process flow:

1. The caller requests Oracle Calendar. The voice XML gateway uses speech recognition to determine caller's request.
2. Voice XML gateway makes an HTTP request to Mobile Collaboration Server for a VoiceXML page containing the user's calendar in audio.
3. Oracle Mobile Collaboration server relays the request to the Calendar server.
4. Oracle Mobile Collaboration server receives a response in MobileXML from Oracle Calendar.
5. Oracle Mobile Collaboration Server generates markup language appropriate for the user's device, in this case VoiceXML.
6. The Voice XML gateway interprets the VoiceXML language and plays the calendar over the phone line for the caller.

Planning for Oracle Mobile Collaboration Deployment

This section discusses planning issues for an Oracle Mobile Collaboration Server deployment.

Oracle Mobile Collaboration Internal Deployment Requirements

This section discusses the internal requirements for deploying Oracle Mobile Collaboration in your organization. The following Oracle Collaboration Suite components must be configured to successful host a complete Oracle Mobile Collaboration solution:

DMZ Environment

Oracle Collaboration Suite provides users with continuous access to corporate e-mail, voice mail, calendar, address book, online files, and employee directories, from any location, using any mobile device. To provide access to corporate content, the Oracle Mobile Collaboration Server component must be deployed and configured correctly. Because most wireless protocols are unable to communicate through traditional firewalls, a special deployment environment must be set up in a DMZ to deploy the Oracle Mobile Collaboration Server component. The DMZ environment must contain an external firewall and a hardware load balancer. For security reasons, only Port 80 and Port 443 are opened on the external firewall for incoming HTTP and HTTPS connections respectively. All requests are routed to the Applications tier from the hardware load balancer.

Notification Engine

The notification event collector and notification delivery server operate together to process UM and Calendar notification events, and to pass the events to the messaging server for ultimate delivery to devices.

Messenging Server

The messaging serve is capable of communicating with various gateways such as the voice gateway, SMS Telco Providers, e-mail gateway or fax gateway for delivering messages. The messaging server can also communicate with a hosted messaging gateway, using the Push driver.

Push Mail Functionality

Oracle Mobile Collaboration Server Push Mail functionality must be to be configured to bypass the Web Cache when routing requests from devices over the internet, directly to the Oracle HTTP Server. To accomplish this, an independent URL with a virtual host is required in your Oracle HTTP Server configuration.

Oracle Mobile Collaboration External Deployment Requirements

This section discusses the external requirements for deploying Oracle Mobile Collaboration in your organization. The following external components must be configured to successful host a complete Oracle Mobile Collaboration solution:

Messenging Gateway Infrastructure Connectivity

Connectivity to a Messaging Gateway Infrastructure for pushing SMS, E-mail, Fax, or Voice messages over the Internet is required. A hosted messaging gateway is actually a collection of transport gateways, with each providing a specific delivery method or channel. Oracle Application Server provides the platform to combine these various transport gateways together under a single umbrella.

SMS Telco or Aggregator Service Level Agreement

For text messaging (2-way asynchronous requests) through SMS channel, a Service Level Agreement with either a SMS Telco provider or an SMS aggregator provider is required.

Oracle Mobile Collaboration Deployment Configurations

Oracle Mobile Collaboration deployment configurations follow the same guidelines as those for Oracle Collaboration Suite. For information on deploying Oracle Mobile Collaboration in a single-computer, multiple-computer, or high-availability environment, refer to Chapter 3, "Deploying Oracle Collaboration Suite".

10

Deploying Oracle Real-Time Collaboration

This chapter contains the following topics:

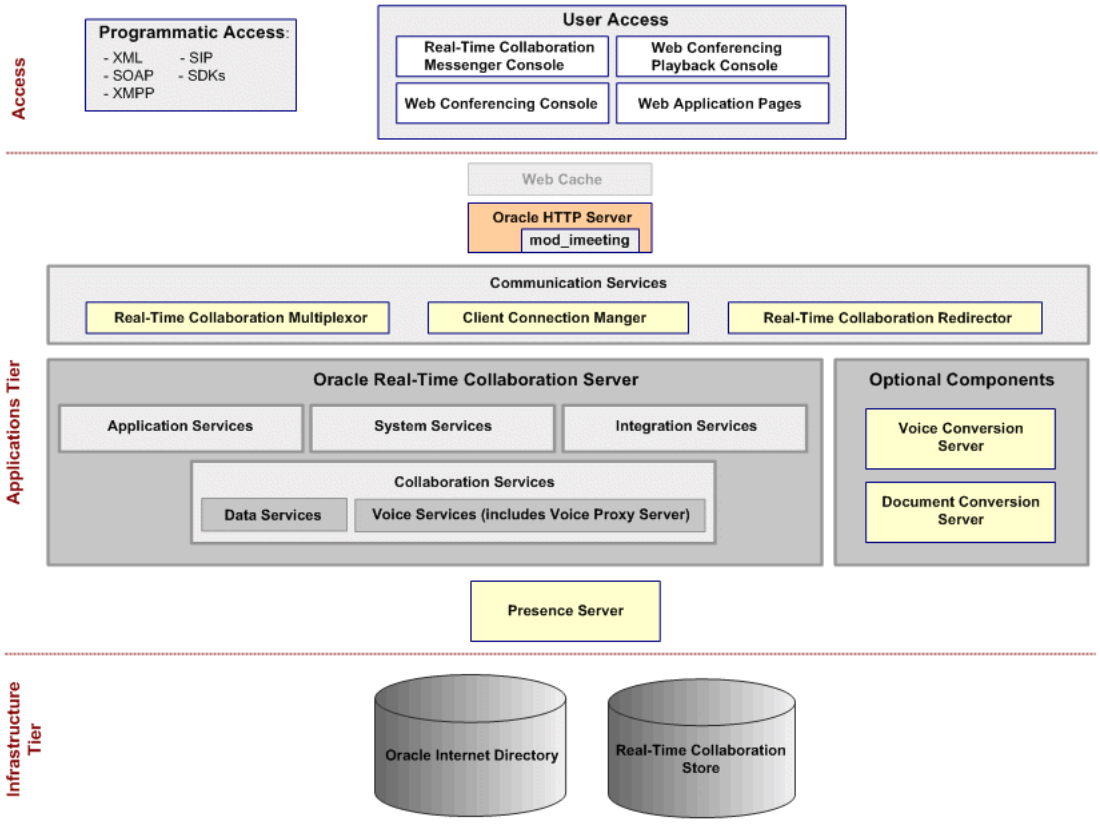
Understanding the Oracle Real-Time Collaboration Architecture, Functionality, and Access Requirements

This chapter provides the conceptual background required to deploy Oracle Real-Time Collaboration. It provides an overview of the Oracle Real-Time Collaboration architecture which is a discussion of deployment planning issues and deployment configurations.

Oracle Real-Time Collaboration Architecture

This section describes the Oracle Real-Time Collaboration architecture.

Figure 10–1 Oracle Real-Time Collaboration Architecture



Infrastructure Tier

In Figure 10–1, the Infrastructure tier contains the following:

- **Oracle Internet Directory** for user authentication and verification
- **Oracle Real-Time Collaboration Store** for storing Web conferencing information.

Applications Tier

In , the Applications tier contains the Oracle HTTP Server and the Oracle Real-Time Collaboration server. The Oracle HTTP Server is used as the listening point for end-user connection requests over the Internet to the Oracle Real-Time Collaboration system. Web cache is automatically installed with Oracle Real-Time Collaboration but is typically not used with the product. The Oracle HTTP Server runs with the `mod_imeeting` service, which does the following:

- Provides unified HTTP listening point
- Passes inbound connections as sockets to the Real-Time Collaboration Multiplexer
- For the Cobrowse mode distributes page content to the browsers of the clients.

The Oracle Real-Time Collaboration Server contains the following components:

Communication Services

Oracle Real-Time Collaboration contains the following communication services:

- **Real-Time Collaboration Multiplexer**: Real-Time Collaboration Multiplexer acts as a communications hub between Web Conferencing console clients (end users participating in a conference) and Web Conferencing servers. It does the following:
  - Accepts inbound connections from Web Conferencing console clients and Web Conferencing Servers.
  - Routes data traffic between all clients and all Web Conferencing Servers on a system.
- **Client Connection Manager**: The Client Connection Manager handles all connections between Oracle RTC Messenger clients (end users participating in chat sessions) and the RTC Messenger router.
- **Real-Time Collaboration Redirector**: The Real-Time Collaboration Redirector redirects accepted connections to the appropriate Oracle Real-Time Collaboration communication processes. These include the Real-Time Collaboration Multiplexer for Web conferences or the Client Connection Manager for chat sessions. The Real-Time Collaboration Redirector also load balances between all requests, sending the connections to the most appropriate, available multiplexer or connection manager.

Application Services

Application Services provide the scheduling and reporting features of the Web Client pages.

System Services

System Services provide system management through properties, statistics reporting, and process monitoring.

Integration Services

Integration Services can be used to tightly integrate any application to the Oracle Real-Time Collaboration functions.

Collaboration Services

Oracle Real-Time Collaboration contains the following collaboration services:

- Data Services
- Voice Services including the voice proxy server. The Voice Proxy server handles real-time, two-way voice communications during voice chat sessions in RTC Messenger, and during voice chats with PC microphone in Web Conferencing.

Presence Server

The Oracle Presence Server provides the services required for instant messaging, chat conferences, and publishing the presence of Oracle Messenger users. There can be more than one Oracle Presence Server in an Oracle Real-Time Collaboration deployment, but only one server runs at a time. If the first goes down, then a special high-availability process associated with each server will start the next.

Voice Conversion Server (Optional)

The Voice Conversion server is used to support streaming voice data during a Web conference and playback of recorded conferences. During a Web conference, it dials in to a voice conferencing system, captures the analog voice stream, digitalizes it, and streams it to a Web Conferencing Server process through the multiplexer. In the figure, the Voice Conversion server is shown residing on another physical computer than

most other Oracle Real-Time Collaboration processes. The Voice Conversion server must be installed on a Windows computer, and has associated required hardware requirements.

Document Conversion Server (Optional)

The Document Conversion server converts Microsoft Office documents to HTML for document presentation. The Oracle Real-Time Collaboration Application provides the front end for a user to convert a document. Like the Voice Conversion server, the Document Conversion server must be installed on a Windows computer.

Programmatic and User Access

This section lists the programmatic access and user access components of the Oracle Real-Time Collaboration architecture.

Programmatic Access

In , programmatic Access includes the following:

- XML
- SOAP
- XMPP
- SIP
- SDKs

User Access

In , user Access includes the following:

- Real-Time Collaboration Messenger Console
- Web Conferencing Console
- Web Conferencing Playback Console
- Web Application Pages

Oracle Real-Time Collaboration Functionality

This section describes the functionality of the Oracle Real-Time Collaboration architectural components.

Oracle Real-Time Collaboration System Terminology

The following terminology must be understood before deploying Oracle Real-Time Collaboration:

Component

A component is a set of one or more identical Oracle Real-Time Collaboration processes that can be considered as logical processes from an operating system perspective. Examples include the Oracle Real-Time Collaboration multiplexer, `mod_imeeting`, and the Oracle Web Conferencing Server.

Instance

An instance is a group of Oracle Real-Time Collaboration components that share the same Oracle Real-Time Collaboration Home. For example, a group of Oracle Real-Time

Collaboration instances running in the United States could be referred to as US Instance 1, and US Instance 2.

Cluster

A cluster is a group of one or more Oracle Real-Time Collaboration Instances that form a logical unit. Clusters provide load balancing, high availability, sharing of Oracle Real-Time Collaboration voice and document conversion services, and ease of management. For example, an organization could have Oracle Real-Time Collaboration clusters in different geographic regions such as the United States (US Cluster) and the United Kingdom (UK Cluster).

Site

A site is set of Oracle Real-Time Collaboration services exposed to a line of business. Examples may include the direct site, development site, and support site of an organization.

System

A system is a group of one or more Oracle Real-Time Collaboration Clusters that share the same Oracle Real-Time Collaboration Repository. For example, `http://iMeeting.acme.com` could encompass a US Cluster and UK Cluster of an organization, both of which share the same Oracle Real-Time Collaboration repository.

Oracle Real-Time Collaboration Component Interaction

This section describes the interaction between Oracle Real-Time Collaboration components.

Figure 10–2 Oracle Real-Time Collaboration Component Interaction

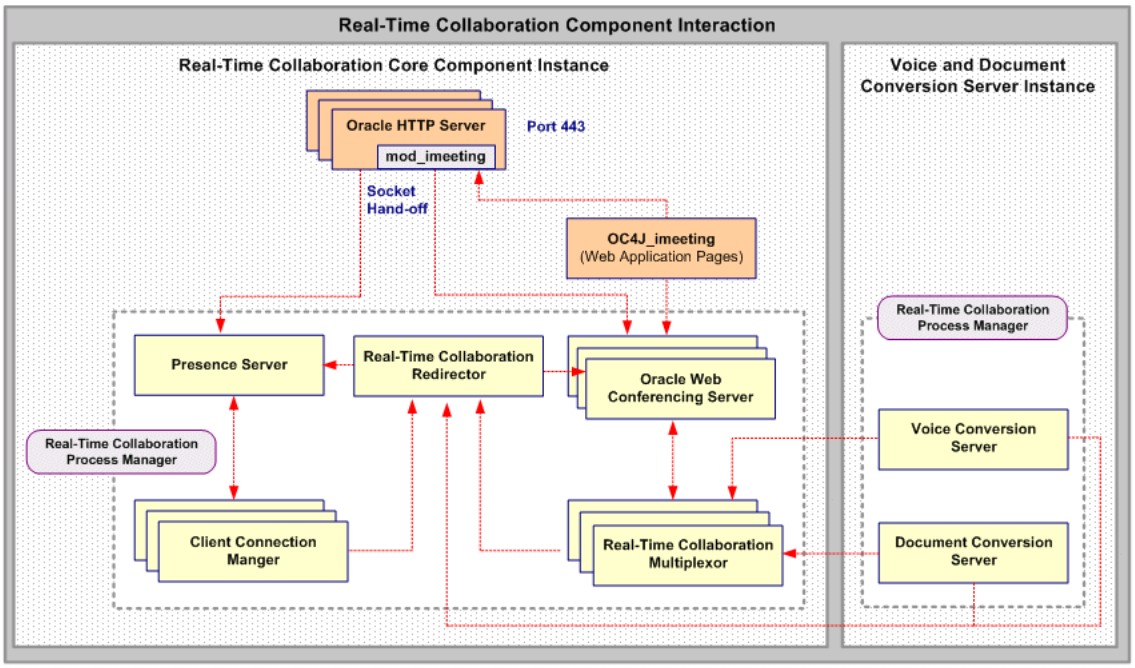


Figure 10–2 illustrates the interaction between components in an Oracle Real-Time Collaboration core component instance and a voice and document conversion server instance.

Oracle Real-Time Collaboration Core Components Instance

An Oracle Real-Time Collaboration core component instance contains the following components. All of the components listed in this section are monitored by a Real-Time Collaboration Process Manager except for the Oracle HTTP Server and `OC4J_imeeting`:

- **Oracle HTTP Server with mod_imeeting** is described in the "Oracle Real-Time Collaboration Architecture" section.
- **Presence server** is described in the "Oracle Real-Time Collaboration Architecture" section.
- **Real-Time Collaboration Redirector** is described in the "Oracle Real-Time Collaboration Architecture" section.
- **Oracle Web Conferencing Server** provides the services for a Web conference by performing the following:
  - Managing all the conference attendees' states and their permissions within the conference.
  - Intelligently distributing real-time data for all the collaboration modes that are active during the conference.
  - Providing services for the recording and archiving of the conference.
- **Client Connection Manager** is described in the "Oracle Real-Time Collaboration Architecture" section.
- **Real-Time Collaboration Multiplexor** is described in the "Oracle Real-Time Collaboration Architecture" section.
- **Real-Time Collaboration Process Manager** watches all the other Oracle Real-Time Collaboration processes (except for `OC4J_imeeting` processes), and provides high availability by restarting processes if they are down. This process itself is monitored by the Oracle Process Management and Notification system.

Voice and Document Conversion Server Instance

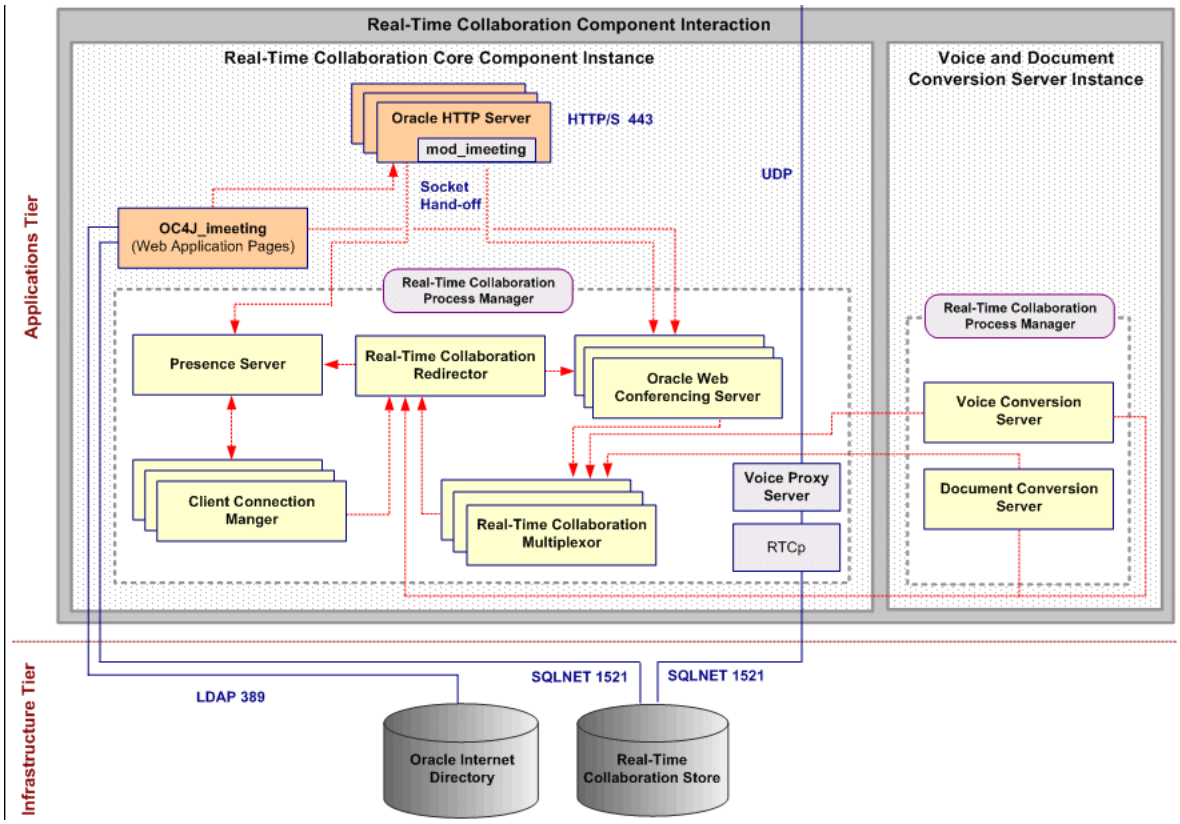
A voice and document conversion server instance contains the following components, both of which are monitored by a Real-Time Collaboration Process Manager:

- **Voice Conversion Server** is described in the "Oracle Real-Time Collaboration Architecture" section
- **Document Conversion Server** is described in the "Oracle Real-Time Collaboration Architecture" section
- **Real-Time Collaboration Process Manager** watches all the other Oracle Real-Time Collaboration processes (except for `OC4J_imeeting` processes), and provides high availability by restarting processes if they are down. This process itself is monitored by the Oracle Process Management and Notification system.

Oracle Real-Time Collaboration Instance

This section describes an Oracle Real-Time Collaboration instance

Figure 10–3 Oracle Real-Time Collaboration Instance



An Oracle Real-Time Collaboration instance is comprised of the following components operating with each other:

- Oracle Real-Time Collaboration core component instance
- Voice and document conversion server instance
- Oracle Internet Directory
- Real-Time Collaboration store
- Voice proxy server
- An additional Real-Time Collaboration Process Manager for the voice proxy server.

Details for each of these components are provided in the "Oracle Real-Time Collaboration Architecture" section and the "Oracle Real-Time Collaboration Component Interaction" section.

Oracle Real-Time Collaboration Access Requirements

External users must be able to connect to the computers containing the Oracle Real-Time Collaboration core component instances. This can be accomplished through a number of different access solutions such as using reverse proxy to bypass the firewall and setup a direct connection with external clients, or using Network Address Translation (NAT) to tunnel into the nodes containing the Oracle Real-Time Collaboration core components instances. Implementation of these solutions may vary depending on an organization's requirements.

> **See Also:** For detailed information about the different Oracle Real-Time Collaboration client connections, see "Oracle Real-Time Collaboration Client Connections and Run-Time Flows" in Chapter 1 of *Oracle Real-Time Collaboration Administrator's Guide*

Oracle Web Conferencing and Oracle Messenger Console Client Connections

The Oracle Web Conferencing and Oracle Messenger console clients attempt to connect to the Oracle Real-Time Collaboration system using one of the following methods, attempting them in the following order until successful:

1. **Direct TCP/IP**: Clients within a corporate intranet connect directly to the RTC Redirector, which hands off connections to the Client Connection Manager (for instant messages) or Multiplexer (for Web conferences), using Jabber XMPP/XMPPS for messaging, or proprietary protocols (MX) with TCP/IP or SSL for Web Conferences.
2. **HTTPS direct**: Clients in the open Internet or across transparent proxies connect using HTTPS. The `mod_imeeting` plug-in uses the Oracle HTTP Server as the single listening point over port 443, hands the socket off to the Connection Manager or Multiplexer, and the console connects directly to one of these.
3. **HTTPS tunnel**: Clients in a different intranet coming through their own internal proxy provide the console with proxy information from the browser settings. The console establishes a connection to the Oracle HTTP Server, which hands the connection off to the Connection Manager or Multiplexer over an HTTPS tunnel through the remote proxy. Again, the listening port is 443.

Requirements for Connections Over the Internet

Oracle Real-Time Collaboration connections do not work over reverse proxies. If you want to allow connections over the Internet to Oracle Real-Time Collaboration, the Applications tier must have an Internet-routable address. You can either do the following:

- Deploy the Applications tier in DMZ of your company, with its IP address publicly routable, with ports 80 (for HTTP) and 443 (for HTTPS) accessible.
- Use a NAT machine to map the internal IP address to an external IP address, with ports 80 (for HTTP) and 443 (for HTTPS) accessible.

Oracle Real-Time Collaboration Access Overview

This section uses an Oracle Real-Time Collaboration cluster to provide an overview of Oracle Real-Time Collaboration access requirements

Figure 10–4 Oracle Real-Time Collaboration Cluster

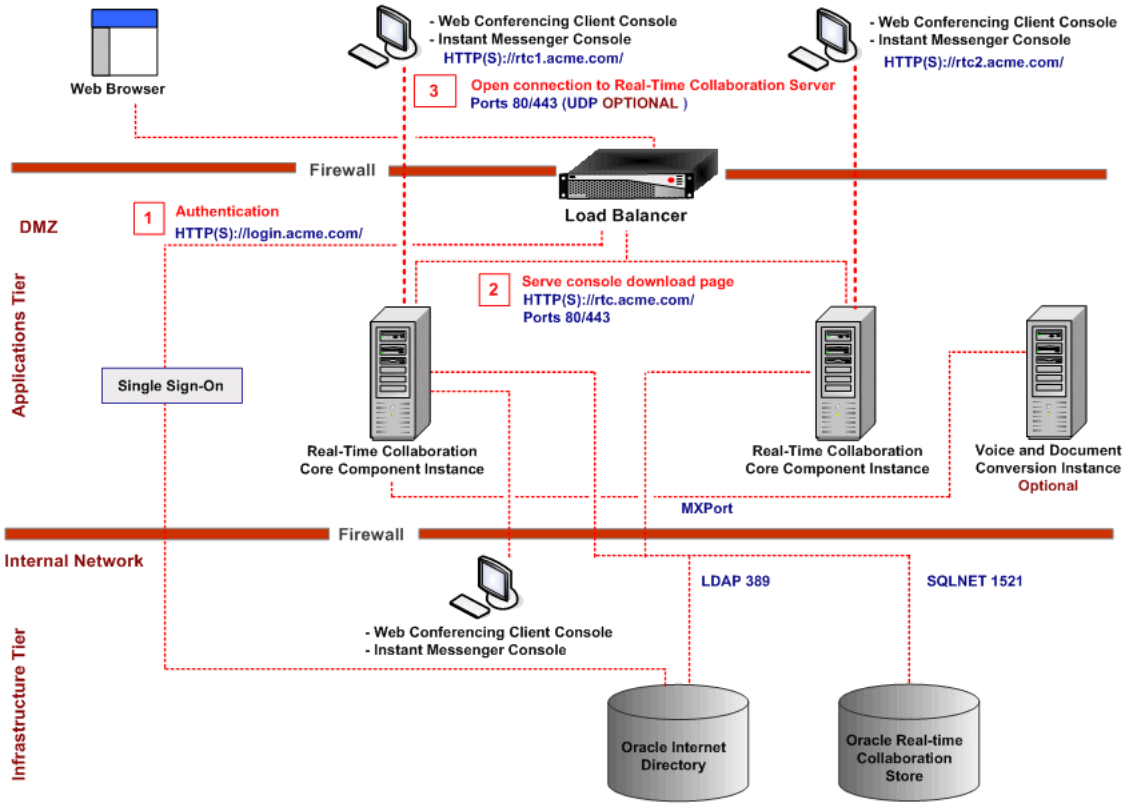


Figure 10–4 illustrates an Oracle Real-Time Collaboration cluster and how Oracle Real-Time Collaboration consoles establish and maintain communication with the Oracle Real-Time Collaboration Applications tier computers.

Network Architecture

In the Applications tier is deployed in a load balanced DMZ (between two firewalls) and the Infrastructure tier is deployed in the internal network of an organization behind a firewall.

Infrastructure Tier

The following components are deployed on the Infrastructure tier:

- Oracle Internet Directory
- The Oracle Real-Time Collaboration store

Applications Tier

The following components are deployed on the Applications tier:

- The single sign-on server, which may be deployed in the DMZ on either a dedicated computer or on any of the Applications tier computers that contain the Oracle Real-Time Collaboration core components. The single sign-on server is not Internet routable and is only routable from the Applications tier.
- Two computers, each containing an Oracle Real-Time Collaboration core component instance.

- A computer with the voice and document instance (optional)

Internal Network Connections

In , users in the internal network of an organization connect directly to the Oracle Real-Time Collaboration Applications tier computer using the Web conferencing client console or the instant messenger console.

Web Connections

In , users connect with Oracle Real-Time Collaboration from the Internet in the following steps:

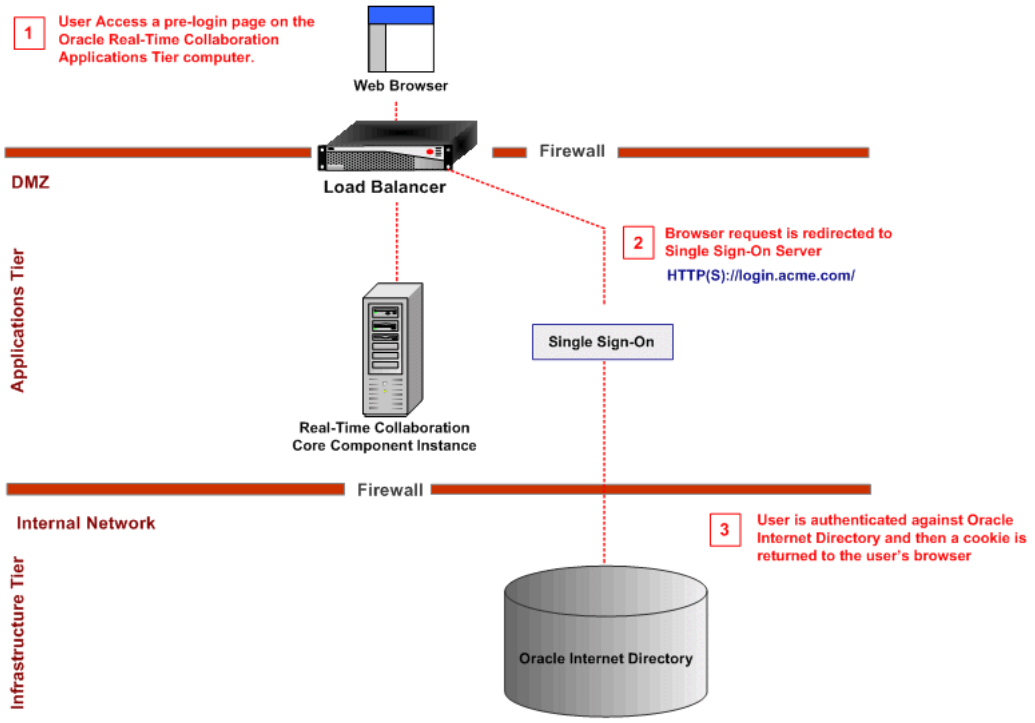
1. A user enters the Web address for the desired Real-Time Collaboration site and is authenticated against Oracle Internet Directory. In this example, the Web address for authentication is `HTTP://login.acme.com/` or `HTTPS://login.acme.com/`.
2. After logging on, the user is redirected to the Oracle Real-Time Collaboration Applications tier computer, which serves a page for downloading the Web conferencing client console and instant messenger console. In this example, the Web address for the download page is `HTTP://login.acme.com/` or `HTTPS://rtc.acme.com/` on Ports 80/443.
3. The user downloads the Web conferencing client console and instant messenger consoles and uses them to connect directly to the Oracle Real-Time Collaboration Applications tier computer without using a load balancer. In this example, two consoles connect to two different Oracle Real-Time Collaboration Applications tier computers with Web addresses `HTTP://rtc1.acme.com/` or `HTTPS://rtc1.acme.com/` and `HTTP://login.acme.com/` or `HTTPS://rtc2.acme.com/`on Ports 80/443.

Details for these steps are provided in the "Client Connection Process Flow" section that follows.

Client Connection Process Flow

This section provides a step-by-step description of how Web conferencing and instant messenger consoles access the Oracle Real-Time Collaboration Applications tier computers. This process takes place in three basic phases:

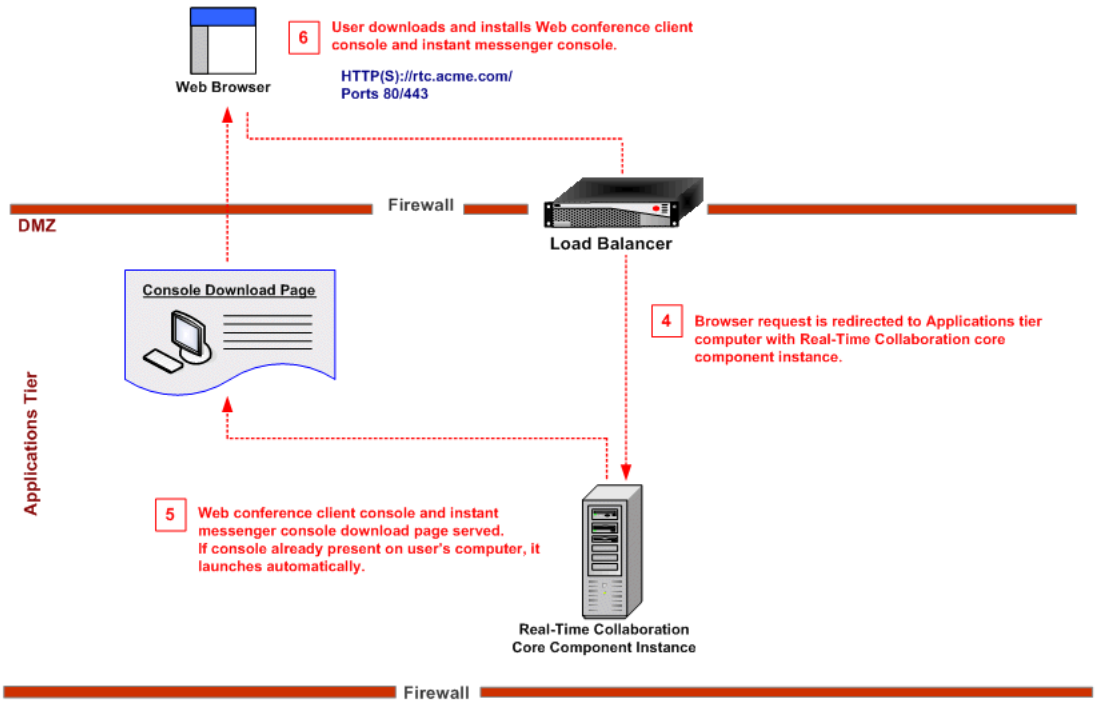
Figure 10–5 Login Flow



The following steps take place during user authentication.

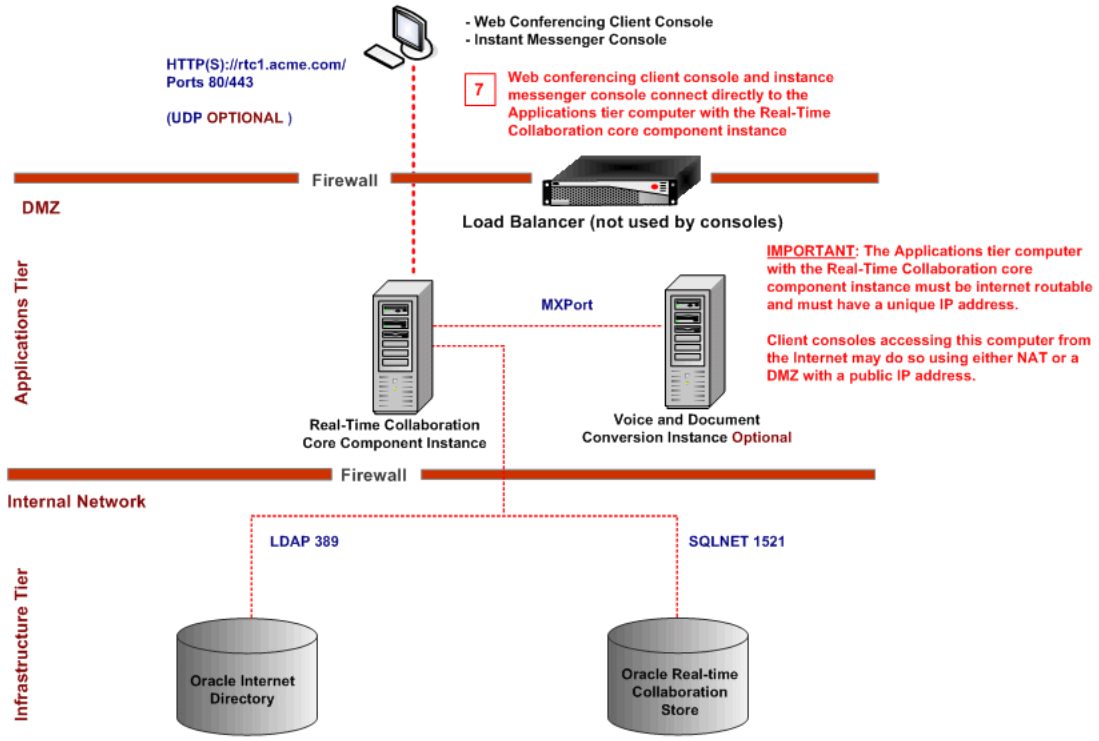
1. The user requests a login to a pre-login page and load balancer directs the request to one of the Applications tier computers that contains the Real-Time Collaboration core component instance.
2. The user request is redirected to the Single Sign-On server, which in this example is located at `HTTP://login.acme.com/` or `HTTPS://login.acme.com/`
3. The user is authenticated against Oracle Internet Directory, a cookie is returned to the browser of a user and the user is redirected to one of the Applications tier computers that contains the Real-Time Collaboration core component instance.

Figure 10–6 Application Pages Access Flow



4. Following successful user authentication, the browser request is redirected to the Applications tier computer that contains the Real-Time Collaboration core component instance. In this example, the browser is redirected to `HTTP://login.acme.com/` or `HTTPS://rtc.acme.com/` on Ports 80/443.
5. The Applications tier computer with Real-Time Collaboration core component instance serves a download page for the Web conference client console and instant messenger console as well as the appropriate Web conferencing address. If the console is already installed on the computer of the user, then it automatically launches.
6. The user downloads and installs the Web conferencing client console and instant messenger console.

Figure 10–7 Console Connection Flow



7. The Web conferencing client console and instant messenger console connect directly to the Oracle Real-Time Collaboration Applications tier computer. In this example, the console connects to the Oracle Real-Time Collaboration Applications tier computer with Web addresses `HTTP://login.acme.com/` or `HTTPS://rtc1.acme.com/` on Ports 80/443 and optionally using the User Datagram Protocol (UDP) for voice.

   IMPORTANT: The Applications tier computer with the Real-Time Collaboration core component instance must be internet routable and must have a unique IP address.

   Client consoles accessing this computer from the Internet may do so using either NAT or a DMZ with a public IP address.

Planning for Oracle Real-Time Collaboration Deployment

This section discusses a range of issues involved in deploying Oracle Real-Time Collaboration components. These include hardware and software prerequisites, sizing guidelines, firewall issues, and topology considerations for a geographically distributed organization.

Oracle Real-Time Collaboration Prerequisites

The following prerequisites are necessary for any deployment of Oracle Real-Time Collaboration.

Optional Document and Voice Conversion Server

Voice and document conversion server (needed if using voice streaming over a PSTN phone line, or document sharing in conferences):

- Windows 2000 Server SP4 and higher
- Intel Dialogic System software 5.1.1 SP1 and higher (for voice streaming over a PSTN line)

System Requirements for Web Conferencing Client

Each Web Conferencing user must have administrative privileges on his system in order to install the client console. Each user's system must meet the following requirements:

- Windows 98 or higher
- Internet Explorer 5.5 or later, Netscape 4.75 or later, Netscape 7.0 or later, Mozilla 1.0 or later, or Firefox 1.1 or higher
- 1024 x 768 screen resolution
- Microsoft Java Virtual Machine (JVM) version 1.1.4 Build 3740 or later, or Sun JVM 1.3.1 or later, installed and enabled

*All listed browsers can perform all tasks in the Real-Time Collaboration Web application pages, and can use the conference whiteboard and desktop sharing features. In addition, Netscape 4.X browsers (prior to Netscape 4.75) can use most Web application features, but they cannot use the **Schedule** tab to schedule a conference.

Only Internet Explorer 5.5 browsers (or later) can share documents in document presentation mode, stream voice data in a conference over PSTN, or play back a recorded conference. Each Internet Explorer user must have Java Virtual Machine (JVM) installed and Java enabled in Internet Explorer in order to use these features. To check whether you have a JVM installed and enabled, do the following:

1. Open Internet Explorer.
2. Select **Tools** and then **Internet Options**.
3. Click the **Advanced** tab.
4. Scroll down to Java (Sun) or Microsoft VM and make sure all boxes under the heading you find are checked ON.

If you do not see any references to Java or VM, then you need to download and install a Java Virtual Machine. Please contact your system administrator for information about what JVM your company uses and supports. After you've installed a JVM, verify that it is enabled by repeating the previous steps.

System Requirements for Oracle RTC Messenger Client

Each RTC Messenger user must have administrative privileges on his system in order to install the client console. Each system must be running Windows NT, Windows 2000, or Windows XP.

Oracle RTC Messenger uses XMPP, an open, industry-standard protocol for instant messaging. For more information about XMPP, go to http://www.jabber.org/protocol/.

The native Oracle RTC Messenger client works only on a Windows computer. For the list of supported instant messaging clients and instructions about using them to connect to RTC Messenger, see the RTC Messenger FAQ at

http://www.oracle.com/technology/products/cs/user_info/ortc/messenger_index.html.

Requirements for Oracle Real-Time Collaborationn Add-in for Microsoft Office

The Oracle Real-Time Collaboration Add-in for Microsoft Office works with Microsoft Office 2000 or later.

Oracle Real-Time Collaboration Sizing Guidelines

This section discusses Oracle Real-Time Collaboration sizing information. Additional information is posted on Metalink.

Load Balancer Considerations for Real-Time Collaboration

The Oracle Real-Time Collaboration components perform load balancing as they handle communications between clients and servers. The Redirector determines which multiplexer or communication manager processes are available as it routes requests from clients. The multiplexer determines which Web Conferencing Server processes are available as it routes communications from and to the Web Conferencing clients.

You may also choose to use a Load Balancer to manage processes handled by your Oracle mid-tier servers. If so, then keep the following considerations in mind:

- All systems behind the load balancer should have intranet-routable IP addresses and must be directly accessible from the Internet at least on the standard HTTP and HTTPS ports (80 and 443).
- If you use geographic load balancers – that is, load balancers to separate loads between geographic locations – then you must create Oracle Real-Time Collaboration *clusters* to partition the system based on geographical distribution
- Messenger also uses ports 5222 and 5223 which in some cases must be open to the Internet.

Distributed Deployment Considerations for Real-Time Collaboration

If you have multiple corporate locations that will use Oracle Real-Time Collaboration Web Conferencing, then you must consider the following:

- The number of conferences held and instant messages sent at a single geographic location
- The number of conferences held and instant messages sent across geographic locations
- The number of streaming-voice conferences held across geographic locations, if voice streaming over PSTN phone lines is used

After evaluating these issues, you can then consider whether creating clusters will help distribute Real-Time Collaboration Web Conferencing and instant messaging processes to distinct geographic locations.

The following sections outline some rules of thumb to apply when considering where to deploy Real-Time Collaboration core components and Voice Conversion servers.

Note: Note that there is only *one* RTC Messenger Router running at any time. The considerations discussed in the following sections apply only to deployment of systems to support the multiple Web Conferencing Server processes.

Deploying Core Components Locally or Globally

Because data from desktop of one user is distributed to other end-user desktops during a Web conference or instant message, end users may experience latency issues depending on their location. Oracle Real-Time Collaboration, by itself, cannot address network latency issues. You must resolve these issues through other mechanisms.

However, you can consider where you will deploy the Real-Time Collaboration core components, depending on how much traffic passes within specific geographic locations, as described the following scenarios.

Scenario 1: Many Meetings or Messages in Separate Geographical Locations

If your company holds many conferences where most of the attendees are in the same geographical region, or sends many instant messages between employees in the same region, then Oracle recommends deploying a set of Real-Time Collaboration Core Components instances in that geographical region.

For example, a company has multiple divisions all over the world, and employees of each division hold many conferences with each other and send many instant messages to each other. Occasionally they hold conferences with or send messages to employees in different locations.

In such a scenario, it does not make sense to force users to use a Real-Time Collaboration cluster in a different location, thereby causing network latency problems for users. Instead, each location can have its own set of Real-Time Collaboration Core Components instances.

Scenario 2: Many Meetings Across Geographical Locations

If attendees of most conferences are in different regions, or instant messages are sent equally between members of different regions, then having a set of Real-Time Collaboration Core Components instances in each geographical region will not help prevent latency issues.

For example, a US-based company has outsourced its sales or support organization to a site in India. If a typical conference involves a sales agent from the site in India and a customer in the US, then deploying Real-Time Collaboration Core Components instances in the India site will not prevent a latency problem.

Deploying Voice Conversion Servers Locally or Globally

If you hold streaming voice conferences using PSTN phone lines, then you should deploy Voice Conversion Servers in areas where the servers are able to successfully dial in to all conference numbers that will be used. It may be beneficial to deploy a Voice Conversion Server in the region where most calls terminate. For example, if a significantly large number of Web Conferencing users dial out to a particular region like the UK, it would be beneficial to have a Voice Conversion Server deployed in the UK instead of using a Voice Conversion Server in the USA to dial the UK numbers.

Oracle Real-Time Collaboration Server Architecture Scalability

Oracle Real-Time Collaboration server is designed to scale well in a Symmetric Multiprocessing (SMP) configuration, or a multi-node configuration. You can scale up. In other words, you can add more components to an Oracle Real-Time Collaboration Applications tier computer. You can scale out. In other words, you add more Oracle Real-Time Collaboration Applications tier computers.

Figure 10–8 Scaling Oracle Real-Time Collaboration

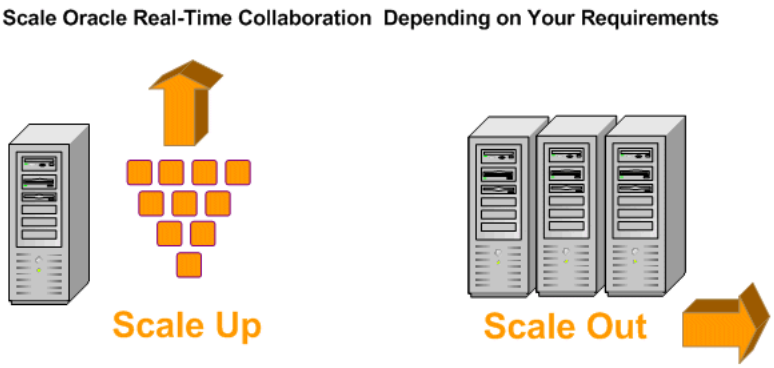


Figure 10–8 illustrates the available options for scaling Oracle Real-Time Collaboration. This figure, shows two configurations, scaling up and scaling out. In the scaling up configuration, more hardware components are added to an Oracle Real-Time Collaboration Applications tier computer. In the scaling out configuration, more Oracle Real-Time Collaboration Applications tier computers are added.

Oracle Real-Time Collaboration Deployment Configurations

Oracle Real-Time Collaboration deployment configurations follow the same guidelines as those for Oracle Collaboration Suite. For information on deploying Oracle Real-Time Collaboration in a single-computer, multiple-computer, or high availability environment, please refer to Chapter 3, "Deploying Oracle Collaboration Suite". Other Oracle Real-Time Collaboration deployment configurations are provided in this section.

Geographic Distribution with Real-Time Collaboration Clusters

By default, all Web Conferencing Server processes in all instances are considered part of one group. Whenever a new conference is created and a Web Conferencing Server process needs to be chosen for a conference, the conference can be assigned to any one of the Web Conferencing Servers in the system. But, as described in the previous sections, it is sometimes useful to partition the system into clusters based on geographical distribution.

Figure 10–9 Geographic Distribution with Oracle Real-Time Collaboration Clusters

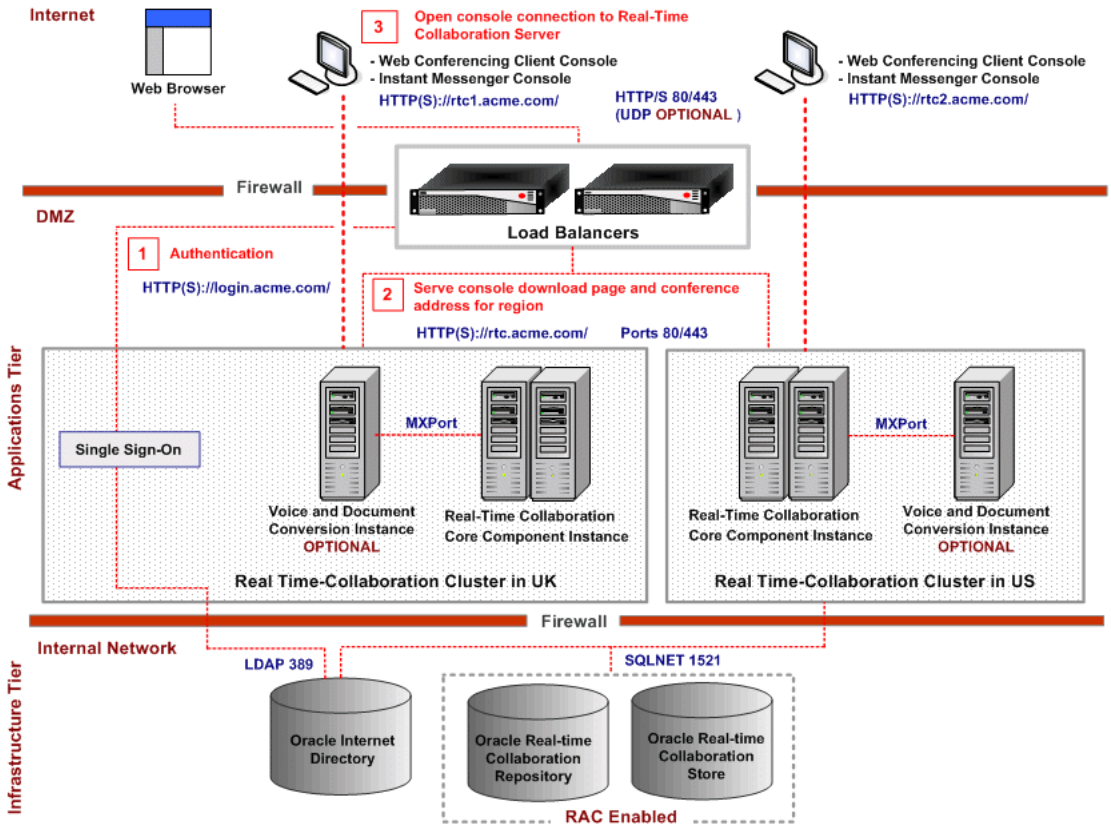


Figure 10–9 illustrates an Oracle Real-Time Collaboration geographic distribution using Oracle Real-Time Collaboration.

Infrastructure Tier

In Figure 10–9, the Infrastructure tier contains Oracle Internet Directory and redundant Oracle Real-Time Collaboration store computers configured for RAC.

Applications Tier

In Figure 10–9, Applications tier consists of two clusters in a DMZ and traffic is served to each cluster from multiple load balancers. Separate clusters of Real-Time Collaboration core components are placed in the US and UK and each configuration has multiple Oracle Real-Time Collaboration Applications tier computers as well as a voice and document conversion server. The single sign-on server, may be deployed in the DMZ on either a dedicated computer or on any of the Applications tier computers that contain the Oracle Real-Time Collaboration core components. The single sign-on server is not Internet routable and is only routable from the Applications tier. The single sign-on server can be deployed in either cluster and will still authenticate against Oracle Internet Directory and return a cookie to the browser of the user.

Internal Network Connections

In ,users in the internal network of an organization connect directly to the Oracle Real-Time Collaboration Applications tier computer using the Web conferencing client console or the instant messenger console.

Web Connections

In ,users connect with Oracle Real-Time Collaboration from the Internet in the following steps:

1. A user enters the Web address for the desired Real-Time Collaboration site and is authenticated against Oracle Internet Directory. In this example, the Web address for authentication is `HTTP://login.acme.com/` or `HTTPS://login.acme.com/`.
2. After logging on, the load balancer determines the user's geographic origin and redirects the user is to the appropriate Oracle Real-Time Collaboration Applications tier computer for the user's desired geographic location (in this example, either the US, or UK). This computer serves a page for downloading the Web conferencing client console and instant messenger console. In this example, the Web address for the download page is `HTTP://rtc.acme.com` or `HTTPS://rtc.acme.com/`on Ports 80/443.
3. The user downloads the Web conferencing client console and instant messenger consoles and uses them to connect directly to the Oracle Real-Time Collaboration Applications tier computer without using a load balancer. In this example, two consoles connect to two different Oracle Real-Time Collaboration Applications tier computers with Web addresses `HTTP://rtc1.acme.com/` or `HTTPS://rtc1.acme.com/`and `HTTP://rtc2.acme.com/` or `HTTPS://rtc2.acme.com/`on Ports 80/443.

11

Deploying Oracle Collaboration Suite Search

This chapter contains the following topics.

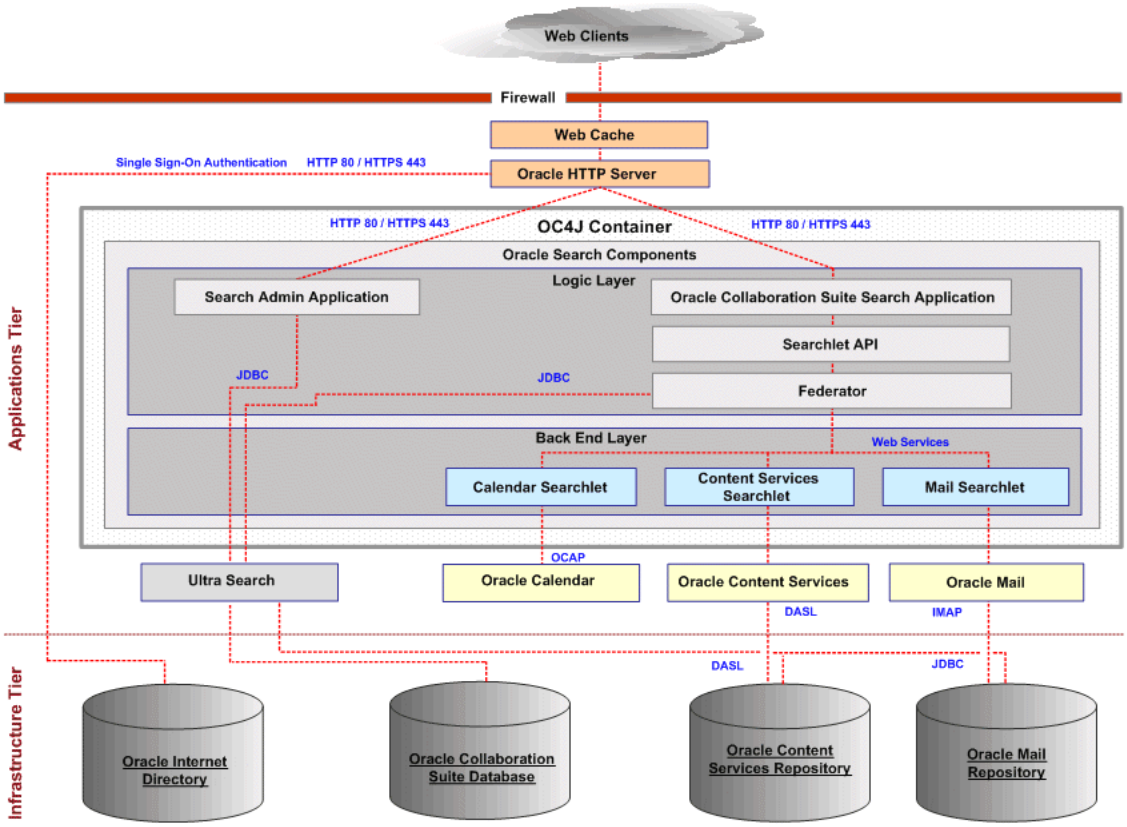
Oracle Collaboration Suite Search Architecture and Functionality

This section discusses the architecture and functionality of Oracle Collaboration Suite Search.

Oracle Collaboration Suite Search Architecture

Oracle Collaboration Suite Search is a light-weight search application that is deployed on the Oracle Collaboration Suite Applications tier and that performs queries on Oracle Calendar, Oracle Content Services, and Oracle Mail data. The Oracle Collaboration Suite Search architecture and functionality are illustrated in the following figure:

Figure 11–1 Oracle Collaboration Suite Search Architecture



In Figure 11–1, Oracle Collaboration Suite Search is deployed on the Applications tier and is used by Web clients to access components on the Applications tier and Infrastructure tier.

Infrastructure Tier

Oracle Collaboration Suite Search is not deployed on the Infrastructure tier, however the Infrastructure tier contains the target repositories for Oracle Collaboration Suite Search and the Oracle Internet Directory.

Applications Tier

Oracle Collaboration Suite Search is not deployed on the Applications tier in an OC4J container with Web cache, Oracle HTTP Server, Oracle Calendar (application and repository), Oracle Content Services, Oracle Mail, and Oracle Ultra Search.

OC4J Container with Oracle Collaboration Suite Search Components.

The OC4J Container comprises the logic layer and back end layer components:

Table 11–1 Oracle Collaboration Suite Search OC4J Logic Layer

Business Layer Component	Definition
Search Admin Application	The Search Admin Application enables administrators to set up and configure various data sources. For example, with the Search Admin Application, administrators can indicate the mail stores for which to perform a search, or which web sites to index. The Search Admin application is stored in OC4J_OCSAdmin.

Table 11–1 (Cont.) Oracle Collaboration Suite Search OC4J Logic Layer

Business Layer Component	Definition
Oracle Collaboration Suite Search Application	The Oracle Collaboration Suite Search Application enables end-users to search for content in the various repositories in which they have accounts, as well as the Web. The Oracle Collaboration Suite Search Application is stored in OC4J_OCSClient.
Searchlet API	The Searchlet API is the application programming interface for defining a Searchlet. A searchlet is the mediator between the Federator and a data source. Searchlets expose data source attributes, folders, and other metadata, translate query syntax and estimate hit counts.
Federator	The federator collects search results from the individual application searchlets including the Calendar searchlet, Content Services searchlet, and Mail searchlet, as well as the Ultra Search engine. It also passes Single Sign-on authentication credentials to the searchlets, enabling an authenticated user to search for data in this applications for which the servlets are deployed.

Table 11–2 Oracle Collaboration Suite Search OC4J Back End Layer

Business Layer Component	Definition
Calendar Searchlet	The Calendar Searchlet performs a basic search for the title and details of appointments, to-do lists, and notes.
Content Services Searchlet	The Content Services searchlet performs a basic search for the title and content of a document stored in the Content Services repository.
Mail Searchlet	The Mail searchlet performs a basic search for the subject and body of e-mail folders and messages.

Oracle Collaboration Suite Search Functionality

Oracle Collaboration Suite Search contains an Admin tool, the Ultra Search engine, and the Oracle Collaboration Suite Search Application. This section describes the functionality of each component.

Search Admin Application Functionality

The following figure illustrates the Search Admin Application functionality.

Figure 11–2 Oracle Collaboration Suite Search Admin Application Functionality

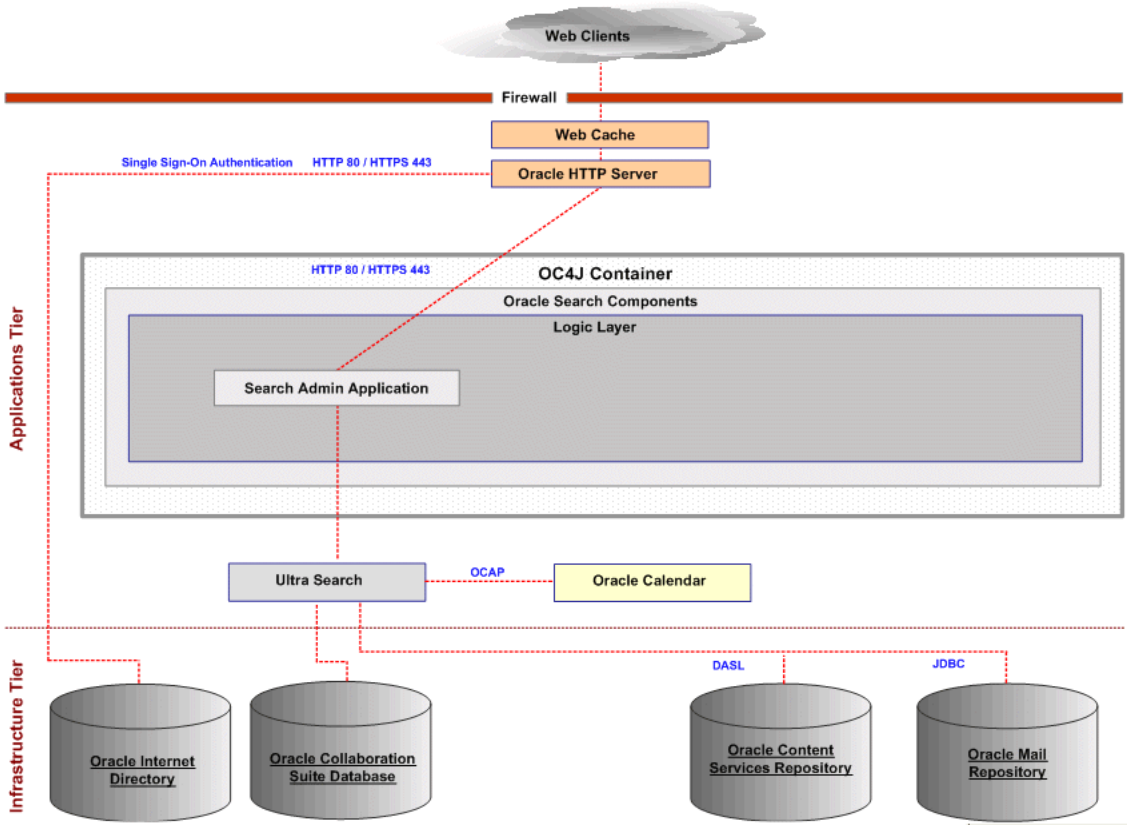


Figure 11–2 illustrates the Search Admin Application functionality. In this figure a Web client connects to the Web Cache and then the Oracle HTTP Server, which authenticates the user against the Oracle Internet Directory. If the user accesses the Search Admin URL, then the user is connected to the Search Admin Application. The user is subsequently able to connect to the UltraSearch application and to the Oracle Calendar repository (deployed on the Applications tier, not the Infrastructure tier), the Oracle Content Services repository, and the Oracle Mail repository.

- Oracle Calendar Access Protocol (OCAP) for Oracle Calendar
- Distributed Authoring and Versioning Searching & Locating (DASL) for Oracle Content Services
- Java Database Connectivity (JDBC) for Oracle Mail.

The Administrator can configure data sources and search indexing for each of these repositories. Crawled or indexed content can include the title, author, subject, and description of calendar appointments, mail messages and documents. Ultrasearch stores crawled or indexed content in the Oracle Collaboration Suite database.

Ultra Search Functionality

Ultra Search integrates with Oracle Collaboration Suite Search Search application as follows:

- Oracle Collaboration Suite Search is built on the federator framework provided by Ultra Search. Oracle Collaboration Suite Search enables users to submit search requests to the Web and to the Calendar, Content Services, and Mail stores using

the Search bar in the Collaboration Suite Portal home page or through the Collaboration Search Search UI (`http://<host>:<port>/search`)

- By itself, Ultra Search supports the Web search but does not support search requests to Web, Calendar, Content Services, and Mail sources. When a search request is submitted to Web sources from the Oracle Collaboration Suite Search, Oracle Collaboration Suite Search sends the request to the Ultra Search repository through the Federator.

The following figure illustrates Ultra Search functionality in Oracle Collaboration Suite Search.

Figure 11–3 Oracle Collaboration Suite Search Ultra Search Functionality

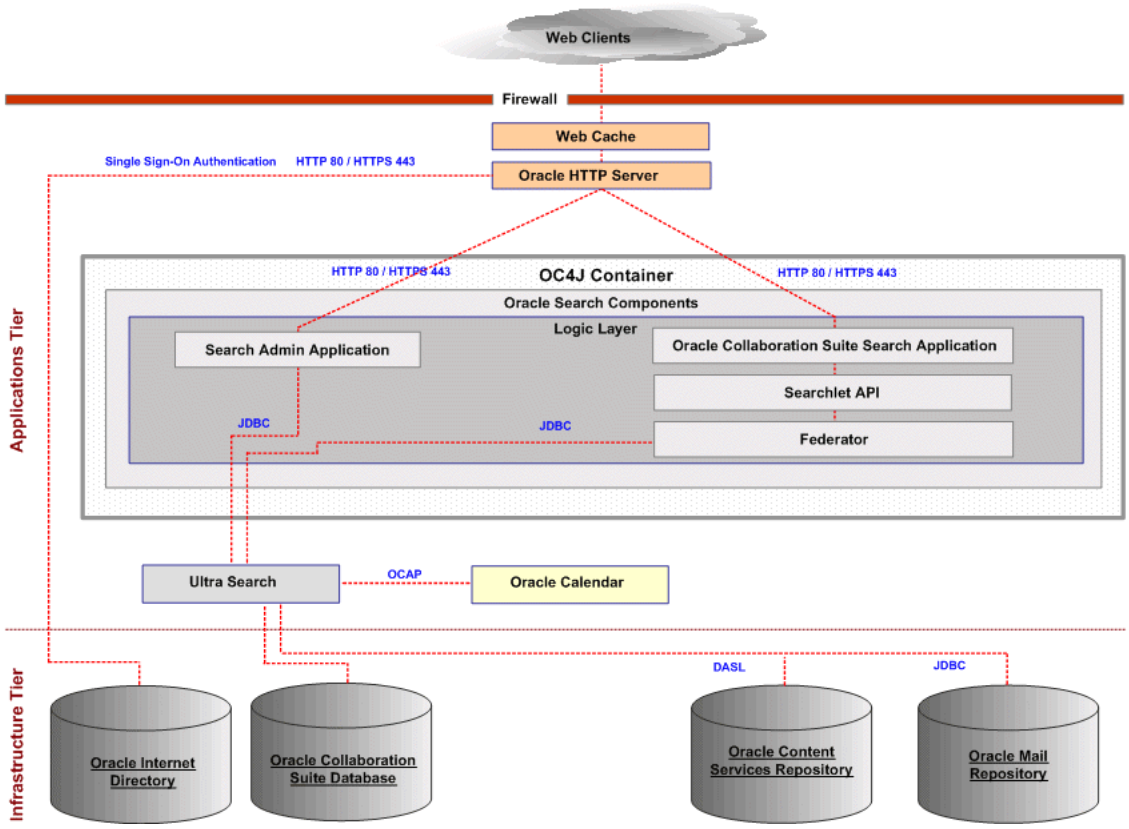


Figure 11–3 illustrates Ultra Search functionality in Oracle Collaboration Suite Search. In this figure a Web client connects to the Web Cache and then the Oracle HTTP Server, which authenticates the user against the Oracle Internet Directory. If the user is authenticated as an administrator, then the user is connected to the Search Admin Application as described in the "Search Admin Application Functionality" section. Otherwise, the user is connected to the Oracle Collaboration Suite Search application. The Oracle Collaboration Suite Search application connects to the Searchlet API and then to the Federator. The Federator connects to Ultra Search using JDBC to search for crawled or indexed content in the Oracle Calendar repository (deployed on the Applications tier, not the Infrastructure tier) the Oracle Content Services repository, and the Oracle Mail repository. Ultra Search connects to the various repositories, using the required protocol:

- OCAP for Oracle Calendar

- DASL for Oracle Content Services
- JDBC for Oracle Mail.

Oracle Collaboration Suite Search Application Functionality

The following figure illustrates the Oracle Collaboration Suite Search Application functionality.

Figure 11–4 Oracle Collaboration Suite Search Application Functionality

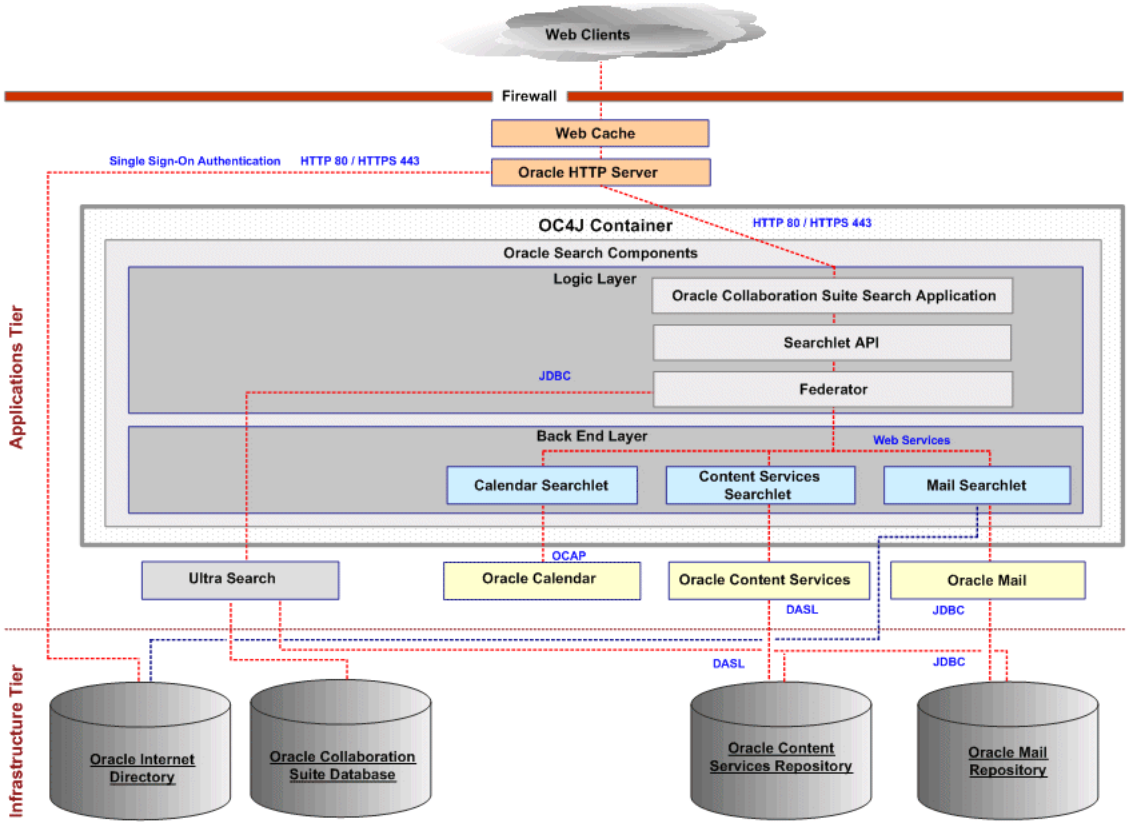


Figure 11–4 illustrates Oracle Collaboration Suite Search Application functionality. In this figure a Web client connects to the Web Cache and then the Oracle HTTP Server, which authenticates the user against the Oracle Internet Directory.The user is connected to the Oracle Collaboration Suite Search application, which connects to the Searchlet API and then to the Federator.

Federator

The Federator connects to Ultra Search using JDBC to search for crawled or indexed content in the Oracle Calendar repository, the Oracle Content Services repository, and the Oracle Mail repository. Crawled or indexed content can include the title, author, subject, and description of calendar appointments, mail messages and documents. Ultrasearch stores crawled or indexed content in the Oracle Collaboration Suite database. Ultra Search connects to the various repositories, using the required protocol:

- OCAP for Oracle Calendar
- DASL for Oracle Content Services

- JDBC for Oracle Mail.

Searchlets

Searchlets perform searches on the individual components. The mail searchlet also searches Oracle Internet Directory for e-mail user identification information.

Planning for Oracle Collaboration Suite Search Deployment

This section discusses planning issues for deploying Oracle Collaboration Suite Search

Light-Weight Application Deployed Across Applications Tier

Oracle Collaboration Suite Search is a light-weight application that can be included with any other Oracle Collaboration Suite Applications tier deployment such as Oracle Calendar, Oracle Content Services, and Oracle Mails.

Searchlet Tuning

Searchlets are deployed with Oracle Collaboration Suite Search as part of the installation process, and can subsequently be tuned to suite the requirements of target applications.

Oracle Collaboration Suite Search Deployment Configurations

Oracle Collaboration Suite Search deployment configurations follow the same guidelines as those for Oracle Collaboration Suite. For information on deploying Oracle Collaboration Suite Search in a single-computer, multiple-computer, or high availability environment, refer to Chapter 3, "Deploying Oracle Collaboration Suite".

12

Deploying Oracle Voicemail & Fax

This chapter contains the following topics.

Understanding the Oracle Voicemail & Fax Architecture and Functionality

This section provides an overview of the Oracle Voicemail & Fax server architecture and functionality. The Oracle Voicemail & Fax server is a computer telephony (CT) server comprised of Oracle Voicemail & Fax applications integrated with CT server solution of Intel and NetMerge CCS 3.0. The Oracle Voicemail & Fax server is installed on the Oracle Collaboration Suite Application tier where it transmits voice information from a private telephone switchboard, also known as a Private Branch Exchange (PBX), to the Oracle Collaboration Suite Infrastructure. Before deploying Oracle Voicemail & Fax, you should understand both the architecture of Oracle Voicemail & Fax server and the different ways that it can be integrated with a PBX.

Note: NetMerge CCS 3.0 software is not provided by Oracle and must come from a third party.

Oracle Voicemail & Fax Components

The Oracle Voicemail & Fax architecture contains the following components:

- Mail Store
- Oracle Internet Directory
- Oracle Voicemail & Fax Server
- Optional POP3 and IMAP4 Servers

Mail Store

Oracle Voicemail & Fax uses the Oracle Mail message store as the store for all voicemail and fax messages. These messages are stored directly into the inbox of the user who is using the Oracle Mail PL/SQL Application Programming Interface (API) to ensure delivery of voicemail messages across the IP network. Oracle Voicemail & Fax also uses Oracle Mail PL/SQL APIs to provide fast access to all messages stored in the inbox of users. Users have real-time access to the mail store through the telephone.

GUI access to voicemail and fax messages is provided through the same infrastructure as normal e-mail traffic. E-mail messages are stored in Internet standard MIME format allowing rendering through any IMAP4 or POP3 mail client that supports multi-part mime messages. In addition to providing message access, the Oracle Collaboration Suite Integrated Client, Oracle Connector for Outlook, and WebMail client allow self-service access to Oracle Mail and Oracle Voicemail & Fax user preferences including greeting selection and changing voicemail passwords.

Oracle Internet Directory

Oracle Internet Directory stores all information about users and their preferences as well as system information. Oracle Voicemail & Fax leverages user information and preferences from Oracle Mail and then extends the stored information to include voicemail-specific attributes such as site, greeting, access to fax, and phone number. System configuration information stored within the directory includes attributes such as system parameters, menus, prompts and other management information.

Oracle Voicemail & Fax Server

The Oracle Voicemail & Fax server is based on Enterprise Computer Telephony Forum (ECTF) standards. Oracle has certified Oracle Voicemail & Fax implementation on Netmerge CCS server of Intel and associated hardware. See the "Oracle Voicemail & Fax Server Architecture" section for more information.

Optional POP3 and IMAP4 Servers

You can optionally configure POP3 and IMAP4 servers to provide e-mail access to voicemail messages.

Oracle Voicemail & Fax Server Architecture

The Oracle Voicemail & Fax server is comprised of Oracle Voicemail & Fax applications integrated with Intel's CT server solution, NetMerge CCS 3.0. As a standards based telephony product, Oracle Voicemail & Fax is written to the Enterprise Computer Telephony Forum (ECTF) CT Standard, specifically calls the S.410 (essentially a Java version of the "c" based s.100 API. It is also known as JTAPI Media) and S.300 APIs. Oracle Voicemail & Fax has been developed, tested and certified against Intel CT Server implementation known as NetMerge CCS.

NetMerge CCS provides an abstraction layer which shelters Oracle Voicemail & Fax from the proprietary nature of telephony implementations and enables the same application to function regardless of PBX integration strategy, underlying telephony board types or bearer channel. The following figure illustrates the Oracle Voicemail & Fax and Intel Netmerge CCS architecture.

Figure 12–1 Oracle Voicemail & Fax Intel Netmerge Architecture

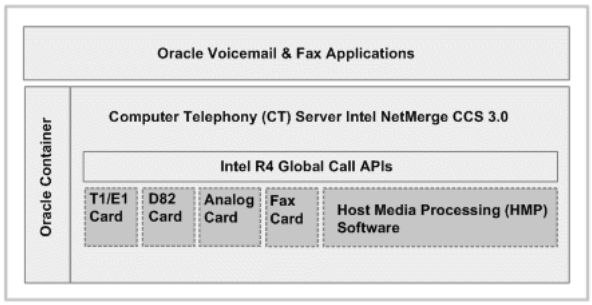


Figure 12–1 illustrates the Oracle Voicemail & Fax Intel Netmerge architecture. This figure contains an upper box and two lower boxes. The upper box represents the Oracle Voicemail & Fax applications. These are java based and interact with NetMerge CCS by making generic s.410 calls such as Answer Call, record, and Play. The lower box to the left represents the Oracle Container and the lower box to the right represents the Computer Telephony (CT) Server Intel NetMerge CCS 3.0. The Computer Telephony (CT) Server Intel NetMerge CCS 3.0 contains a box representing the Intel R4 Global Call APIs and five boxes beneath it. Four of these boxes represent available cards for connecting to the PBX using a circuit switched configuration. These include T1/D1, D82, Analog, and Fax. The fifth box represents the Host Media Processing (HMP) software used to connect to the PBX with VoIP gateway.

The Oracle Container sub-system is an extension of the standard "C" based s.300 container provided with Intel Netmerge CCS which normally stores or retrieves media from the local file system. The Oracle extension maps standard container calls to the Oracle Mail message store allowing the recording and retrieval of voicemail messages directly from the database. Calls to the message store database are made over the IP network using standard Net protocol of Oracle. The Oracle Container is multi-threaded and takes advantage of connection pooling into the database.

Oracle Voicemail & Fax PBX Integration

Oracle Voicemail & Fax supports integration with many popular traditional and VoIP based telephone systems using a combination of technologies available from Oracle integration partners.

Most PBXs provide proprietary interfaces to integrate additional functionality such as Voice Mail systems. Intel or Dialogic provides telephony cards which support common telephone systems found in most enterprise and carrier environments.

Oracle Voicemail & Fax integrates with a PBX using either a Circuit Switched or VoIP configuration.

- Simple analog connectivity and Bellcore standard SMDI provides basic support for the majority of carrier grade or high end CPE market.
- Digital E1 or T1 protocols and Bellcore standard SMDI provides a better solution for carrier and large campus implementations.
- Digital handset emulation using the Intel D82 series boards and Intel PBX-IP-Media-Gateway (PIMG) devices provide an alternative integration method for many common enterprise class PBX or Switches and less standard VoIP solutions.

- Inbound DTMF integration through Analog provides a lowest common denominator approach for smaller PBX or key system integration.
- VoIP support (h.323) through the Intel IP Link series of cards. Future versions will include native SIP capabilities.
- SIP based VoIP for IP gateways.

Circuit Switched Configuration

With the Circuit Switched configuration, the Oracle Voicemail & Fax software uses telephony cards to communicate directly with the PBX. These cards vary depending on with which PBX the Oracle Voicemail & Fax server communicates.

Figure 12–2 Oracle Voicemail & Fax Circuit Switched Configuration

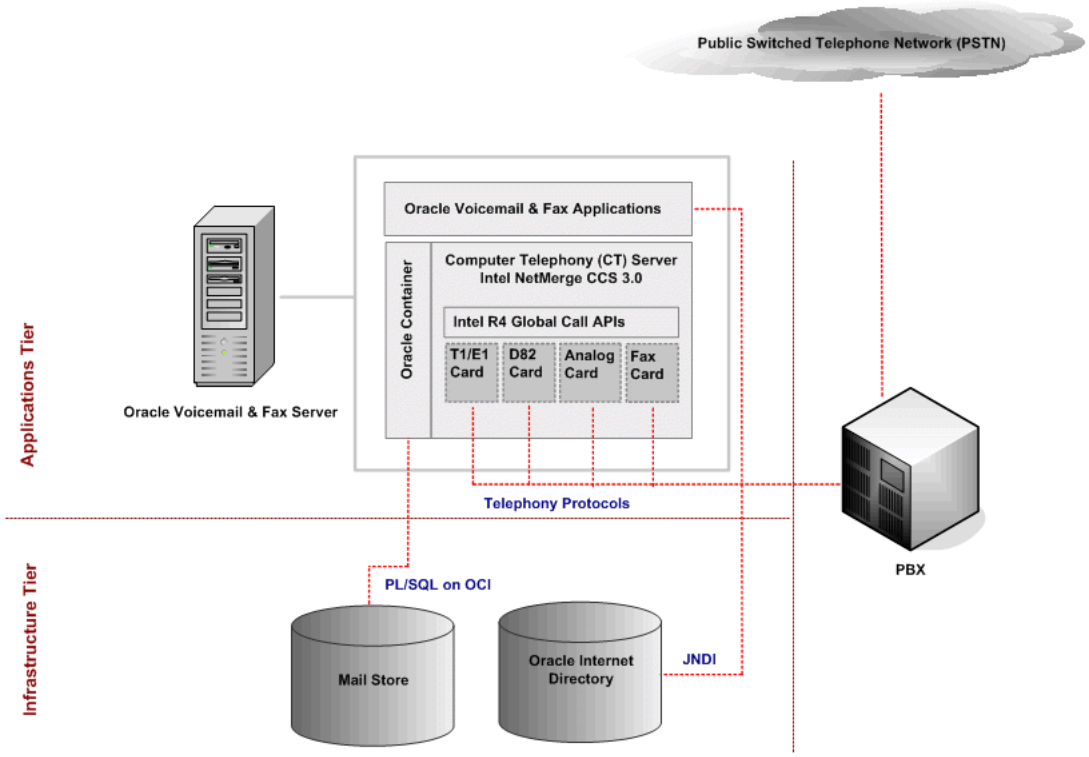


Figure 12–2 illustrates an Oracle Voicemail & Fax circuit switched configuration. This figure contains the Oracle Collaboration Suite Infrastructure tier, Application tier, a PBX and the Public Switched Telephone (PSTN) network.

Infrastructure Tier

In , the Infrastructure tier contains the mail store and the Oracle Internet Directory.

Applications Tier

In the Applications tier contains the Oracle Voicemail & Fax server. Details of the Oracle Voicemail & Fax server are described in the section.

Functionality

Communication between the Oracle Container in the Oracle Voicemail & Fax server and the mail store takes place using Procedural Structured Query Language on Oracle Call Interface (PL/SQL on OCI). Communication between the Oracle Voicemail & Fax applications and Oracle Internet Directory takes place using the Java Naming Directory Interface (JNDI). Communication between the Oracle Voicemail & Fax server telephony cards and the PBX takes place using a variety of telephony protocols depending on which card is used:

- Digital E1 or T1 protocols and Bellcore standard SMDI provides a better solution for carrier and large campus implementations.
- Digital handset emulation using the Intel d82 series boards provides an alternative integration method for many common enterprise class PBX or switches and less standard VoIP solutions.
- Simple analog connectivity and Bellcore standard SMDI. This provides basic support for the majority of carrier grade or high end CPE market.

When a call is received from the PBX, the Oracle Voicemail & Fax applications check the Oracle Internet Directory to discover the address of the message recipient.

VoIP Configuration

This section discusses Oracle Voicemail & Fax VoIP configuration.

Figure 12–3 Oracle Voicemail & Fax VoIP Configuration

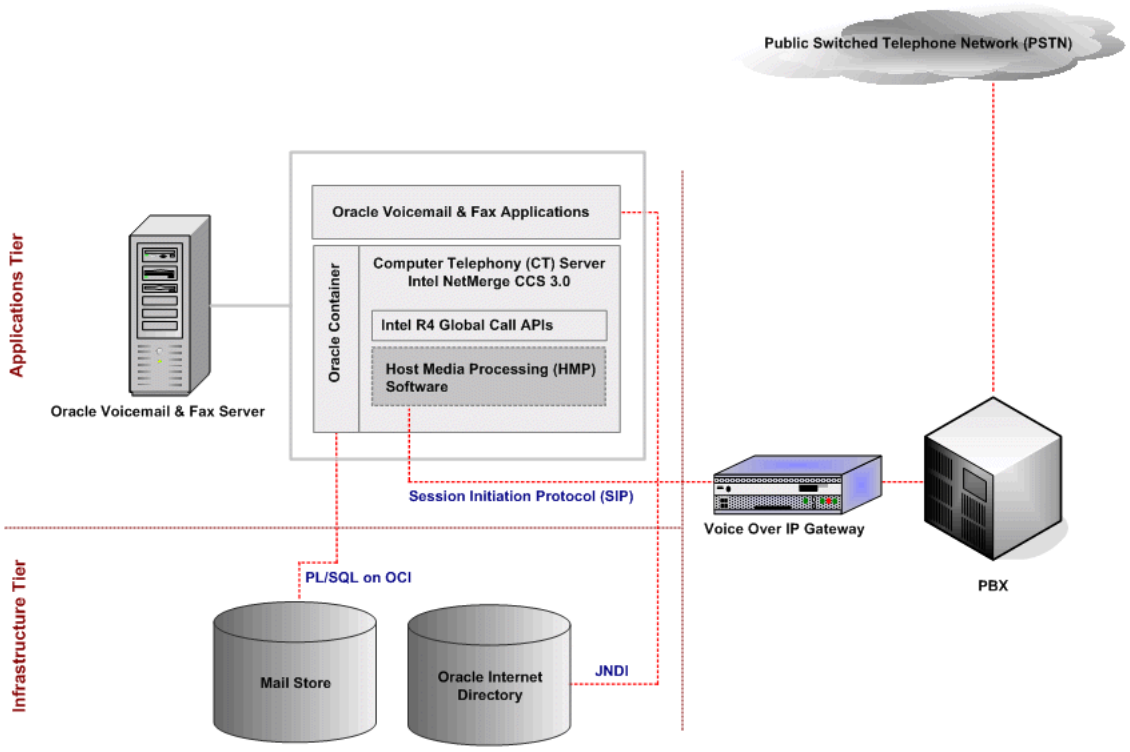


Figure 12–3 illustrates an Oracle Voicemail & Fax VoIP configuration. This figure contains the following components:

- Oracle Collaboration Suite Infrastructure tier
- Application tier
- VoIP Gateway
- PBX
- PSTN

Infrastructure Tier

In , the Infrastructure tier contains the mail store and the Oracle Internet Directory.

Applications Tier

In the Applications tier contains the Oracle Voicemail & Fax server. Details of the Oracle Voicemail & Fax server are described in the section.

Functionality

Communication between the Oracle Container in the Oracle Voicemail & Fax server and the mail store takes place using PL/SQL on OCI. Communication between the Oracle Voicemail & Fax applications and Oracle Internet Directory takes place using JNDI. Communication between the Oracle Voicemail & Fax HMP and the VoIP Gateway and between the VoIP Gateway and the PBX takes place using the Session Initiation Protocol (SIP).

Planning for Oracle Voicemail & Fax Deployment

This section contains Oracle Voicemail & Fax deployment planning information. Deploying Oracle Voicemail& Fax involves a wide range of issues. These include hardware and software prerequisites, sizing guidelines, firewall issues, and topology considerations for a geographically distributed organization.

Deployment Steps

Before deploying Oracle Voicemail & Fax, you should review the required deployment steps.

Step 1: Architect and Design the Voicemail Solution

You can choose from a number of different deployments of Oracle Voicemail & Fax depending on your organization's requirements. For example, your organization may have several different sites each with their own PBX. You may wish to distribute the Oracle Voicemail & Fax server to each of these sites instead of at the data center that contains the Oracle Collaboration Suite infrastructure components. You may also select either a Circuit Switched or VoIP configuration and a high availability version of each depending on your requirements. You should consult the "Oracle Voicemail & Fax Deployment Configurations" of this chapter when architecting and designing your voicemail solution.

See Also: For more information, please see:

- The "Oracle Voicemail & Fax Deployment Configurations" section of this chapter
- *Oracle Voicemail & Fax Administrator's Guide*

Step 2: Provide Telephony Server Hardware and Software

When deploying Oracle Voicemail & Fax, you must provide the required CT server hardware and software. For more information, please see the "Hardware and Software Requirements" section.

Step 3: Install and Configure the Telephony Server(s)

For information on installing and configuring the CT Servers, see the following guides:

- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

Step 4: Configure the Oracle Collaboration Suite Infrastructure Tier and Application Tier Components

For information on configuring the required Oracle Collaboration Suite Infrastructure tier and Applications tier components, see*Oracle Voicemail & Fax Administrator's Guide*

Step 5: Install the Oracle Voicemail & Fax Components on Each Telephony Server

For information on installing the Oracle Voicemail & Fax Components on each CT Server, see the following guides:

- *Oracle Collaboration Suite Installation Guide for Solaris Operating System*
- *Oracle Collaboration Suite Installation Guide for Microsoft Windows*

Step 6; Start the Different Processes

For information on starting the different Oracle Voicemail & Fax processes, see*Oracle Voicemail & Fax Administrator's Guide.*

Step 7: Add Voicemail & Fax Users

For information on adding Oracle Voicemail & Fax users, see *Oracle Voicemail & Fax Administrator's Guide*

Hardware and Software Requirements

This section describes the hardware and software requirements for deploying Oracle Voicemail & Fax.

Hardware Requirements

Oracle Voicemail & Fax has the following hardware requirements:

> **Note:** Requirements will be partly based on usage (e.g. a small server can handle a small number of concurrent calls while a larger server can handle many more).

- Intel Based Server
- Single or Dual Pentium 3 or higher CPU
- 2 GB RAM
- CD ROM Drive
- NIC

- Windows 2000 Professional

Certified Configurations

Oracle Voicemail & Fax may be deployed on many different Intel based platforms depending upon customer requirements. The following configuration are certified by Oracle for use in our own data centers and can be used as guidelines.

> **Note:** Oracle operational requirements may or may not match your organizations requirements. Oracle does not endorse or promote any server provider.

- Dell PowerEdge 2850
- Dual 2.5 Xeon with 1MB Cache
- 2GB DDR SDRAM
- 1.44MB Floppy Drive,
- 24x CD ROM,
- RAID 1 with (2) 36GB Hard Drives
- Dual 100= NIC Card,
- Keyboard/Mouse,
- Windows 2000 Server

Software Requirements

Oracle Voicemail & Fax has the following software requirements:

- Microsoft Windows 2000 Server Edition or higher
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows Server Resource Pack
- Intel NetMerge CCS 3.0 Service Pack 1
- Sun Java 2 RTE (version 1.3.1_03), installed with Intel NetMerge CCS 3.0

Overall Implementation Considerations

This section discusses overall implementation considerations.

Switching Infrastructure

Often, the decision to switch infrastructure drives the options available for voicemail implementation. As a media server application, Oracle Voicemail & Fax can support any combination of the following common switching options:

- **Distributed Switchin**g: Each office or site of an organization has its own switching infrastructure and direct access to the PSTN. This configuration is common in the United States CPE market. Implementing Oracle Voicemail & Fax in this environment replaces the voicemail solution already in place and re-uses existing switching infrastructure. Site sizes range from the very small office (for example, sales offices with less than 50 users) to complete buildings or large campuses.

- **Centralized Switching**: In Europe and other parts of the world, centralized switching supporting multiple locations or regions is common. Implementing Oracle Voicemail & Fax in this environment also replaces the existing voicemail solution and can reuse the same switching infrastructure. These environments will normally have larger user populations.
- **Centralized VoIP**: VoIP implementations offer distributed offices the ability to appear as a consolidated environment without the need for new large telecommunications networks. Oracle Voicemail & Fax implementations can be centralized in the data center alongside the voice call control capabilities.

Comparative Network Costs

Another implementation consideration is the cost comparison between the traditional circuit switched network and the IP network. An organization with low-cost call providers may choose to route all calls to a centralized set of media servers rather than acquire the necessary IP network bandwidth to each site. Conversely, a company with a low-cost or well-developed IP network may decide to place media servers in each site or implement VoIP call transport in order to maximize efficiency of the general purpose IP network. Cost considerations should be analyzed with an understanding of the organization's overall network strategy (circuit switched and IP) and VoIP strategy.

IP Network Considerations

Quality of service (QoS) across the network is perhaps the largest issue with VoIP implementations and related telephony applications (such as Oracle Voicemail & Fax). When reviewing the IP Network infrastructure, organizations should take into account projected network bandwidth (size of the pipe), latency (pipe speed), and QoS (pipe congestion and performance during a call or application session). Running VoIP and Oracle Voicemail & Fax on the IP network may also impact the performance of other applications sharing the network. Care should be taken to evaluate the complete network traffic profile rather than individual applications when sizing the underlying network.

High Availability Considerations

The Oracle Voicemail & Fax solution enables you to implement the appropriate amount of availability for each site. High availability considerations generally fall into three areas:

- Telephony servers
- Message store
- Network

Telephony Servers

Storing messages in a central Oracle database rather than the telephony server itself, enables you to deploy redundant servers at a single site. In this configuration, telephone-hunt groups (configured on the switch) provide both load balancing and backup or fail over capabilities if one of the telephony servers become disabled. Server vendors also provide a number of high availability options and components allowing you to acquire hardware that meets your individual requirements.

Implementing redundant telephony servers is more cost-effective for larger organizations than smaller ones. If you have a large organization, then you may want to consider centralizing both the switching and telephony servers in a data center. This has the added benefit of lower management and service requirements.

Service requirements and spares strategies are another important consideration when comparing the costs of a distributed instead of a consolidated voicemail implementation. Depending upon the hardware vendor used and the location of the office, the cost of providing 2 or 4 hour response times and additional spares storage onsite may be prohibitive.

Message Store

Oracle Voicemail & Fax utilizes the Oracle Mail message store for voicemail and fax storage. You can optionally implement Oracle10*g* Real Application Clusters as well as all Oracle Data Guard technologies for offsite business resumption and standby database capabilities.

> **See Also:** For more information on making the mail store highly available, see the "Oracle Collaboration Suite High Availability Architectures" section of Chapter 3, "Deploying Oracle Collaboration Suite"

Networks

Oracle Voicemail & Fax is dependent upon the underlying network (circuit switched or IP). You should review network architectures of your organization for single points of failure (even in multi-vendor environments) and aggregate bandwidth requirements.

VoIP Deployment Considerations

This section discusses VoIP deployment considerations.

Bandwidth Requirements

Bandwidth between the expected end points is one of the first areas to research when deploying any VoIP solution, including Oracle Voicemail & Fax. Depending upon the codec (encoding of voice in the IP packets), the bandwidth requirements will vary between 95 kbps each channel (two way call) when using the g.711 codec and 37 kbps each channel when using g.729a. Oracle Voicemail & Fax and the associated Intel infrastructure can support both of these codecs. These numbers are approximate and depend upon your use of other technologies including header compression, comfort noise detection (CNG) and voice activity detection (VAD).

Other factors to consider include the features supported by your chosen VoIP gateway and if fax will be used within the implementation. Today, many VoIP gateways support the ability to re-negotiate the codec depending upon the media type. This is especially useful when inbound fax is implemented as it enables the use of a lower bandwidth codec for voice calls while switching to higher bandwidth codecs (g.711) for accurate fax support.

Another gateway dependent capability that will help to determine the appropriate codec (and therefore the needed bandwidth) is support for Out of Band DTMF (RFC 2833). This standard enables all DTMF traffic to be broken out from the RTP voice traffic and sent to the Voicemail & Fax endpoint using other IP transport, thus allowing the use of lower bandwidth compressed codec like g.729. If your VoIP Gateway does not support this capability, then Oracle recommends that all voice traffic be g.711 as the lower quality voice associated with highly compressed codecs may not normally allow adequate DTMF recognition.

Latency

Latency, also known as delay, is defined as the time a packet takes to travel between the beginning endpoint and destination endpoint, including all network hops. Recommendations for maximum one-way latency range from 150 milliseconds (ITU-T recommendations) through about 250 milliseconds in real life for traditional two way conversations. Once latency increases beyond 250 milliseconds, talk-over (where the delay causes end users to start talking before hearing a response,) can become an issue.

When compared to voice conferencing or two party live phone calls, the effects of latency are somewhat less apparent with Oracle Voicemail & Fax as the caller expects to interact with an application and is prompted for actions. It is not recommended that customers deploy Oracle Voicemail & Fax using VoIP when end point latency is over approximately 300 milliseconds.

Packet Loss

Loss of packets or receiving packets in mixed order is another typical issue associated with running VoIP on a mixed (data and voice) network. This is the second component of what is normally called jitter (the first is latency discussed earlier) and usually manifests itself to end users as stuttering or silent spots within the conversation or message. This situation occurs frequently in saturated networks where packet collisions cause lost packets and packet queues. This is common at network choke points such as routers and switches.

Misordered packets generally occur when the packets take differing routes across the network to the same destination. Just as with packet loss, this can occur in any IP network but occurs more frequently as network saturation increases.

Both of these conditions can be managed to some degree with techniques such as packet replacement and Jitter buffers. As it's name implies, the Jitter buffer enables the receiving end point to assemble the packets in the correct order before rendering to the caller. Packet replacement applies algorithms that look at the surrounding packets and make a best guess of the contents of the missing packets. These solutions come with a price in both latency and additional computing power requirements that become more visible as the underlying network latency increases.

Neither of these solutions will provide a perfect end user experience and a poorly performing network will eventually manifest itself. These technologies can help mask smaller hiccups and issues.

The Intel infrastructure that Oracle certifies with supports these techniques. Your choice of VoIP gateway will determine availability on the gateway side.

Network Availability (VoIP)

Network availability is a complex subject that ranges from disaster recovery planning to onsite hardware redundancy. While many organizations look at their overall data infrastructure and networks as business critical, data networks have traditionally been viewed (and managed) as less reliable than the concurrent telephone network. With the addition of voice services to the IP network, availability of the core IP network becomes a key issue. Following are important network availability considerations for Oracle Voicemail & Fax deployment:

- **Redundant network providers**: For key sites, consider the use of multiple network providers. This enables your organization to function even if the primary network provider goes down. Be aware that different network providers may provide connectivity on the same underlying link.

- **Redundant routes**: Plan for situations where connectivity is lost between outlying sites and a main site by ensuring redundant network access through multiple network hubs. The level of redundancy is a business decision driven by the cost of downtime compared to the network costs.
- **Redundant equipment**: A single point of failure on a network may be as bad as a single point of failure in a physical server. Plan to have multiple routers, switches and gateways.
- **Traffic studies**: Traffic studies provide insight into the volume and types of network traffic. Clearly this is a pre-requisite for determining if your network will support deploying VoIP based Oracle voicemail
- **Network monitoring**: Once the application is up and available, managing the system and ensuring a good user experience is critical. Network management tools and methodologies will vary based on your preferred network and network management vendor.

Oracle Voicemail & Fax

Sizing requirements for Oracle Voicemail & Fax are based on the expected number of concurrent callers recording, retrieving messages, and receiving faxes. Table 12–1 lists guidelines for configuring your hardware.

Table 12–1 Recommended User-to-Port Ratios

Number of Users	User-to-Port Ratio
Under 100	20:1
100 - 300	30:1
300 - 500	40:1
500 - 1000	50:1
1000 or more	75-100:1

Actual requirements vary based on the roles and responsibilities of end users. For example, a site with call center users who receive large numbers of voice mail messages may require a lower ratio compared to a back-office site which receives little call activity.

The following considerations apply:

- A normal scenario is to size the system based on two calls each voice mail message: one for leaving a message and one for retrieving a message. The number of calls will normally be reduced to between 1.25 and 1.5 each voice mail message when deploying Oracle Voicemail & Fax and Oracle Mail together, because some users will retrieve Voicemail through their e-mail client.
- Additional cards can be added to the configurations up to the number of free slots available in any server number. The number of slots available is dependent on server hardware.
- Multiple Oracle Voicemail & Fax servers may be used to support a single site.

Oracle Voicemail & Fax Hardware Recommendations

The following tables list CPU and telephony card hardware configuration recommendations based on the expected number of users each site and redundancy requirements.

Note: The following table assumes a digital PBX compatible with an Intel D82JCTU card with eight ports. Other cards with different port counts and interfaces can also be used

Table 12–2 500 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	1	1
Dual-CPU servers	0	0
Intel Dialogic/82JCTU cards	2	2
VFX/PCI cards	1	1

Table 12–3 1000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	0	0
Dual-CPU servers	1	1
Intel Dialogic/82JCTU cards	4	4
VFX/PCI cards	1	1

Table 12–4 2000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	1	0
Dual-CPU servers	1	1
Intel Dialogic/82JCTU cards	7	5
VFX/PCI cards	2	1

Table 12–5 3000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	0	0
Dual-CPU servers	2	1
Intel Dialogic/82JCTU cards	8	5
VFX/PCI cards	2	1

Table 12–6 4000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	1	0
Dual-CPU servers	2	1
Intel Dialogic/82JCTU cards	11	5
VFX/PCI cards	3	1

Table 12–7 5000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	0	0
Dual-CPU servers	3	1
Intel Dialogic/82JCTU cards	13	5
VFX/PCI cards	3	1

Table 12–8 10000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	1	0
Dual-CPU servers	5	1
Intel Dialogic/82JCTU cards	26	5
VFX/PCI cards	6	1

Table 12–9 20000 User Site

Resource	Primary System	Secondary Systems
Single-CPU servers	1	0
Dual-CPU servers	10	1
Intel Dialogic/82JCTU cards	52	5
VFX/PCI cards	11	1

Oracle Voicemail & Fax Deployment Configurations

This section discusses available deployment configurations for Oracle Voicemail & Fax

Consolidated Oracle Voicemail & Fax Server Configuration

In a consolidated Oracle Voicemail & Fax Server configuration, all voicemail and e-mail services are centralized in one data center supporting all components of the messaging solution. Telephony servers running the Oracle Volcano & Fax applications are connected to one or more switches that are either PBXs or VoIP gateways.

Figure 12–4 Consolidated Oracle Voicemail & Fax Server Configuration

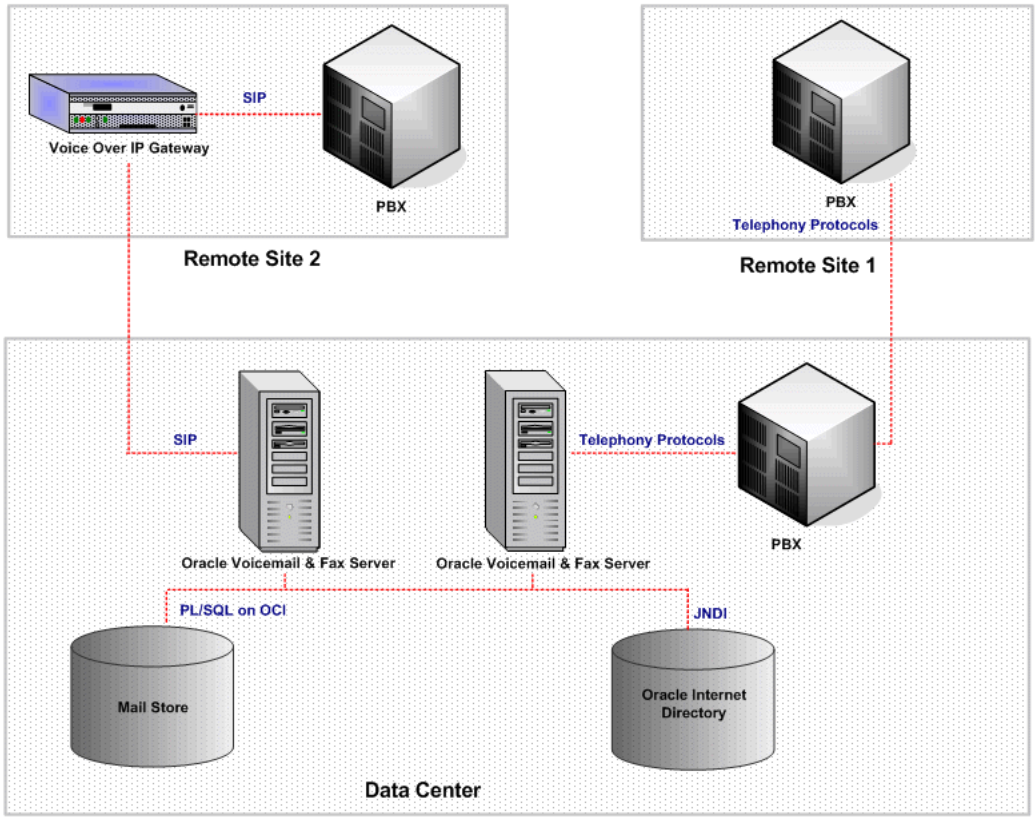


Figure 12–4 illustrates the consolidated Oracle Voicemail & Fax Server configuration. In this figure the Oracle Voicemail & Fax Server, mail store, and Oracle Internet Directory are centralized in one data center supporting all components of the messaging solution. The PBX or PBX with VoIP Gateway are optionally deployed in the datacenter itself, or in remote sites. If the data center supports both a PBX and a VoIP Gateway, then it requires one Oracle Voicemail & Fax server for each.

Advantages

This configuration has the advantage of consolidating management and all infrastructure in one place. This lowers management, administration, and ongoing hardware support costs (spares management requirements are minimized) while also reducing to a minimum the cost to maintain hardware footprints in multiple sites.

Disadvantages

Total consolidation requires that all sites ship calls to the data center. This can be accomplished over leased lines, the PSTN or over a VoIP implementation. While conceptually the most pure, this configuration requires additional infrastructure costs that may not be appropriate for some organizations. When consolidating switching to support this approach, dial plans may need to be re-evaluated.

Distributed Oracle Voicemail & Fax Server Configurations

In a distributed Oracle Voicemail and Fax Server configuration, the Oracle Voicemail and Fax Server is stored in sites with their own circuit switched or VoIP telephone

systems. This is also known as a partial consolidation because the voicemail and e-mail services are partially consolidated.

Distributed Circuit Switched Oracle Voicemail & Fax Configurations

The following figure illustrates a distributed circuit switched, Oracle Voicemail & Fax server configuration.

Figure 12–5 Distributed Circuit Switched Configurations

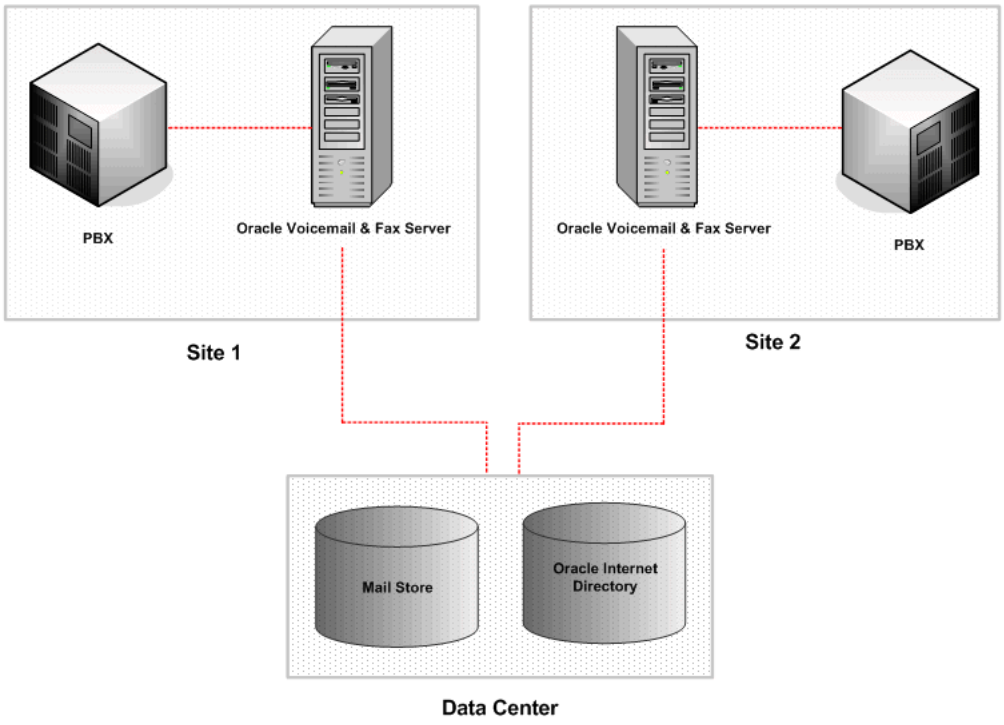


Figure 12–5 illustrates a distributed circuit switched, Oracle Voicemail & Fax server configuration. This figure contains a data center and two remote sites labeled Site 1 and Site 2. The data center contains the mail store and Oracle Internet Directory. Site 1 and Site 2 each contain a PBX and the Oracle Voicemail & Fax server.

Advantages

This configuration enables your organization to keep its investment in existing switching technologies and to leverage its IP network for messages movement between the CT Server and message store. No change in dial plan is needed.

Disadvantages

While distributed telephony servers can be managed and administered from the data center, support and deployment costs are higher compared to the consolidated deployment due to the number of individual sites that must be supported.

Distributed VoIP Configurations

The following figure illustrates a distributed VoIP, Oracle Voicemail & Fax server configuration.

Figure 12–6 Distributed VoIP Configurations

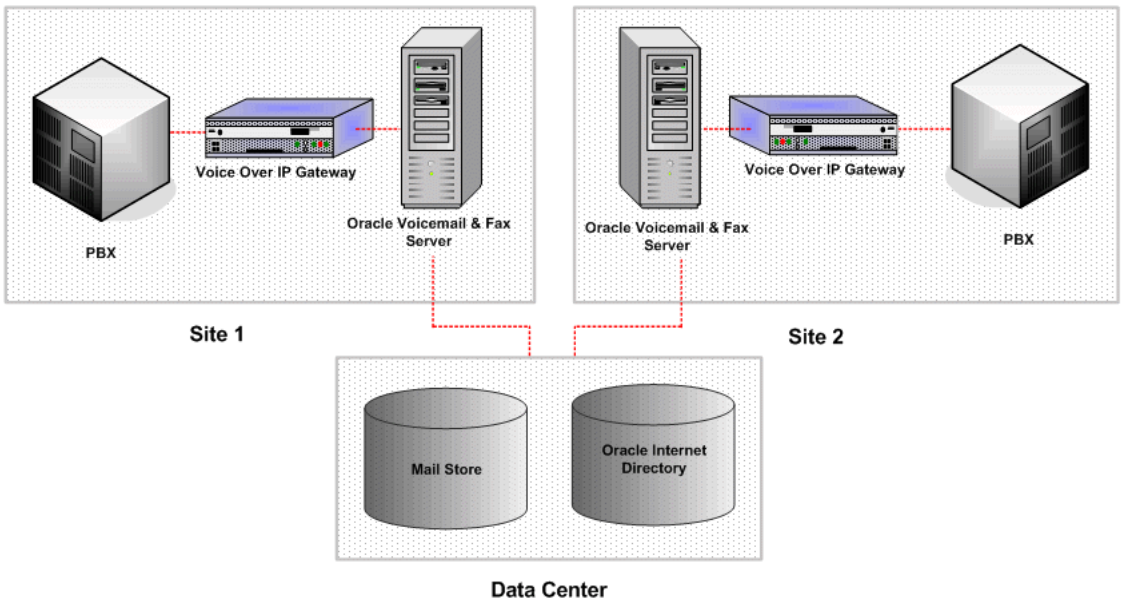


Figure 12–6 illustrates a distributed VoIP, Oracle Voicemail & Fax server configuration. This figure contains a data center and two remote sites labeled Site 1 and Site 2. The data center contains the mail store and Oracle Internet Directory. Site 1 and Site 2 each contain a PBX, a VoIP Gateway and the Oracle Voicemail & Fax server.

VoIP Multiple PBX Configuration

You can deploy Oracle Voicemail & Fax with the VoIP Gateway to support multiple PBXs. This configuration is especially useful in organizations that have a number of smaller offices that cannot easily provide server maintenance and that do not require all of the capacity of a single server. In this case, the number of individual offices can continue to grow until the Voicemail & Fax server reaches capacity.

Figure 12–7 VoIP Multiple PBX Configuration

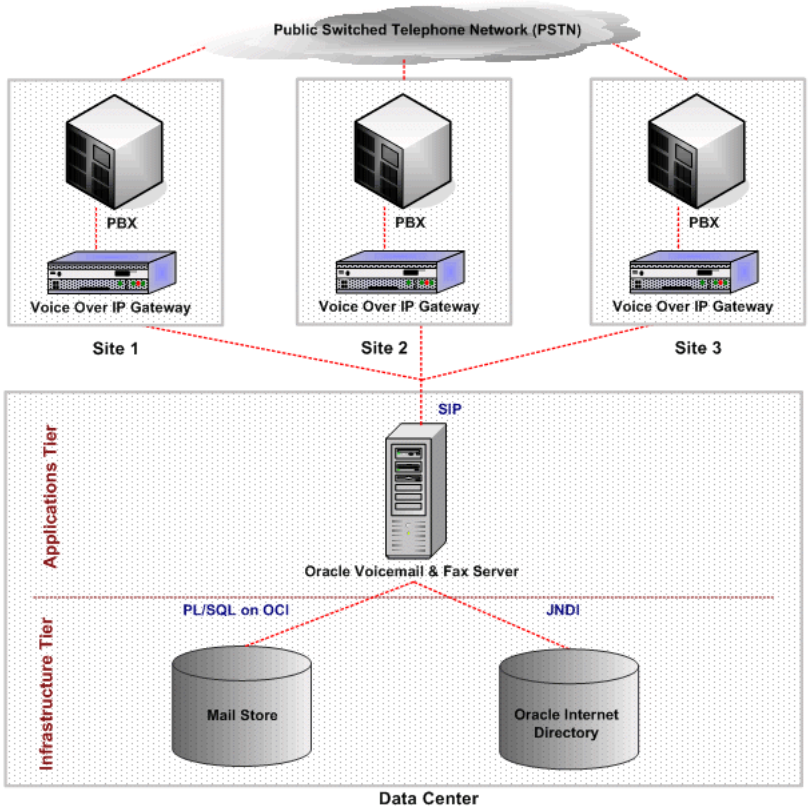


Figure 12–7 illustrates a VoIP multiple PBX configuration. This figure contains a data center and three remote sites labeled Site 1, Site2 and Site 3. The Infrastructure tier of the data center contains the mail store and Oracle Internet Directory. The Applications tier of the data center contains the Oracle Voicemail & Fax server. Each of the remote sites contains a PBX and VoIP gateway. The VoIP gateways communicate with their respective PBXs and to the Oracle Voicemail & Fax server using SIP. The Oracle Voicemail & Fax server communicates with Oracle Internet Directory using JNDI and with the mail store using PL/SQL on OCI.

Oracle Voicemail & Fax Server Mixed Switching Configuration

A complete Oracle Voicemail & Fax system can support multiple sites and integration types. In this configuration, some sites may use VoIP to transport calls to a voicemail & fax server co-located with the Oracle collaboration Suite infrastructure in the data center, while other sites may use a boarded voicemail & fax server sitting next to the PBX.

Figure 12–8 Oracle Voicemail & Fax Server Mixed Switching Configuration

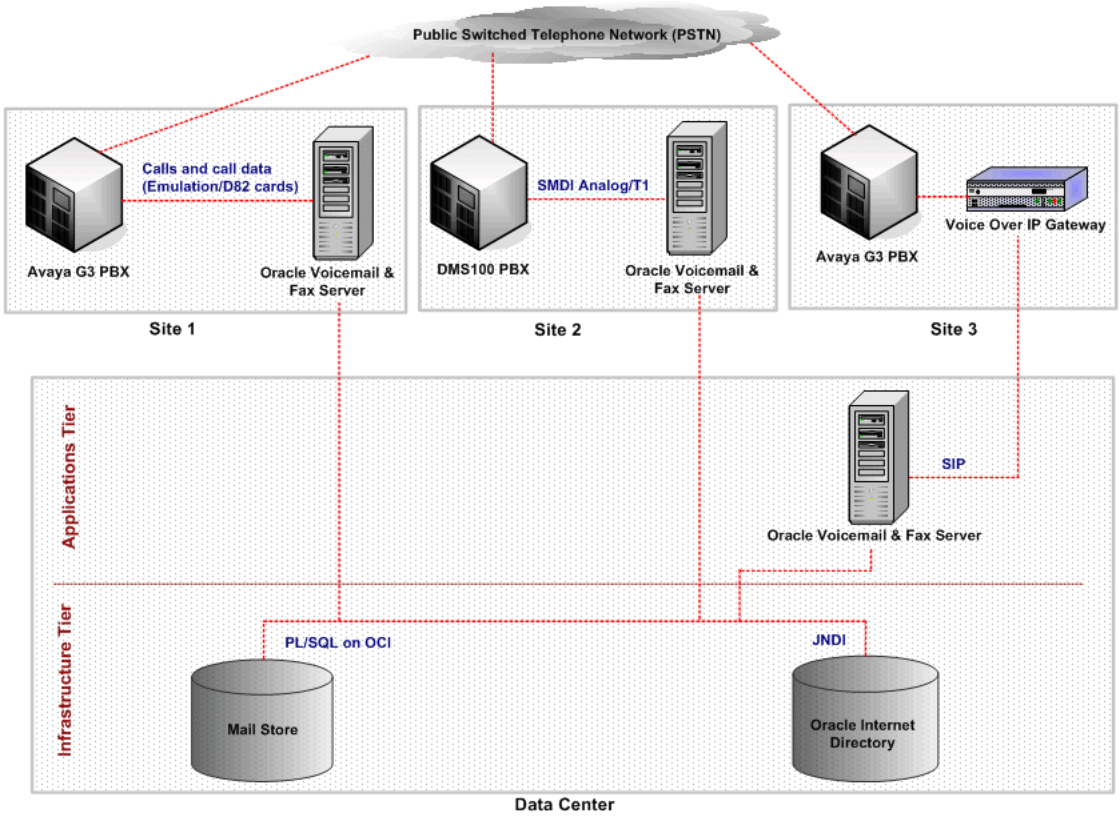


Figure 12–8 illustrates an Oracle Voicemail & Fax Server Mixed Switching Configuration. This figure contains a data center and three remote sites labeled Site 1, Site2 and Site 3. The data center's Infrastructure tier contains the mail store and Oracle Internet Directory and its Applications tier contains the Oracle Voicemail & Fax servers. Site 1 contains an Avaya G3 PBX, Site 2 contains a DMS100 PBX and each site contains the Oracle Voicemail & Fax Server. Site 3 contains an Avaya G3 PBX and a VoIP Gateway.

The PSTN communicates with the PBXs in each remote site, In Site 1 and Site 2, the PBXs communicate with the Oracle Voicemail & Fax Server using telephony protocols and in Site 3 the PBX communicates with the VoIP Gateway using SIP. The Oracle Voicemail & Fax Server on Site 1, Site2 and the data center communicate with Oracle Internet Directory using JNDI and with the mail store using PL/SQL on OCI. The VoIP Gateway in Site 3 communicates with the Oracle Voicemail & Fax server using SIP.

High-Availability Configurations

With Oracle Voicemail & Fax, the PBX can be configured to act like a load balancer. PBXs can determine when a call is answered or not (usually known as a Ring No Answer in the industry). Groups of telephone lines known as hunt groups are configured with a routing plan which can be configured to follow specifics routes depending upon the result of a call handling request. A typical deployment rule may include:

- If call is not answered at user desk phone, then roll over call to voicemail huntgroup 1 (7200).

- If call is not answered at voicemail huntgroup 1 after 3 rings, then roll call over to voicemail backup huntgroup (7250).
- If voicemail huntgroup 1 is busy, then camp call on voicemail huntgroup 1 for 5 rings.
- If call is not answered at voicemail backup huntgroup after 3 rings, then roll call over to voicemail.

With Oracle Voicemail & Fax, you can set up circuit switched and VoIP configurations for high availability.

CIrcuit Switched High-Availability Configuration

The following figure illustrates a circuit switched high-availability configuration.

Figure 12–9 Circuit Switched High-Availability Configuration

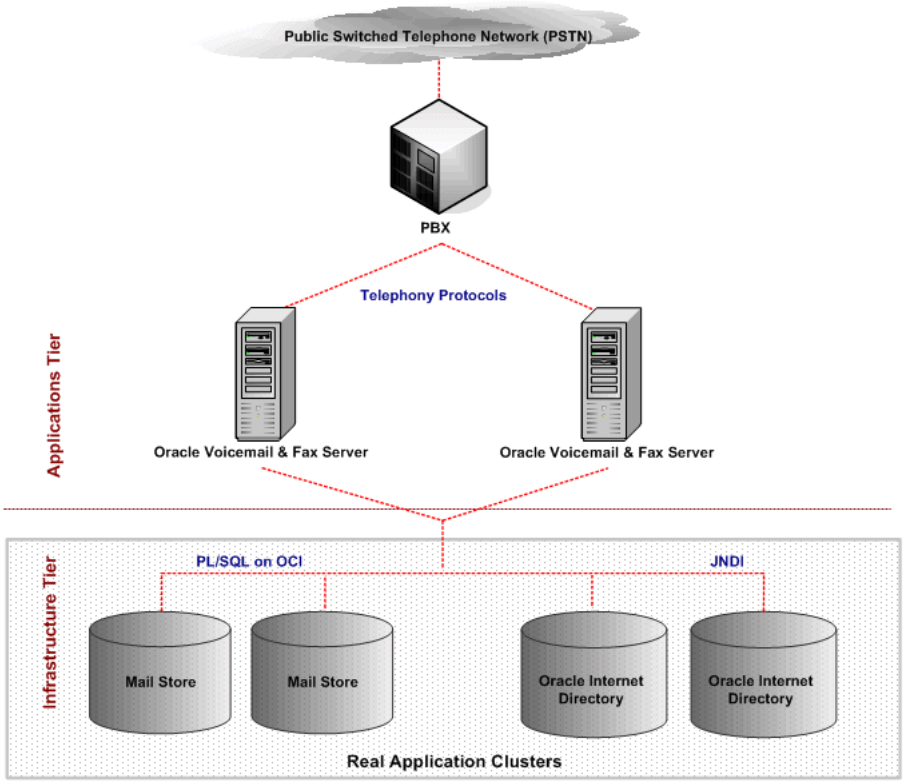


Figure 12–9 illustrates a circuit switched high-availability configuration. In this figure, a PBX routes calls to one of two Oracle Voicemail & Fax servers. If one Oracle Voicemail & Fax servers is not available, then the VoIP Gateway routes calls to the other one. Infrastructure tier components are configured with Oracle10*g* Real Application Clusters for hardware redundancy.

VoIP High-Availability Configuration

Voice applications and the telephone network are normally considered more reliable than data applications and have much higher user expectations in areas such as performance and availability. When deployed with VoIP, Oracle Voicemail & Fax can be deployed redundantly at a number of levels in order to minimize downtime and

maximize performance. One example of this is the ability to support multiple VoIP gateways connected to the same PBX.

This model provides both device redundancy and additional capacity when using low cost VoIP gateways such as the Intel PIMG. Voicemail call carrying capacity can be added with the addition of more gateways. Redundant gateways provide an ideal way to ensure that a single gateway failure does not cause a complete service outage. In this scenario, the PBX continues to route calls to the surviving gateways until the failed device can be repaired or replaced.

Additionally, multiple Voicemail & Fax servers can be deployed behind a SIP Proxy or traditional IP load balancer in order to ensure that there is no single point of failure for the voicemail application. The Infrastructure tier can be deployed using Oracle10*g* Real Application Clusterswhich provides fault tolerance and enhanced scalability for the Suite infrastructure.

Figure 12–10 VoIP High Availability Configuration

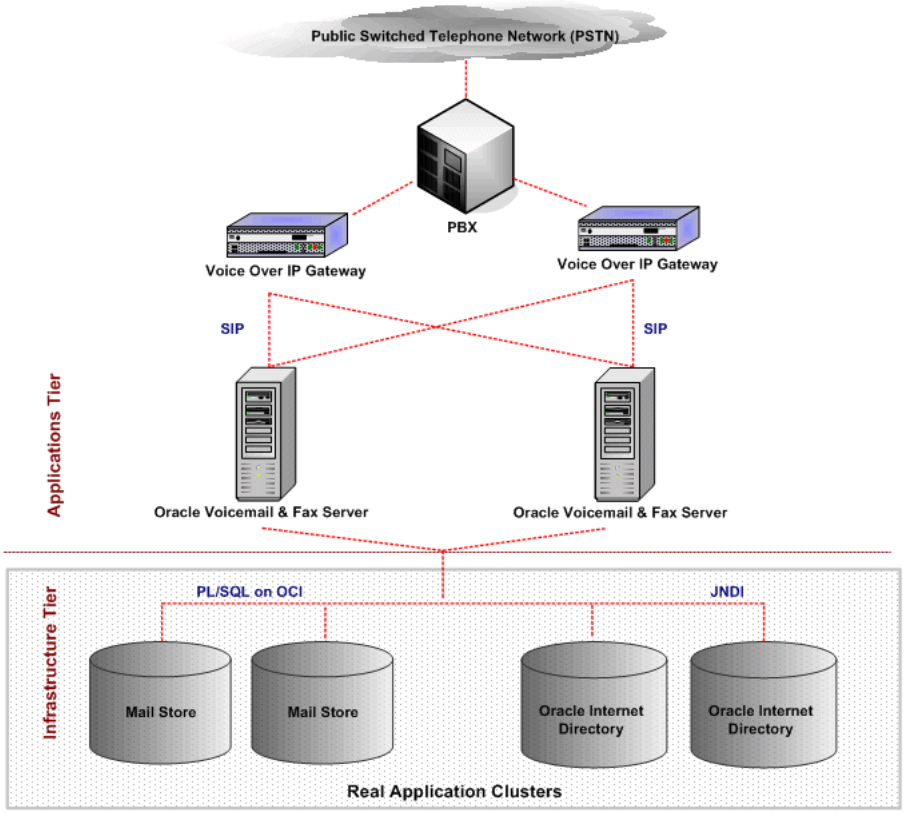


Figure 12–10 illustrates a VoIP high-availability configuration. In this figure a PBX routes calls to one of two VoIP gateways. If one of the VoIP gateways is not available, then the PBX routes calls to the other one. The VoIP gateways routes calls to one of two Oracle Voicemail & Fax servers. If one Oracle Voicemail & Fax servers is not available, then the VoIP Gateway routes calls to the other one. Infrastructure tier components are configured with Oracle10*g* Real Application Clusters for hardware redundancy.

13

Deploying Oracle Workspaces

This chapter contains the following topics:

Understanding the Oracle Workspaces Architecture and Functionality

This section provides an overview of Oracle Workspaces and explains the application's architecture and functionality.

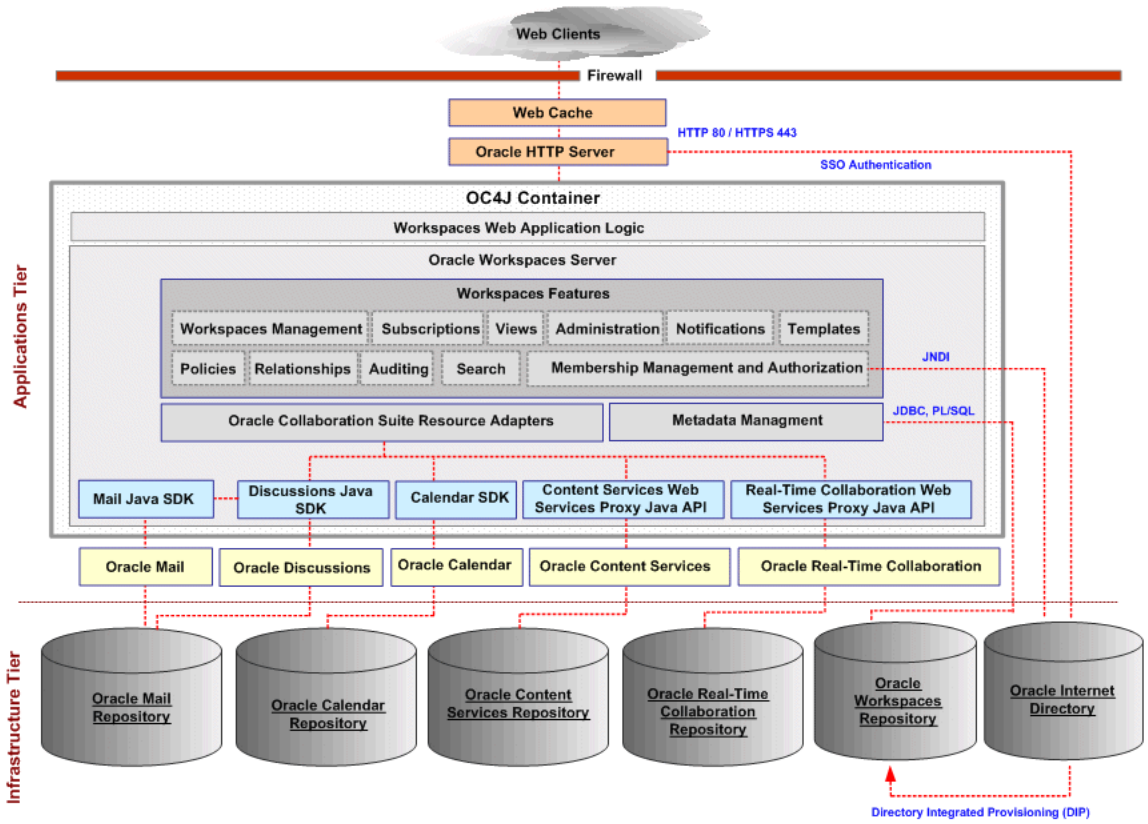
Overview

Oracle Workspaces is a collaborative application that captures information from other Oracle Collaboration Suite applications including Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, and Oracle Real-Time Collaboration and makes this information persistently available to members of a project team within the context of the project. For example, a project development team can have its own project workspace from which its members share documents, start discussion topics on specific development problems, schedule team meetings, and send each other messages. All project collaboration information is captured and made persistently available to all team members who access the workspace.

Oracle Workspaces Architecture

Oracle Workspaces is built upon other Oracle Collaboration Suite applications including Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, and Oracle Real-Time Collaboration. The following figure illustrates the Oracle Discusssions architecture and functionality:

Figure 13–1 Oracle Workspaces Architecture and Functionality



Applications Tier

The Applications tier contains the following components:

- **Web Cache:** Web client requests are process through Web Cache and then forwarded to the Oracle HTTP Server.
- **Oracle HTTP Server**: First it sends an HTTP or HTTPS requests Oracle Internet Directory to perform single sign-on authentication, and then sends an HTTP or HTTPS request to the OC4J container.
- **OC4J Container**: Oracle Workspaces is deployed as a J2EE application in an OC4J container. The application comprises the following:
  - **Workspaces Web Application Logic**: The Workspaces Web Application Logic contains the Web application which enables users to interact with Oracle Workspaces. The Web application enables users to create and manage workspaces as well as workspace content such as files, meetings, tasks, discussions, and web conferences. It also provides access to additional workspace features such as views, links, and notifications. The Workspaces Web Application is built on the Oracle Workspaces Java SDK APIs.
  - **Oracle Workspaces Server:** The Oracle Workspaces Server contains the following:
    * **Workspaces Services**: The workspaces services are discussed in the following table.

Table 13–1 Oracle Workspaces Features

Oracle Workspaces Feature	Definition
Workspaces Management	Enables the creation and deletion of workspaces as well as the editing of the metadata that describes a workspace.
Subscriptions	Allow users to receive e-mail that is sent to the workspace inbox service in a push-style fashion.
Views	Allow users to group disparate items within a workspace into logical, named containers for convenient access.
Administration	Enables users with sufficient privilege to administer workspaces and application-level settings. These include workspace creation policies and defaults, recovery of damaged workspaces, application role assignment, template management, and service status management.
Notifications	Each workspace settings allow workspace administrators to set up automatic e-mail notifications when members are added or removed from a workspace. In addition, many common operations within a workspace support convenient single-click manual notification of members.
Templates	A template defines the skeletal structure of a workspace, including the content in its associated services. A workspace with a specified set of properties and initial service content can be created in a single operation using a template. In addition, an existing workspace can be used to define a template.
Policies	Policies at the application level govern which users can create workspaces, whether notification features are enabled, the format and content of notification e-mail messages, and the default template to use in workspace creation.
Relationships	Most service content in a workspace, including files, folders, meetings, tasks, discussion forums, discussion topics, and discussion messages, can be related to other content. A relationship is a logical link between the two items. Such links can have descriptions and can be viewed with the properties of an item. Relationships provide a powerful way to realize semantic connections between items.
Auditing	Whenever a workspace or a content item within a workspace is modified, the user performing the modification and the time of modification are stored. These properties are presented in the user interface. In addition, login and logout times of users are stored, which enables workspaces to determine whether any new activity has taken place. An icon is presented in the user interface to indicate new activity.
Search	Users may search for content both within a workspace or across all workspaces to which they have access. The search can be for a specified content type or for all supported content types. Users may also search for workspaces based on their names and descriptions.
Membership Management and Authorization	Members may be added to or removed from workspaces; they are given the role of reader, writer, or administrator in each workspace to which they belong. The workspace role of a member determines which workspace actions are permitted.

* **Oracle Collaboration Suite Resource Adapters**: Each resource, or service, is presented through the workspaces user interface in addition to its own native interface. The adapters present the disparate service content within

a single logical entity, the workspace. Each adapter has an associated Java API which can be used to programmatically manipulate service content within a workspace. The Java APIs for different services follow the same design guidelines and share the same class hierarchy.

* **Metadata Management**: In addition to exposing service content, the workspaces user interface enables users to manipulate workspaces and workspace metadata. This is built upon a Java API for workspace metadata management, which together with the set of resource adapters APIs, comprises a single unified Java API for programmatically interacting with workspaces and workspace content.
* **Mail Java SDK**: The Mail Java SDK is used by Oracle Discussions, which in turn is a dependency of Oracle Workspaces. This enables discussion forums within Oracle Workspaces to be viewed as IMAP shared folders from standard email clients.
* **Discussions Java SDK**: The Discussions Java SDK is used by Oracle Workspaces to interface with the Discussions product and provide workspace-centric forums and inbox capabilities.
* **Calendar SDK**: The Calendar SDK is used by Oracle Workspaces to interface with the Calendar product and provide workspace-centric meetings, tasks, and web conferences. Note that Calendar SDK internally depends on the RTC Proxy Java API to provide web conferencing features.
* **Content Services Web Services Proxy Java API**: The Content Services Web Services Proxy Java API is used by Oracle Workspaces to interface with the Content Services product and provide workspace-centric file and folder management.
* **Real-Time Collaboration Proxy JAVA API**: The Real-Time Collaboration Proxy Java API is used by Oracle Workspaces to provide presence information for workspace members. It is also used indirectly by Workspaces through the Calendar SDK, which depends on the Real-Time Collaboration Proxy Java API.

Oracle Collaboration Suite Applications

Oracle Workspaces uses the earlier referenced APIs to capture information from other Oracle Collaboration Suite applications including Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, and Oracle Real-Time Collaboration. Once this information is captured from these applications, Oracle Workspaces makes it persistently available to members of a project team within the context of the project.

Infrastructure Tier

The Infrastructure tier contains the following components:

Oracle Internet Directory

Oracle Workspaces authorization information is stored in the Oracle Internet Directory. The Oracle Workspaces Web Application is designed so that permissions are checked through on Oracle Internet Directory lookup before performing any write operation, such as creating and managing workspaces.

Oracle Calendar Repository

The Oracle Calendar repository contains Oracle Calendar data. Oracle Workspaces takes calendar data and makes this information persistently available to members of a project team within the context of the project.

Oracle Content Services Repository

The Oracle Content Services repository contains Oracle Content Services data. Oracle Workspaces takes content from Oracle Content Services and makes this information persistently available to members of a project team within the context of the project.

Oracle Discussions Repository

The Oracle Discusssions repository contains Oracle Discusssions data. Oracle Workspaces takes content from Oracle Discusssions and makes this information persistently available to members of a project team within the context of the project.

Oracle Mail Repository

The Oracle Mail repository contains Oracle Mail data. Oracle Workspaces takes e-mail messages and makes them persistently available to members of a project team within the context of the project.

Oracle Real-Time Collaboration Repository

The Oracle Real-Time Collaboration repository contains Oracle Real-Time Collaboration data. Oracle Workspaces takes content from Oracle Real-Time Collaboration and makes this information persistently available to members of a project team within the context of the project.

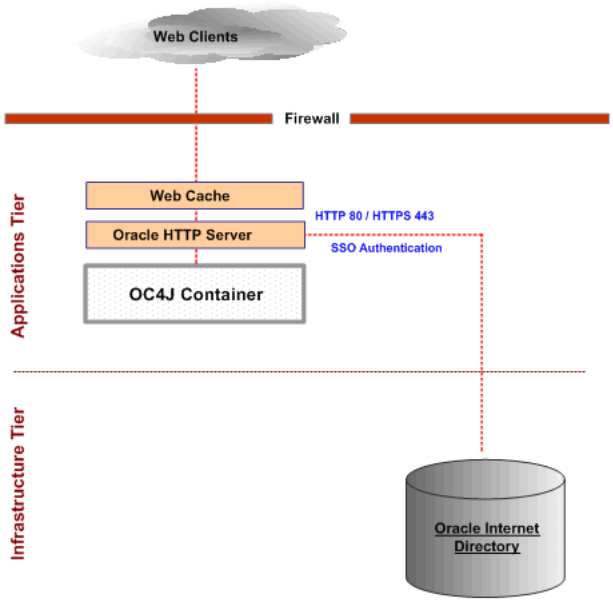
Oracle Workspaces Functionality

Oracle Workspaces is built upon other Oracle Collaboration Suite applications including Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, and Oracle Real-Time Collaboration. If some of these applications are not deployed with Oracle Workspaces, then it still functions properly but the content type supported by those applications is not available through Oracle Workspaces.

User Verification and Authentication

Web browser clients send an HTTP request to the Web cache which forwards the request to Oracle HTTP Server. Oracle HTTP Server performs single sign-on authentication against Oracle Internet Directory and then forwards the request to the OC4J container that contains the Oracle Workspaces Web application logic and server.

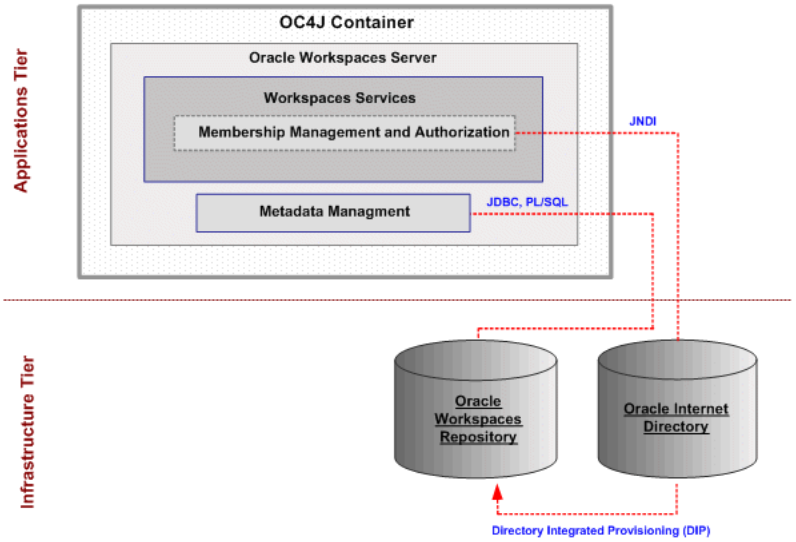
Figure 13–2 Oracle Workspaces User Verification and Authentication



Membership Management and Authorization

The membership management and authorization service connects to Oracle Internet Directory using JNDI. It then provisions the Oracle Workspaces repository with members and membership roles using the Directory Integrated Provisioning.

Figure 13–3 Oracle Workspaces Membership Management and Authorization

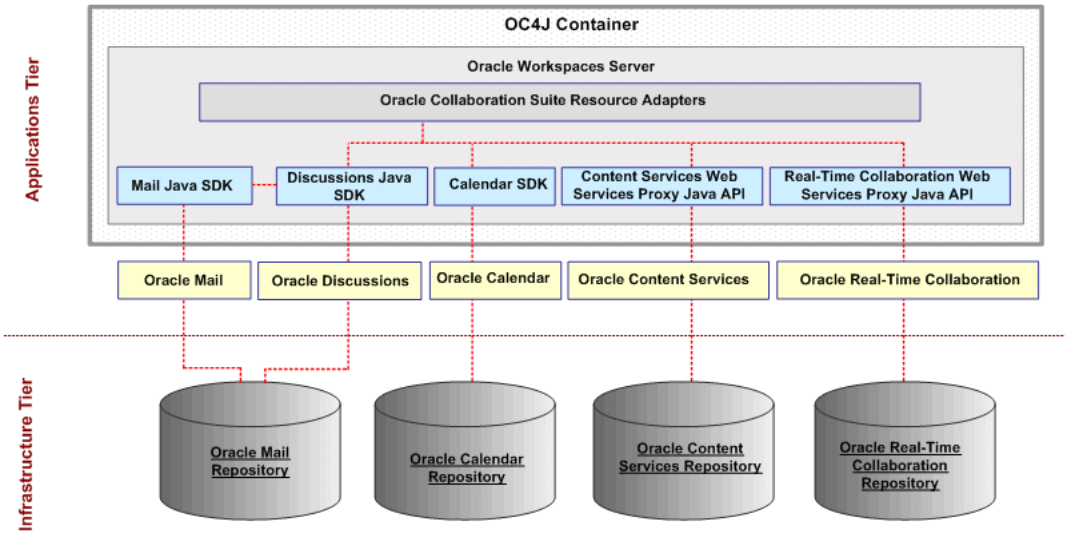


Interaction with Other Oracle Collaboration Suite Applications

The Oracle Collaboration Suite resource adapters present data from Oracle Collaboration Suite application through Oracle Workspaces in addition to the native application interfaces. Each Oracle Collaboration Suite resource adapter has a

corresponding JAVA API that can be programmed to manipulate target application data to appear within the Oracle Workspaces user interface. The Oracle Mail and Oracle Discusssions applications share the same repository.

Figure 13–4 Oracle Workspaces Interaction with Oracle Collaboration Suite Applications



Planning for Oracle Workspaces Deployment

This section discusses Oracle Workspaces deployment planning issues. Oracle Workspaces provides system properties for controlling application sizing and performance.

Sizing and Performance Tuning

Oracle Workspaces provides system properties to control application sizing and performance tuning. For information on configuring these properties, see *Oracle Collaboration Suite Administrator's Guide*.

Oracle Workspaces Deployment Configurations

This section discusses Oracle Workspaces deployment configurations.

Multiple Computer Configurations

Oracle Workspaces supports all of the multiple computer deployment configurations supported by Oracle Collaboration Suite. Oracle Workspaces need no additional configuration to support any of the Oracle Collaboration Suite multiple computer configurations.

> **See Also:** For information regarding all Oracle Collaboration Suite deployment configurations, see Chapter 3, "Deploying Oracle Collaboration Suite".

Multiple OC4J Deployment Cache Issues

Oracle Workspaces caches some information in-memory, and when deployed in a multiple OC4J Containers scenario, each container has its own cache. As a result, a user accessing Workspaces from one OC4J Container may not immediately see changes made by a user accessing Workspaces from another OC4J Container.

Figure 13–5 Cache Update Delay in an Oracle Workspaces Multiple OC4J Deployment Scenario

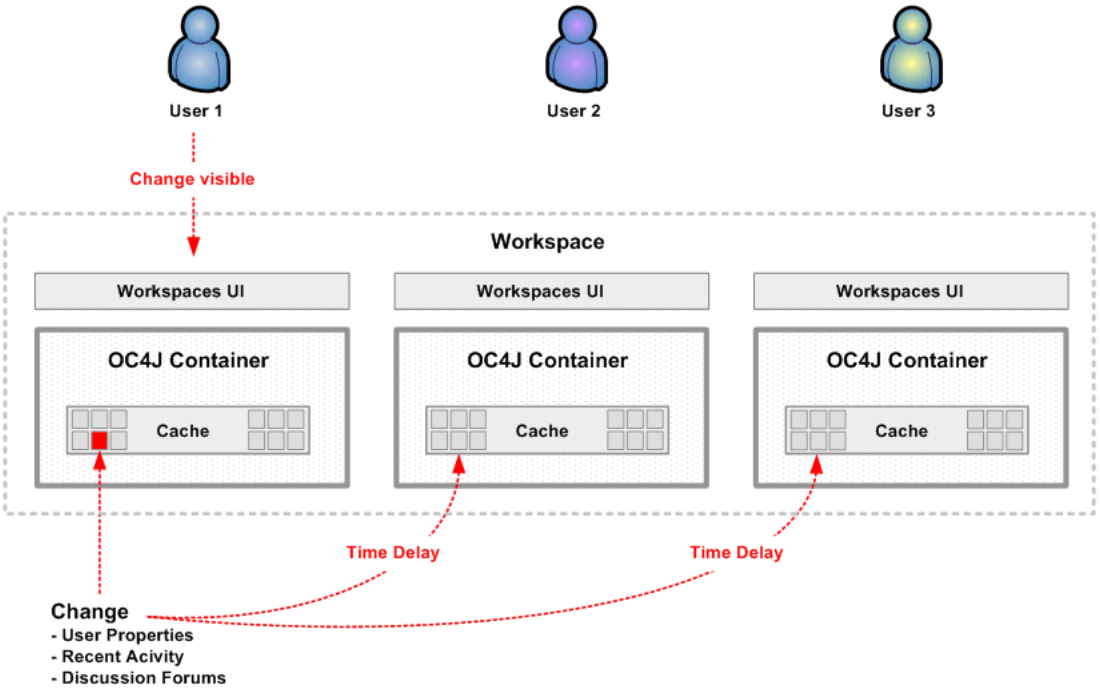


Figure 13–5 illustrates the results of cache update delays in an Oracle Workspaces multiple OC4J deployment scenario. In this figure the Oracle Workspaces user interface can be accessed by one of three OC4J containers. Data changes in one of the OC4J containers to either user properties, recent activity, or discussion forums, however this change is not immediately updated in the other two OC4J containers. As a result, a user accessing the workspaces user interface from the OC4J in which the change has occurred can see the change. Users accessing the workspace user interface from the other OC4J containers do not see the change until the update occurs.The expected delay times for different types of data are described as follows.

User Properties

User properties are cached in memory for thirty minutes. If user properties are updated in Oracle Internet Directory, then provisioning is used to propagate those changes to the workspaces repository. The changes may not be reflected in the workspaces application for up to 30 minutes due to the in-memory caching, and may be reflected in one OC4J Container before they are reflected in a different OC4J Container.

Recent Activity

Recent activity is shown when you enter a workspace on the workspace home page. This data is cached in memory for thirty minutes, but with some additional rules. Any

time an operation occurs which modifies workspace content, the cache is invalidated (so that changes made in the same OC4J Container appear instantly). Note that changes made in a different OC4J Container do not cause the cache to be invalidated. For this reason, a conditional TTL (time to live) is also used in the cache. If a cached item is more than five minutes old, then a check is made to see whether any item in the workspace was updated since the item was placed in the cache. This check uses data stored in the database, and so will capture any changes that occurred in different OC4J Containers. This means that it will take at most five minutes for changes from one OC4J Container to be seen in another OC4J Container.

Discussion Forums

The list of discussion forums is also cached in memory for each workspace. The caching scheme used is identical to that used for recent activity, so any changes made in one OC4J Container will take at most five minutes to propagate to other OC4J Containers.

Adding Oracle Collaboration Suite Applications to Oracle Workspaces as Required

If Oracle Workspaces is initially installed without a particular service such as Oracle Calendar, Oracle Content Services, Oracle Discusssions, Oracle Mail, and Oracle Real-Time Collaboration, then the service can easily be added later and subsequently can be used by existing workspaces.

Figure 13–6 Adding Features to Oracle Workspaces as Required

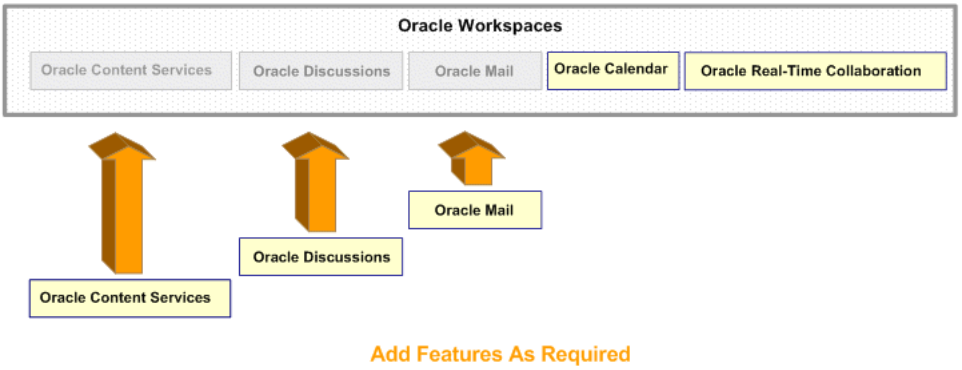


Figure 13–6 illustrates how new services can be added to Oracle Workspaces. In this figure Oracle Calendar, and are already up and running as Oracle Workspaces features. These features are illustrated as yellow boxes inside Oracle Workspaces. Oracle Content Services, Oracle Mail, and Oracle Discusssions are illustrated as grayed out boxes in Oracle Workspaces to indicate that they are inactive features. Yellow-box versions of these features are indicated later the Oracle Workspaces application with arrows pointing toward the grayed out version of these features in Oracle Workspaces. This indicates that the features will be added to Oracle Workspaces. New features can be integrated as follows.

Reinitialize only that Feature

After verifying that the newly-installed feature is up and running, an application administrator can access the Administration tab, then the Services subtab, and reinitialize only the newly-installed feature. Reinitializing the newly-installed feature will establish or re-establish a connection with the service so that it can be used in by

Oracle Workspaces. The workspaces server remains up and functional throughout this process.

Bounce the OC4J Container

An alternative to reinitializing the newly installed service is to take down the OC4J Container which contains the workspaces application and bring back up. The same initialization steps occur as the ones that take place when reinitializing the feature.

Glossary

Applications tier

The tier of Oracle Collaboration Suite that runs the server applications that provide specific functionality to end users. The term "Applications tier" replaces the term "middle tier" that was used in previous releases. Each Applications tier corresponds to an instance of Oracle Application Server. See also Oracle Collaboration Suite Applications

availability

Availability is the percentage or amount of scheduled time that a computing system provides application service.

Client tier

The tier of Oracle Collaboration Suite that consists of the end-user applications that reside on client devices, such as desktops, laptops, wireless phones, and PDAs. See also Oracle Collaboration Suite Applications.

Calendar daemons/ services

Six UNIX daemons or multi-threaded Windows services:

- Oracle Calendar Lock Manager (`unilckd`)
- Oracle Calendar Engine (`uniengd`)
- Oracle Calendar Synchronous Network Connections (`unisncd`)
- Oracle Calendar Corporate-Wide Services (`unicwsd`)
- Oracle Calendar Server Manager (`unicsmd`)
- Oracle Calendar Directory Access Server (`unidasd`) - external directory only

directory server

A directory server defines a hierarchical view of an organization's employees, units, and other resources.You can protect applications using directory servers by limiting access to the virtual paths of the applications to particular branches in the directory server.

DMZ

The demilitarized zone (DMZ) is the area between outer and inner firewalls. It is normally used to protect the internal application servers from being attacked by those attempting to gain unauthorized access to a network or intranet.

failover

Failover is the ability to reconfigure a computing system to utilize an alternate active component when a similar component fails.

firewall

A firewall is a machine that acts as an intermediary to protect a set of computers or networks from outside attack. It regulates access to computers on a local area network from outside, and regulates access to outside computers from within the local area network. A firewall can work either by acting as a proxy server that forwards requests so that the requests behave as though they were issued by the firewall machine, or by examining requests and attempting to eliminate suspect calls

host

A host is a computer with a unique domain name.

HTTP

Hypertext Transfer Protocol (HTTP) is the underlying format used by the Web to format and transmit messages and determine what actions Web servers and browsers should take in response to various commands. HTTP is the protocol used between Oracle Application Server and clients.

HTTP server

An HTTP server is a server that receives HTTP requests from remote browsers, converts the requested URL to a filename, and returns the file to the requester.

HTTPS (secure HTTP)

HTTPS is a version of HTTP with provisions for secure data transmission.

Hypertext Transfer Protocol

See **HTTP**.

Infrastructure tier

The tier of Oracle Collaboration Suite that consists of the components that provide services, such as identity management and metadata storage, for the Applications tier. Components of the Infrastructure tier include **Oracle Collaboration Suite Database** and Oracle Identity Management. See also **Oracle Collaboration Suite Infrastructure**.

IMAP4

Internet Message Access Protocol is an Internet protocol for accessing e-mail on a remote server from a local client. It enables efficient operation such as downloading only essential data by first getting the e-mail header before the actual e-mail download. This makes the protocol well suited to remote environments.

LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol that enables clients to access information from a directory server. This protocol enables corporate directory entries to be arranged in a hierarchical structure that reflects geographic and organizational boundaries.

Lightweight Directory Access Protocol

See LDAP.

computer

See host.

OC4J

Oracle Application Server Containers for J2EE (OC4J) is a complete set of J2EE containers written entirely in Java that execute on the Java Virtual Machine (JVM) of the standard Java Development Kit (JDK).

OID

See Oracle Internet Directory.

OJMA

The Oracle Java Mail API (OJMA)

Oracle Application Server Metadata Repository

Oracle Application Server Metadata Repository is a pre-seeded database containing metadata required by Oracle Application Server instances.

Oracle Collaboration Suite Applications

The applications that comprise Oracle Collaboration Suite.

Oracle Collaboration Suite

An integrated suite of software applications to enable communication, messaging, and content sharing in an enterprise environment. At an architectural level, it includes three tiers: an Applications tier, which consists of server applications that provide the basic functionality, a Client tier, which consists of applications on desktops, laptops, and wireless devices, and an Infrastructure tier, which provides centralized services, such as identity management and metadata storage, for the applications.

Oracle Collaboration Suite Applications

The applications that make up Oracle Collaboration Suite, namely:

- Oracle Calendar
- Oracle Content Services
- Oracle Discusssions
- Oracle Mail
- Oracle Mobile Collaboration
- Oracle Real-Time Collaboration
- Oracle Collaboration Suite Search
- Oracle Workspaces

Each of the preceding applications is a component of Oracle Collaboration Suite Applications. These applications rely on the services provided by the Infrastructure tier. See also Applications tier.

Oracle Collaboration Suite Database

The default database included with Oracle Collaboration Suite to hold application data and metadata. The Oracle Collaboration Suite Database is part of the Oracle Collaboration Suite Infrastructure.

Oracle Collaboration Suite Infrastructure

The underlying components that support Oracle Collaboration Suite and provide centralized product metadata and security services, configuration information, and data repositories for Oracle Collaboration Suite Applications. Oracle Collaboration Suite Infrastructure uses and builds on OracleAS Infrastructure. It includes the Oracle Collaboration Suite Database and Oracle Identity Management. See also Infrastructure tier.

Oracle HTTP Server

Oracle HTTP Server is the Web server that Oracle Application Server uses, which is built on Apache Web server technology. Oracle HTTP Server offers scalability, stability, speed, and extensibility. It also supports Java servlets, JavaServer Pages (JSPs), Perl, PL/SQL, and CGI applications.

Oracle Identity Management

An integrated set of components that provide distributed security to Oracle products and make it possible to centrally and securely manage enterprise identities and their access to applications in the enterprise. It includes the following components: Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, OracleAS Single Sign-On, and Oracle Application Server Certificate Authority.

Oracle Internet Directory

Oracle Internet Directory (OID) is a general purpose directory service that enables retrieval of information about dispersed users and network resources. Oracle Internet Directory combines LDAP version 3 with the high performance, scalability, robustness, and availability of the Oracle database.

Oracle Internet Directory runs as an application in the Oracle database. It communicates with the database, which may be on the same or a different operating system.

Oracle Real-Time Collaboration Multiplexer (MX)

Accepts inbound connections from Oracle Web Conferencing clients and Oracle Web Conferencing Servers and routes data traffic between them. Acts as a communication hub for Web conferencing components.

Oracle Real-Time Collaboration Redirector

Redirects the accepted connections to the Oracle Real-Time Collaboration communication processes (the Real-Time Collaboration Multiplexer for Web conferences or the Client Connection Manager for chat sessions) and load balances between them.

Oracle Real-Time Collaboration Server

The Oracle Real-Time Collaboration Server consists of the following:

Oracle Real-Time Collaboration Communication Services – Services that enable system communications such as Secure Sockets-Layer (SSL) connections, firewall traversal, and multiplexer processing of multiple conference connections.

Oracle Real-Time Collaboration Data Services – Services that support the transfer of Oracle Web Conferencing and chat data.

Oracle Real-Time Collaboration Group Services – Services that let multiple users interact with a group of contacts, and members of the group interact with each other.

Oracle Real-Time Collaboration Integration Services – A set of interfaces that can be used to tightly integrate any application to the functionality provided by the Oracle Real-Time Collaboration system. Integrators can create applications customized for the entire enterprise or for any business application (for example sales, training, customer support) within the enterprise.

Oracle Real-Time Collaboration Presence Server – A server that supports the declaration and detection of individual and group presence.

Oracle Real-Time Collaboration System Services – Services that provide administrative features such as system management through properties, statistics reporting, and process monitoring.

Oracle Real-Time Collaboration Voice Services – Services that enable voice streaming in Web or chat conferences, full-duplex voiceover IP (VoIP), and pass-the-mic voice streaming.

Oracle Real-Time Collaboration Web Client – A Web-based user interface that lets users and administrators download Oracle Web Conferencing and Oracle Messenger clients, schedule and join conferences, manage conference materials, view and manage conference and message archives and reports, and monitor the Oracle Real-Time Collaboration system.

Oracle Real-Time Collaboration Web Conferencing Server – Backend server that enables real-time Web conferencing, including intelligently distributing real-time data, managing conference attendees' states, and providing services for recording and archiving conferences. Clients never directly communicate with the Web Conferencing Server. Instead, clients communicate with the HTTP Listener, which uses mod_meeting to communicate with the appropriate Web Conferencing Server.

PBX

Private branch exchange, a private telephone network within an enterprise. Users of the PBX share a number of lines for making telephone calls external to the PBX. The PBX enables switching of multiple incoming and outgoing lines between multiple internal phones.

POP3

Post Office Protocol 3 is a standard protocol used by a client to receive e-mail that has been sent to the client over the Internet. The protocol is used to retrieve the client's e-mail from the server.

POP3 is the most recent version of this protocol and is typically included in software e-mail applications such as Outlook Express; it is also built into popular browsers, for example, Microsoft Explorer and Netscape. POP3 is usually employed with SMTP. IMAP is the alternative protocol to POP3, with more features for handling the e-mail on the server.

Port

A port is a number that TCP uses to route transmitted data to and from a particular program.

private branch exchange

See PBX.

Proxy Server

A proxy server typically sits on a network firewall and enables clients behind the firewall to access Web resources. All requests from clients go to the proxy server rather

than directly to the destination server. The proxy server forwards the request to the destination server and passes the received information back to the client. The proxy server channels all Web traffic at a site through a single, secure port; this enables an organization to create a secure firewall by preventing Internet access to internal machines, while allowing Web access.

RAC

Real Application Clusters (RAC) is a parallel database clustering technology from Oracle. RAC is an active-active cluster with shared storage, whereby multiple servers can work in parallel on the same set of data.

Real Application Clusters

See RAC

Scalability

Scalability is the ability to handle increasing numbers of hardware requests without adversely affecting latency and throughput.

Schema

A schema is a collection of database objects, including logical structures such as tables, views, sequences, stored procedures, synonyms, indexes, clusters, and database links.

A schema has the name of the user who controls it.

SMTP

Simple Mail Transfer Protocol is the main protocol used to control the transfer of electronic mail (e-mail) messages on the Internet. SMTP is the TCP/IP protocol, and this specifies the format of the messages, and how servers and terminals are to interact.

SMTP is usually employed for the sending of the messages, with other protocols used to receive them, for example, POP3 or IMAP, which can save the messages in a mailbox for download from the server to a particular terminal, as required by the user. ESMTP, Extended Simple Mail Transfer Protocol, enables multimedia files to be sent as e-mail.

Telephony Server

Intel NetMerge Converged Communications Software (CCS) and the Oracle Container comprise the Telephony Server. The Telephony Server is a resource manager for the Voicemail & Fax Application services. Calls from the PBX are handed off to the Telephony Server which then hands off the call to the appropriate Oracle Voicemail & Fax service.

VoIP

A category of hardware and software that uses the Internet as the transmission medium for telephone calls. Voice data is sent in digital form in packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it eliminates ordinary toll charges.

source: http://www.google.com/search?hl=en&lr=&oi=defmore&q=define:VoIP

Index

I

L

M

N

O

P

R

S

T

U

V

W