Oracle® Collaboration Suite

Deployment

Release 2 (9.0.4)

Part No. B15606-01

November 2004

ORACLE®

Oracle Collaboration Suite Deployment, Release 2 (9.0.4)

Part No. B15606-01

Primary Author: David Wood

Contributors: M. Brown, K Burridge, K. deSmidt, C. G. Doherty, M. Kavanaugh, Richard Hall, Tait McCarthy, Valarie Rosamond Moore, S. Sharma, U. Srinivasan, R. Sunkara, Lyju Vadassery

Contents

4 Oracle Collaboration Suite Deployment Examples

Index

List of Figures

Send Us Your Comments

Oracle Collaboration Suite Deployment, Release 2 (9.0.4)

Part No. B15606-01

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

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

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

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

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

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

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

Preface

This preface contains the following topics:

Intended Audience

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 Release 2 (9.0.4)* and before *Oracle Collaboration Suite Pre-installation Requirements Release 2 (9.0.4)*.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Structure

This manual contains four chapters.

Chapter 1, "Introduction to Oracle Collaboration Suite Deployment"

This chapter provides an overview of Oracle Collaboration Suite and describes how to use this guide.

Chapter 2, "Oracle Collaboration Suite Network Planning"

This chapter provides an overview of Oracle Collaboration Suite network services and components, and describes strategies and questions to consider when planning your network.

Chapter 3, "Oracle Collaboration Suite Architecture Planning"

This chapter provides an overview of Oracle Collaboration Suite architectures, and describes strategies and questions to consider when planning your architecture.

Chapter 4, "Oracle Collaboration Suite Deployment Examples"

This chapter describes several real-life examples of Oracle Collaboration Suite deployments.

Related Documents

For more information, see the following manuals in the Oracle Collaboration Suite documentation set:

- *Oracle Collaboration Suite Concepts Release 2 (9.0.4)*
- *Oracle Collaboration Suite Sizing and Performance Tuning Release 2 (9.0.4)*
- *Oracle Collaboration Suite SSL Configuration Release 2 (9.0.4)*
- *Oracle Collaboration Suite High Availability Configuration Release 2 (9.0.4)*
- *Oracle Collaboration Suite Backup and Recovery Release 2 (9.0.4)*
- *Oracle Email Anti-Spam Configuration Release 2 (9.0.4)*
- *Oracle Collaboration Suite Pre-installation Requirements Release 2 (9.0.4)*
- *Oracle Collaboration Suite Installation and Configuration Guide Release 2 (9.0.4.1)*

Conventions

The following conventions are also used in this manual:

Convention	Meaning
. . .	Vertical ellipsis points in an example mean that information not directly related to the example has been omitted.

Convention	Meaning
. . .	Horizontal ellipsis points in statements or commands mean that parts of the statement or command not directly related to the example have been omitted
boldface text	Boldface type in text indicates a term defined in the text, the glossary, or in both locations.
< >	Angle brackets enclose user-supplied names.
[ ]	Brackets enclose optional clauses from which you can choose one or none.

1

Introduction to Oracle Collaboration Suite Deployment

This chapter provides an overview of Oracle Collaboration Suite and describes how to use this guide. This chapter contains the following topics:

What Is Oracle Collaboration Suite?

Oracle Collaboration Suite is a set of integrated software components that provide communication and collaboration services. These components are based on Oracle9*i* Application Server and Oracle9*i* Database. With Oracle Collaboration Suite, users can exchange e-mail, voice mail and faxes. They can also organize appointments, share documents, and arrange, track, and conduct online meetings. Users can access these services through the Web or wireless networks, by telephone or fax, or with client applications such as Microsoft Outlook.

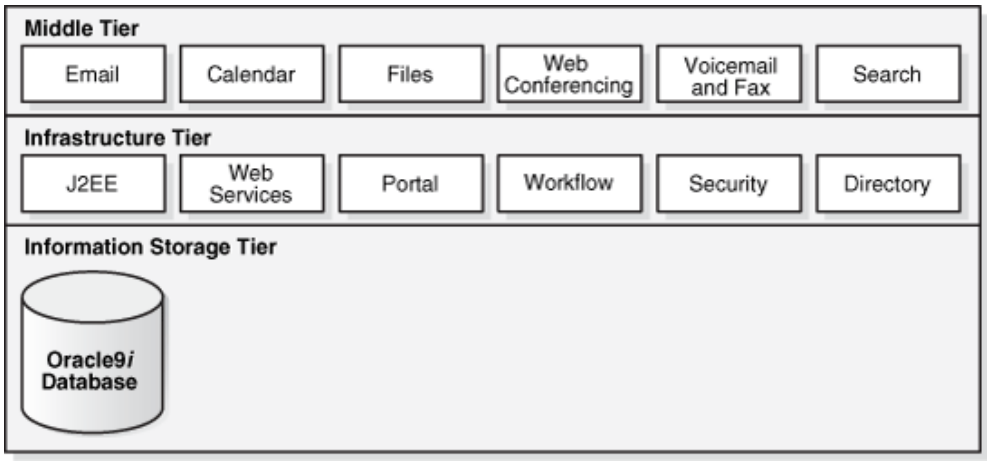
The following figure provides a conceptual view of the components that constitute Oracle Collaboration Suite and the services they provide.

Figure 1–1 Oracle Collaboration Suite components and services

What Are the Elements of Oracle Collaboration Suite?

At a high level, Oracle Collaboration Suite can be divided into three tiers. There are different options for deploying the components that constitute these tiers. The following figure provides a high-level view of the components of these three tiers.

Figure 1–2 The three tiers of Oracle Collaboration Suite



The three tiers and their components are summarized in the following sections:

- Oracle Collaboration Suite Information Storage Tier
- Oracle Collaboration Suite Infrastructure Tier
- Oracle Collaboration Suite Middle Tier

Oracle Collaboration Suite Information Storage Tier

The information storage tier is based on Oracle9*i* Database. It consists of the Oracle Files and Oracle Email database, and can be deployed with Oracle9*i* Real Application Clusters.

Oracle Collaboration Suite Infrastructure Tier

The infrastructure tier is built on Oracle9*i* Application Server. It consists of a common set of services, such as security, directory, and portal services. These services are used by Oracle Collaboration Suite applications.

Oracle Collaboration Suite Middle Tier

The middle tier consists of Oracle Email, Oracle Files, Oracle Calendar, Oracle Voicemail and Fax, Oracle Web Conferencing and Oracle UltraSearch. Users interact with Oracle Collaboration Suite by using these applications, which can be accessed through a wide variety of communications media.

How Should I Use this Guide?

The network setup and architecture you choose for Oracle Collaboration Suite determine the degree of availability, security, scalability and performance of the product. To ensure that Collaboration Suite provides service reliably and efficiently, you must plan these elements carefully in order to optimize your system.

Use this guide to plan your network and architecture before you start installing Oracle Collaboration Suite. The next two chapters in this book, Oracle Collaboration Suite Network Planning and Oracle Collaboration Suite Architecture Planning, describe how to set up and plan your network and architecture, and how to leverage existing elements that might be available. Both chapters also include a list of questions you should ask when evaluating your needs. Chapter 4, "Oracle Collaboration Suite Deployment Examples", includes real-world examples of Collaboration Suite deployments, upon which you can model your own deployment.

2

Oracle Collaboration Suite Network Planning

This chapter provides an overview of Oracle Collaboration Suite network services and components, and describes strategies and questions to consider when planning your network. This chapter contains the following topics:

Introduction to Oracle Collaboration Suite Network Planning

When planning your network, you want to take advantage of Oracle Collaboration Suite's features while making the most out of your existing network services and components. You must determine factors such as how much access you want to allow from external sources, how much capacity is required to meet the needs of your users, how available you need your network to be, what your budget allows and what your business reasons are for setting these goals.

You should also be ready to contemplate how much (or how little) you are willing to change in your network, and whether or not you have the mandate or flexibility to update business processes if necessary.

In smaller deployments of Oracle Collaboration Suite, network and architectural planning become intertwined. This is because the smaller the pool of available servers, the fewer options there are for deployment. When you are planning an architecture with only one or two servers, there will often be a trade-off between component accessibility and location of servers. Security demands often dictate where certain servers must reside, and access to these servers must be planned accordingly. This can easily be done with the proper use of network services.

Oracle Collaboration Suite Access and Security

Access and security are two characteristics of Oracle Collaboration Suite that must be planned simultaneously, because they directly affect one another. This is especially true in 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 access methods depend on the user's location when attempting to

access the network, whether or not a thick or thin client is used and the component to which the user is attempting to connect.

Because access is such a 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 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 in a Typical Installation of Oracle Collaboration Suite

A typical installation of Oracle Collaboration Suite separates 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 Web Conferencing, the Oracle Calendar Web client, Oracle Files and the Oracle Calendar desktop clients.

External Traffic

Externally, only a few encrypted, hardened and monitored services are exposed. HTTPS and SMTP are the only services typically available from the outside world, and these may be proxied accordingly.

Users who access Oracle Collaboration Suite from outside are generally relegated to the Oracle Calendar Web client and Oracle Web Mail over HTTPS.

SMTP is proxied though a mail relay and accepts e-mails from the outside world.

General Network Considerations for Oracle Collaboration Suite

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 Email 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 reverse proxy, DNS and mail relay.

- **Where should these be accessible from?**

  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 DMZs or external access to e-mail.

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

  It is 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 4, "Oracle Collaboration Suite Deployment Examples" 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

Questions to Ask about an Existing Network Before Deploying Oracle Collaboration Suite

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 Web Conferencing to be available through the Internet?
- What services might your organization want to deploy for the first time, or upgrade?

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 services need to be protected with SSL. If the answer to this is yes, 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.

If there is a DMZ:

- How is it used for external access?
- How is it used for internal access?
- Are DNS (Domain Name Server) servers used? If so, consider the following issues.
  - Often, two DNS servers ("split DNS") are used, which helps separate internal from external traffic. This makes internal traffic more secure. Internal traffic might include access to printers or other material not to be made public.
  - DNS servers can be separated onto separate networks; for example, one in the DMZ and one in the internal network.
  - 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 NAT.

  Having two DNS servers is more secure 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?

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 middle 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:

Split DNS

Split DNS means that there is more than one naming service for a domain; generally one for inside the organization and one for outside. In Oracle Collaboration Suite, HTTP services are very domain-name specific, and in fact are mostly accessed through Single Sign-On. Oracle Collaboration Suite can only answer on one host name / domain name, so it is convenient to be able to map this to internal or external IPs as needed.

Ideally, you can have the same Oracle Collaboration Suite installation serving both internal and external requests. However, you don't necessarily want internal users having to access the instance from outside. Therefore, you use NAT with the Oracle Collaboration Suite servers so that:

- Internal, non-routable addresses are mapped to external routable addresses.
- Internal addresses are mapped to other internal addresses, if necessary.

You should configure the respective DNS servers to return the appropriate IP addresses for NAT, depending on whether the requests originate internally or externally.

Split DNS configurations are common and should be anticipated when designing the virtual host names for services prior to installation.

Single DNS

Configuring a single DNS instance is more difficult. Requests for 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?

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 middle 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 MX records (to map domain names to mail servers) early.

Does your organization use hardware encryption acceleration?

If you are planning on using the Secure Sockets Layer (SSL) protocol to encrypt communications, it is an excellent idea to make use of SSL accelerators to optimize performance. SSL processing is a CPU-intensive task that can greatly reduce CPU 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?

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, including:

- **Use of milters**: If a milter is installed, you may have to configure a server-side rule to remove flagged spam. If so, this may impact the server configuration and tuning process. Alternatively, you can use a third-party service to catch and delete spam. You should also evaluate whether there will be other input that you will have to accommodate. Ideally, you want to remove spam before it reaches the relay. The open source Postfix mail relay has a built-in spam tagger.
- **Server-side configuration**: Like virtually any network traffic filtering, mail filtering can be configured directly on the server. Make sure you account for anything else that this configuration needs to be integrated with.

Will your organization want Web Conferencing to be available through the Internet?

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

If Web Conferencing cannot be installed on its own server, the Web Conferencing server must still be available directly to clients, and not put behind a proxy server, for example (although NAT is supported). Web Conferencing clients first attempt to connect directly to the Web Conferencing servers, and then attempt to connect directly to the Oracle HTTP Server. Oracle HTTP Server and Oracle Web Cache cannot share the same IP address/port combination, so an organization may choose to deploy a second IP address for Web Conferencing traffic (also on ports 80/443).

Another issue to consider is how to manage using Web Cache and Web conferencing on the same middle tier. This is further addressed in Chapter 3, "Oracle Collaboration Suite Architecture Planning".

What services might your organization want to deploy for the first time, or upgrade?

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 reverse proxy, for example), or upgrade existing services (such as a mail relay).

3

Oracle Collaboration Suite Architecture Planning

This chapter provides an overview of Oracle Collaboration Suite architectures, and describes strategies and questions to consider when planning your architecture. This chapter contains the following topics:

Introduction to 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 Email, and not for Calendar, Files and other components, can save an organization a lot of time and money.

Planning for Oracle Collaboration Suite Workload and Security

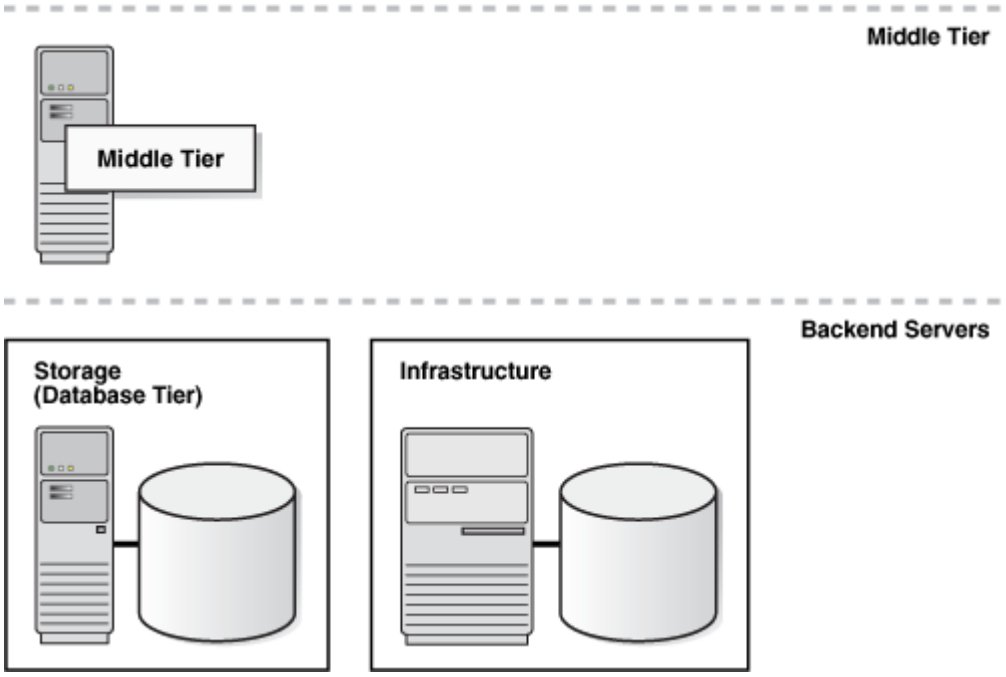
You can deploy all three tiers of Oracle Collaboration Suite on a single node. However, such a deployment architecture may not be able to meet all the availability, security, and scalability requirements of your organization. Distribution of the tiers on multiple nodes makes it easier to meet these requirements.

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

The three Oracle Collaboration Suite tiers handle different types of workloads. The middle tier is CPU-intensive and memory-intensive with few disk I/O operations. The infrastructure and information storage tiers are disk I/O intensive. The information storage tier disk I/O consists of comparable numbers of read and write operations, and the infrastructure tier disk I/O consists of more read operations than write operations.

In Oracle Collaboration Suite, the demand for middle 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 the need for a distributed architecture. With a distributed architecture, you can scale up the information storage tier and middle tier independently. The following figure displays the information storage tier and middle tier on different nodes.

Figure 3–1 Oracle Collaboration Suite Tiers and Nodes



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. It must also provide protection against known security threats, such as Denial of Service (DoS) attacks and viruses.

Planning for Oracle Collaboration Suite 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.

Consult the document *Oracle Collaboration Suite Sizing and Performance Tuning Release 2 (9.0.4)* for information on memory and server needs, and see the section in this document, "Planning for Oracle Collaboration Suite Scalability", for information on planning for future expansion of your network architecture.

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.

Middle 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 nodes with larger memory requirements.

Properly deployed middle tier systems can serve as backups to each other. This style of "duplicated" middle tiers provides flexibility of deployment and allows the load to be spread across all the middle tier systems as the load swings from, for example, e-mail to Oracle Files access through the day.

Planning for Oracle Collaboration Suite Access

As described in Chapter 2, "Oracle Collaboration Suite Network Planning", 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 middle 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 Single Sign-On. More often though, one set of middle 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.

Planning for Oracle Collaboration Suite 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 allows for growth and memory expansion. See "Planning for Oracle Collaboration Suite Capacity" for more information.

Planning for Oracle Collaboration Suite High Availability

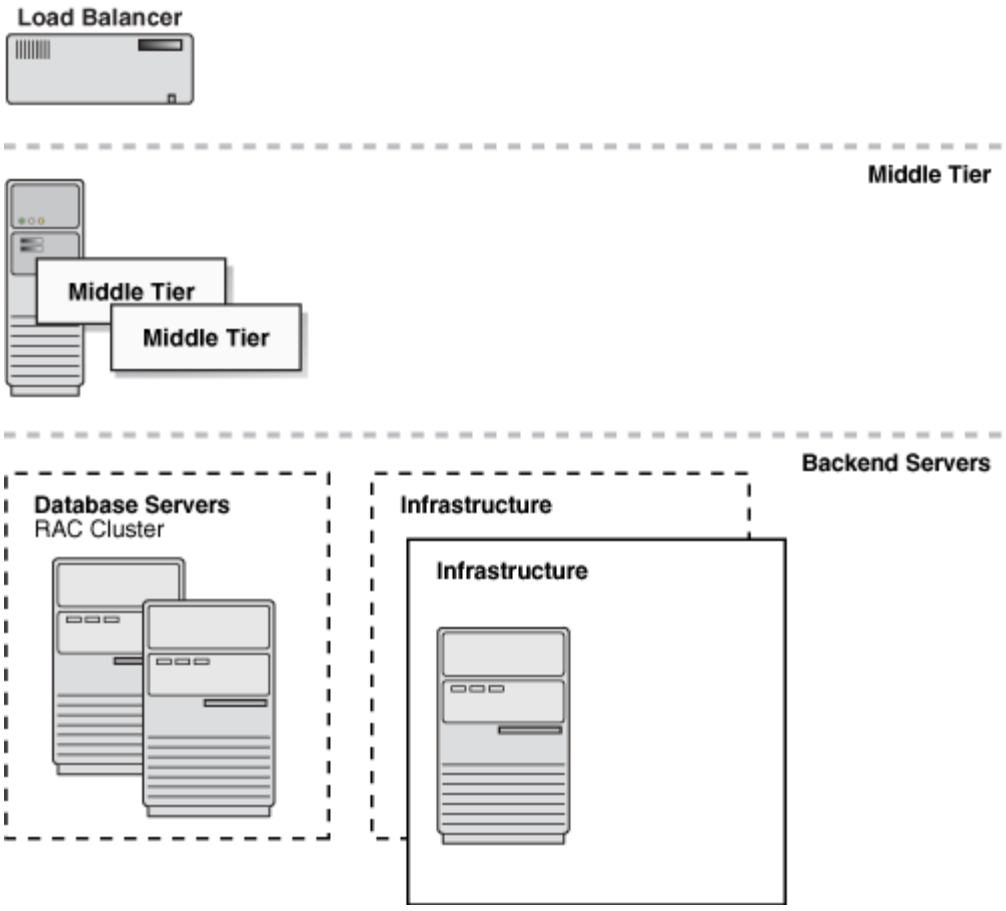
The term "high availability" refers to the capability of a network to keep running should a component or application fail. This is especially important for a core

communication tool such as e-mail, or a real-time communication tool such as Web Conferencing.

Distribution of middle tiers over multiple nodes does not ensure high availability. All the tiers of the system must be available in order to provide continuous access to services such as e-mail and voice mail. To provide continuous access to services, you must replicate components of the system and implement failover mechanisms for redirecting users from failed components to working components.

In the following figure, the three tiers of Oracle Collaboration Suite are distributed and replicated.

Figure 3–2 Distributed and Replicated Tiers in Oracle Collaboration Suite



Availability is maximized when you duplicate and replicate all the tiers of Oracle Collaboration Suite. Load balancing is used to handle failure in the middle tier. Oracle9*i* Real Application Clusters is used to handle failure in the information storage tier. A cold standby server is used as a failover measure for the infrastructure tier.

Oracle Collaboration Suite 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.

Oracle Collaboration Suite Redundancy Strategies

Network redundancy encompasses strategies you put into place to keep things running in the case of network failure. Strategies can range from performing basic backups in-house to maintaining high-level site mirroring. The latter is not possible yet with Oracle Collaboration Suite, so it is best to implement a thorough backup strategy.

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 you would like to restore first. Make sure you put in place an efficient failover plan for those components, using duplicated tiers or other backup strategies. If you feel that all components are essential, then you need a high level of redundancy.

Questions to Ask about Existing or Planned Oracle Collaboration Suite Architectures

This section provides the following detailed questions you should ask about an existing or planned architecture in which you want to deploy Oracle Collaboration Suite.

- 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?

Use the document "Oracle Collaboration Suite Sizing and Performance Tuning Release 2 (9.0.4)" to determine how many servers you will need for your deployment.

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.

What type of platform is your organization comfortable with?

Oracle Collaboration Suite supports AIX, Solaris, HP-Unix, Linux, Tru64 and Windows. The platform you choose can influence the hardware you can use. 64-bit servers are often used for databases, while 32-bit servers are often used for middle tiers. See "Planning for Oracle Collaboration Suite Capacity" for more details.

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 "Planning for Oracle Collaboration Suite Scalability". With this strategy, you can "grow" into a duplicated middle 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 using Oracle9*i* 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.

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 Email, Calendar and Files.

Does your organization have archiving needs?

Oracle Email allows 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.

Oracle Collaboration Suite Architecture Types

This section, and the rest of this chapter, describes and illustrates the various architecture types used with Oracle Collaboration Suite. You can refer to these illustrations when planning your own deployment, and should definitely also consult Chapter 4, "Oracle Collaboration Suite Deployment Examples" for "real-world" examples of working deployments.

This section contains the following topics:

- Comprehensive Oracle Collaboration Suite Duplicated Middle Tier Deployment

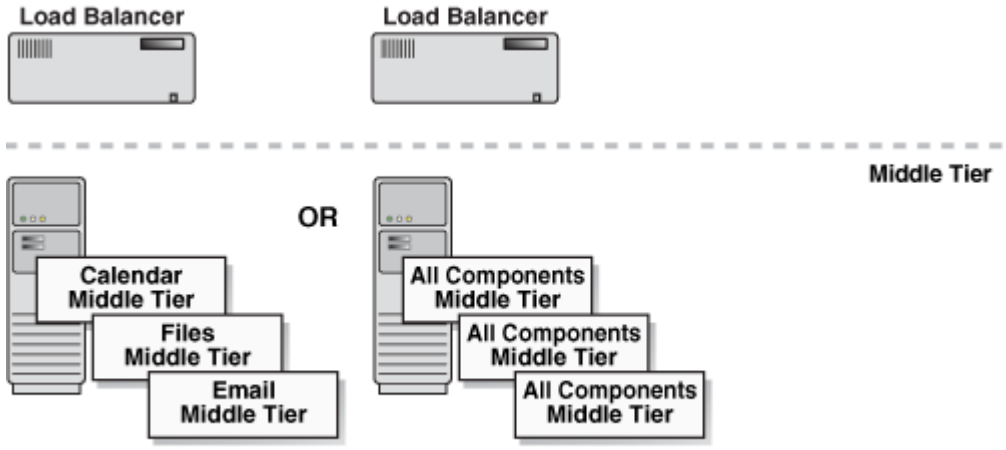
About Oracle Collaboration Suite Dedicated and Duplicated Middle Tiers

In Oracle Collaboration Suite, you can deploy dedicated middle tier nodes to handle specific applications, such as Oracle Email and Oracle Files. Alternatively, you can duplicate the middle tier nodes that run these applications. This form of duplication offers the following benefits:

- **Simplification of middle tier management**: This is because the requirements and processes for managing each duplicated node are the same.
- **Better use of middle tier resources**: This is because the demand for various applications varies with the time of day. For example, if peak e-mail usage is at the start of the day and peak file usage at all other times, then all the middle tier nodes can respond to this change in service requirements.

The following figure illustrates the difference between the dedicated tiers and duplicated tiers options.

Figure 3–3 Dedicated Tiers and Duplicated Tiers in Oracle Collaboration Suite



If you were using dedicated middle tier nodes, then at the start of the business day, Oracle Files nodes would be underused and Oracle Email nodes would struggle to cope with peak load.

However, if the system is evolving, then you may want to phase in components. For example, you can implement Oracle Email first, then implement Oracle Files, and later the Oracle Calendar server. In such cases, to reduce the impact on the earlier phases of implementation, it may be more appropriate to dedicate hardware to specific middle tier components.

Functionality of Oracle Collaboration Suite Tiers

This section describes the services and components of each of the three tiers of Oracle Collaboration Suite. This section contains the following topics:

- Oracle Collaboration Suite Middle Tier Functionality
- Oracle Collaboration Suite Infrastructure Functionality
- Oracle Collaboration Suite Information Storage Tier Functionality

Oracle Collaboration Suite Middle Tier Functionality

The middle tier provides the following services:

- E-mail protocols
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol, version 3 (POP3)
  - Internet Message Access Protocol, version 4 (IMAP4)
- File protocols
  - File Transfer Protocol (FTP)
  - Server Message Block (SMB)
  - Network File System (NFS)
  - AppleTalk Filing Protocol (AFP)
  - Web-based Distributed Authoring and Versioning (WebDAV)
- Web protocols
  - Hypertext Transfer Protocol (HTTP)
  - HTTP-Secure (HTTPS)
- E-mail services, including Webmail/HTTP
- File services, including Oracle Files/HTTP
- Calendar services
  - Webcal/HTTP
  - SyncML/HTTP
  - Oracle Calendar server
- Wireless services, including Wireless/HTTP
- Portal services, including Oracle9*i* Application Server Portal/HTTP
- Oracle UltraSearch services, including Oracle UltraSearch/HTTP
- Web Cache

Oracle Collaboration Suite Infrastructure Functionality

The infrastructure tier consists of the following components:

- Directory services
  - Lightweight Directory Access Protocol (LDAP)
  - Oracle Delegated Administration Services/HTTP
- Oracle9*i* Application Server Single Sign-On server, which provides single sign-on and HTTP services
- Infrastructure database, which contains Oracle Internet Directory, Oracle9*i*AS Single Sign-On, and Oracle9*i* Application Server Portal data

Oracle Collaboration Suite Information Storage Tier Functionality

The information storage tier contains the databases for the following components:

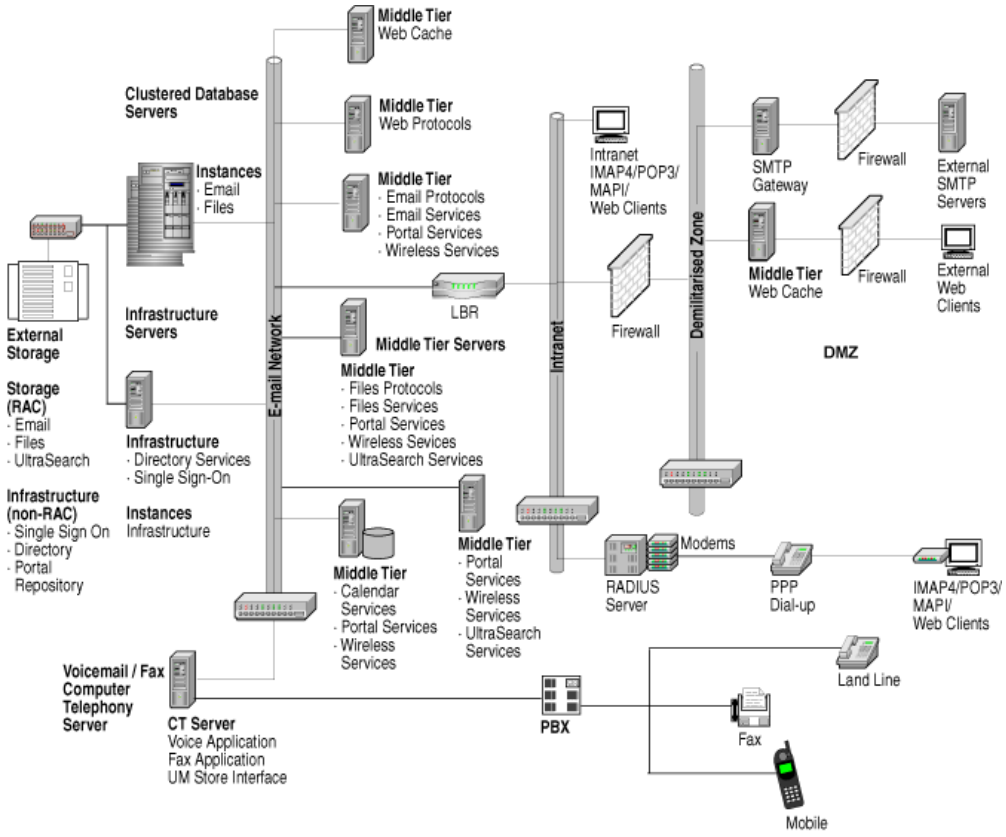
- Oracle Email

- Oracle Files
- Oracle UltraSearch

Illustration of Oracle Collaboration Suite Dedicated Middle Tiers

Figure 3–4 illustrates an implementation of dedicated middle tiers.

Figure 3–4 Oracle Collaboration Suite dedicated middle tiers



Details on this illustration are provided in the following topics:

- Physical Location of Oracle Collaboration Suite Dedicated Tier Components
- Oracle Collaboration Suite Dedicated Tier Workload
- Oracle Collaboration Suite Dedicated Tier Installation and Management
- Oracle Collaboration Suite Dedicated Tier Scalability
- Oracle Collaboration Suite Dedicated Tier Availability
- Oracle Collaboration Suite Dedicated Tier Cost

Physical Location of Oracle Collaboration Suite Dedicated Tier Components

In the Dedicated Tiers option, the middle tier, infrastructure tier, and information storage tier are installed on individual, dedicated nodes. On the middle tier, dedicated nodes handle requests for Oracle Email, Oracle Files, and the Oracle Calendar server services. On the database tier, dedicated nodes handle requests to access the Oracle Email, Oracle Files, and infrastructure databases.

Information storage is installed on each of two or more clustered nodes. It consists of both Oracle Files and Oracle Email instances, and databases that are configured to use Oracle9*i* Real Application Clusters that are placed on a shared disk.

In relatively large deployments, you can use individual instances of Oracle9*i* Real Application Clusters for the Oracle Files and Oracle Email databases. This feature helps separate the two databases in the event that one of them fails. The infrastructure is installed on a separate node. The infrastructure database is placed on a shared disk and accessed from a dedicated instance on this node. The middle tier is installed on several nodes, but only specific processes are started according to the role of each node.

If you replicate dedicated nodes to ensure availability, then you must implement hardware load balancing to distribute e-mail requests over multiple e-mail nodes, file access requests over multiple file nodes, and so on. The exceptions to this are Oracle Calendar server nodes, for which the load must be statically partitioned over multiple calendars.

Oracle Collaboration Suite Dedicated Tier Workload

One of the advantages of the Dedicated Tiers option is that all the workload types are separated and you can configure and tune the nodes according to the role they play in the system. This improves the performance of each node. However, a solution that is based on this deployment architecture option requires the use of an accurate sizing methodology and an in-depth understanding of the usage profile of each Oracle Collaboration Suite component.

Oracle Collaboration Suite Dedicated Tier Installation and Management

There are only four types of installations involved in implementing the Dedicated Tiers option: Storage, infrastructure, middle tier, and Computer Telephony Server. However, because nodes are dedicated to performing specific roles, you need to set up as many as six different configurations and process combinations in the middle tier. In addition, there are two setup procedures on the database tier. A node dedicated to a particular role will have different setup and administration tasks as compared to a node dedicated to another role.

In theory, patches need to be applied only to the nodes they affect. For example, an Oracle Files middle tier patch need not be applied to the Oracle Email middle tier nodes. This feature helps reduce the overall work involved in maintaining the system.

Oracle Collaboration Suite Dedicated Tier Scalability

From the scalability perspective, the Dedicated Tiers option offers the flexibility of independently scaling up different elements of the system to accommodate of shifts in the workload. For example, if there is an increase in file usage over a period of time, then you can add more nodes to the system to handle the Oracle Files services with little impact on the rest of the system. This holds true as long as the increased load on the database tier is accommodated.

If SSL is implemented on the system, then you can add more nodes to handle HTTPS requests. These extra nodes are required to manage the increased workload of encryption. In addition, the increments in which you are allowed to scale up the system can be fine-grained.

Oracle Collaboration Suite Dedicated Tier Availability

To improve the availability of the infrastructure, you can use duplicated nodes, with each running an instance of Oracle Internet Directory. These instances of Oracle

Internet Directory are synchronized by using Oracle Internet Directory Replication. For standard operation, you can statically partition Oracle Internet Directory workload across these servers.

For the Oracle Calendar server, you must provide a failover node that can access the calendar on a shared disk. For other middle tier dedicated servers and servers in the DMZ, you can replicate and use load balancing. For the database tier, you can use clustered database servers running Oracle9*i* Real Application Clusters for the Oracle Files and Oracle Email databases.

Oracle Collaboration Suite Dedicated Tier Cost

You can implement the Dedicated Tiers option by using small, inexpensive hardware devices that run either Linux or Windows. However, due to the complexity of the system, the management costs may be higher than that of other deployment options.

To ensure high availability, you will need to use a large number of nodes if the nodes are individually dedicated to a variety of different roles. This factor would increase the hardware costs associated with this option.

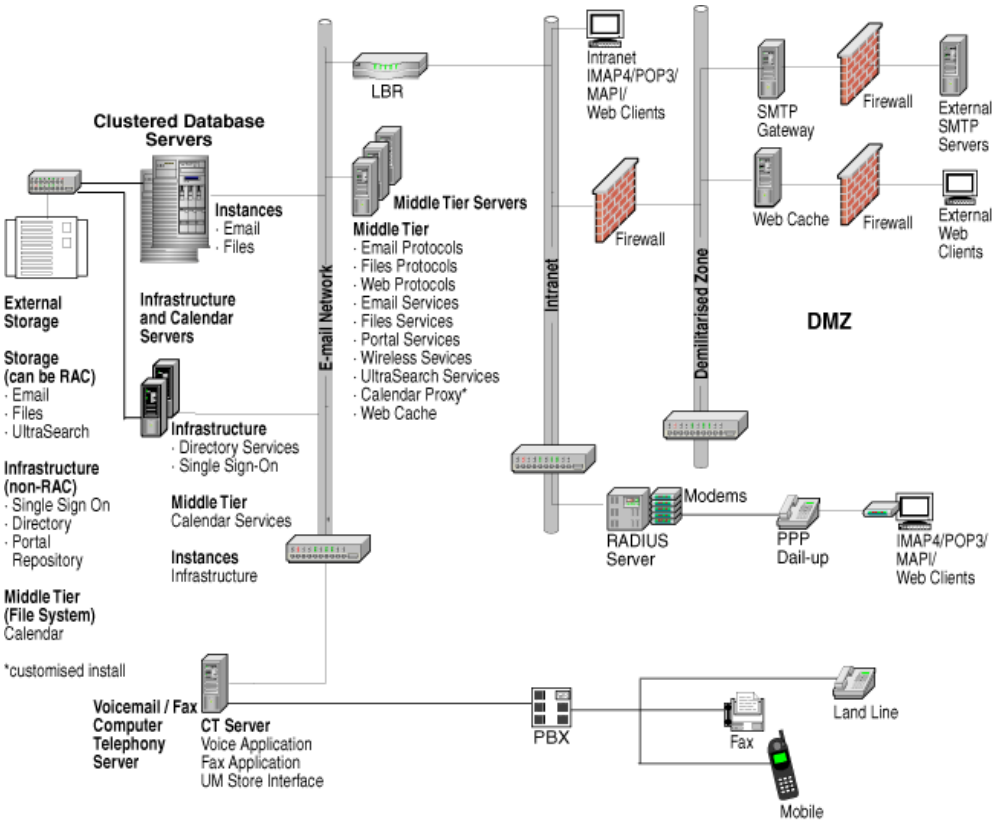
Illustration of Oracle Collaboration Suite Duplicated Middle Tiers

The Duplicated Tiers option must be used if the solution is to be outsourced or based on Collaboration Certified Configuration.

Note: Collaboration Suite Certified Configuration is a well-defined configuration of an Oracle Collaboration Suite installation. This configuration is used by Oracle Outsourcing to standardize the administration and maintenance activities for an Outsourced Oracle Collaboration Suite service. It features Oracle Collaboration Suite deployed in a standard file layout and is supported with management scripts and procedures.

Figure 3–5 illustrates an implementation of Duplicated Tiers.

Figure 3–5 Oracle Collaboration Suite duplicated middle tiers



Details on this illustration are provided in the following topics:

- Physical Location of Oracle Collaboration Suite Duplicated Tier Components
- Oracle Collaboration Suite Duplicated Tier Workload
- Oracle Collaboration Suite Duplicated Tier Installation and Management
- Oracle Collaboration Suite Duplicated Tier Scalability
- Oracle Collaboration Suite Duplicated Tier Availability
- Oracle Collaboration Suite Duplicated Tier Cost

Physical Location of Oracle Collaboration Suite Duplicated Tier Components

By implementing the Duplicated Tiers option, you can simplify the system, reduce the number of nodes needed for a small system, and obtain the flexibility of distributing components. In this deployment architecture, there are at most four types of nodes: middle tier, information storage, infrastructure and the Oracle Calendar server, and Computer Telephony.

The middle tier nodes handle requests for all components: Oracle Email, Oracle Files, the Oracle Calendar server, and Oracle UltraSearch. These nodes can also handle requests from both Web and wireless clients. These nodes must all have the same installation, setup, and process profile.

information storage is installed on each of two or more clustered nodes. It consists of both Oracle Files and Oracle Email instances with databases configured to use Oracle9*i* Real Application Clusters placed on a shared disk. In larger deployments, you can use

an Oracle9*i* Real Application Clusters for each of the Oracle Files and Oracle Email databases, which would help separate them in the event of a failure.

The infrastructure is installed on a separate node. Its database, which is not certified for use with Oracle9*i* Real Application Clusters, is placed on the shared disk and accessed from a dedicated instance on the node.

The Oracle Calendar server processes are either installed on the same node as the infrastructure or on a dedicated node, and the Oracle Calendar server file system is placed on a shared disk. An Oracle Calendar server proxy is placed on each middle tier node to pass on requests for the Oracle Calendar server to the combined infrastructure and the Oracle Calendar server node. As a variation of this option, you can run the Oracle Internet Directory processes on the middle tier nodes, instead of the combined or dedicated infrastructure node. In this case, the installation becomes compliant with the `Advanced Configuration: Multi Oracle Collaboration Suite mid-tier` option of Collaboration Suite Certified Configuration. This option offers good separation of the application tier and database tier.

Oracle Collaboration Suite Duplicated Tier Workload

The Duplicated Tiers option allows for some separation of workload types. This separation is not as comprehensive as the separation allowed by the Dedicated Tiers option. By using the Duplicated Tiers option, you can optimize the performance of the information storage nodes and the middle tier nodes.

One of the advantages of this deployment architecture option is that when the workload shifts between components during the business day, the capacity of the entire middle tier is available to respond to all types of requests. This is in contrast to the Dedicated Tiers scenario described earlier, in which the Oracle Email nodes would be underused and the Oracle Files nodes would have to cope with the peak load.

Oracle Collaboration Suite Duplicated Tier Installation and Management

In the Duplicated Tiers option, there are only four types of installation, configuration, and combination of processes involved, even when the system grows very large. The fact that all middle tier nodes handle all types of requests means that you can automate the management of these nodes, which are likely to be duplicated multiple times in large systems, by using appropriate tools or shared installation images. By using Blade Servers and shared installation images, you can easily add new middle tier processing capability by mounting the appropriate disk and starting the middle tier processes. Any middle tier patch must be applied to all the middle tier nodes. However, if you use shared images, then you need to apply the patch only once.

Oracle Collaboration Suite Duplicated Tier Scalability

From the scalability perspective, this deployment architecture option provides a lot of flexibility for scaling up in small increments. However, you cannot scale up specific components. Because all middle tier nodes handle all types of requests, all the components will have access to any new resource that is added. If the size of a particular workload grows, then the proportion of all middle tier nodes that are used to handle this workload will increase.

Oracle Collaboration Suite Duplicated Tier Availability

With the Duplicated Tiers option, the alternatives for improving availability are the same as those for the Dedicated Tiers option. To improve the availability of the infrastructure, you can provide duplicated nodes with instances of Oracle Internet Directory synchronized by using Oracle Internet Directory Replication.

You can statically partition the Oracle Internet Directory service workload across these nodes for normal operation. For the Oracle Calendar server, you must provide a failover node that can access the Oracle Calendar server on a shared disk. You can replicate and use load balancing for the other middle tier dedicated servers and servers in the DMZ. For the database tier, you can use clustered database servers that run Oracle9*i* Real Application Clusters for the Oracle Files and Oracle Email databases.

Oracle Collaboration Suite Duplicated Tier Cost

You can implement the Duplicated Tiers option by using small, inexpensive hardware devices that run Linux or Windows. In addition, management costs may be lower than that for other deployment architecture options due to the simplicity of the system. It is possible to start with a lower number of nodes for a small system as compared to the number of nodes required when implementing the Dedicated Tiers option.

Comparison between Oracle Collaboration Suite Architecture Types

Each deployment architecture option offers advantages. The Duplicated Tiers option allows for a certain degree of workload separation and the ability to start relatively small and maximize resource use as the workload for particular services increases. In addition, this deployment architecture option is relatively cheap to manage and is consistent with Collaboration Suite Certified Configuration.

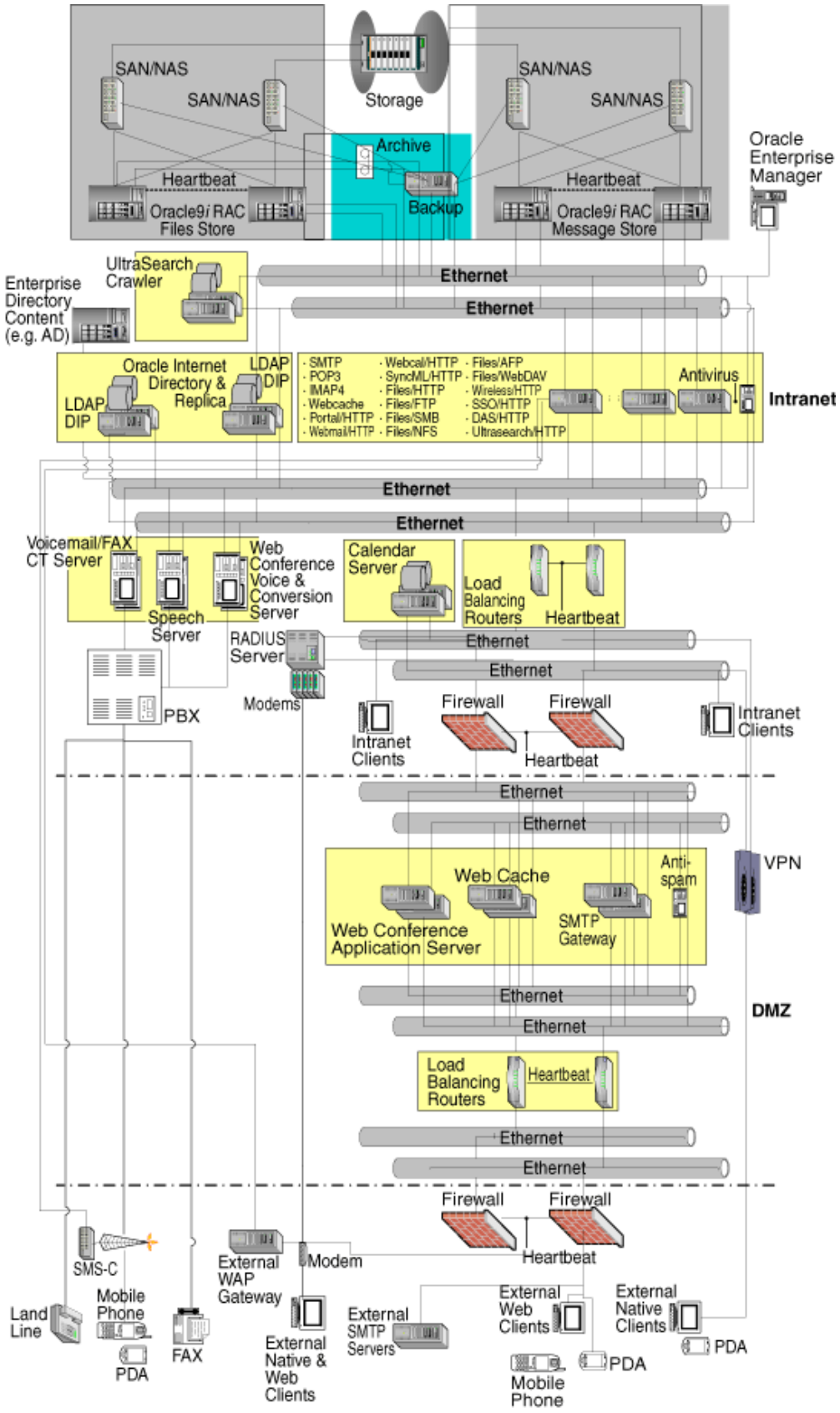
The Dedicated Tiers option offers the greatest flexibility to tune servers for specific uses and to scale up by component. However, this architecture is more expensive to manage. It is preferred for systems in which the implementation of components is being phased in, and for large systems in which the resource demands can be estimated.

Comprehensive Oracle Collaboration Suite Duplicated Middle Tier Deployment

This section describes an Oracle Collaboration Suite deployment in which every client and every service is deployed across an architecture that allows intranet and internet access while optimizing security, availability, scalability and fault coupling. This is a duplicated middle tier deployment. Figure 3–6 shows a fully fault-tolerant network, and multiples of each and every component to provide a full, high-availability, multiple network zone deployment.

Note: Figure 3–6 is for illustrative purposes only. It is intended to show a sample deployment that might be appropriate for the needs of a large organization. For smaller organizations, Oracle Collaboration Suite can be deployed with a much simpler architecture and lesser hardware requirements. See Chapter 4, "Oracle Collaboration Suite Deployment Examples" for examples of typical Oracle Collaboration Suite deployments appropriate for the needs of small, medium, and large organizations, with differing levels of requirements for security, performance, and availability.

Figure 3–6 Comprehensive Oracle Collaboration Suite Duplicated Middle Tier Deployment



This deployment is described in the following topics:

- Oracle Collaboration Suite Duplicated Tiers: Network Infrastructure
- Oracle Collaboration Suite Duplicated Tiers: Clients
- Oracle Collaboration Suite Duplicated Tiers: DMZ Tier
- Oracle Collaboration Suite Duplicated Tiers: Intranet Tier
- Oracle Collaboration Suite Duplicated Tiers: Database Tier

Oracle Collaboration Suite Duplicated Tiers: Network Infrastructure

This section describes the following elements of the network infrastructure:

- Security Zones
- Redundant Network Paths
- Firewalls
- Load Balancers

Security Zones The security of an Oracle Collaboration Suite network architecture is based on a three-zone setup. This setup consists of the intranet, a DMZ, and external networks such as the Internet.

Redundant Network Paths The network is configured to be redundant, with dual network paths to each Oracle Collaboration Suite component. To reduce the switch count, you can use virtual LANs. The entire Oracle Collaboration Suite network infrastructure must be at least 100 MBps. If you want to use network-attached storage, then the leftmost network segment next to the database servers in the diagram must be at least 1000 MBps, with redundancy. Remember that to ensure redundancy, you must use multiple network adapter cards (two or four) for each server host.

Firewalls Firewalls demarcate the intranet from the DMZ and the DMZ from the Internet. These firewalls are configured to monitor each other using a heartbeat mechanism so that if one fails, then the other continues to provide service.

For security, the DMZ firewall is configured to allow only HTTPS access over the Web or wireless media and SMTP services. In addition, it is configured to allow connections to ports required by Oracle Web Conferencing for enabling Web seminars and meetings.

The intranet firewall is configured to allow only HTTP and SMTP service to pass from the DMZ to the intranet. In addition, if Web seminars or meetings enabled by Oracle Web Conferencing need to be conducted over the Internet, then Oracle Network and LDAP access must be provided by the firewall exclusively to the Web Conferencing application servers in the DMZ.

Load Balancers Load balancers play a key role in the Oracle Collaboration Suite deployment architecture. They are configured in heartbeat-failover pairs in the DMZ as the front end for services such as e-mail relay and Web access to the Internet. They also form the front end of the Oracle Collaboration Suite service complex in the intranet. Load balancers route requests to pools of active servers that provide application services, to distribute the load dynamically across available resources. If a node fails, then the content switches route service requests to the surviving servers. For both pairs of load balancers, the "sticky for session" attribute must be set for all services.

The load balancer pair in the DMZ is configured with virtual hosts. These virtual hosts are mapped to the HTTPS service through the Web Cache servers and the Web Conferencing application servers, and to the SMTP service through the SMTP relay server pool.

In addition, a common feature of some load balancers is the ability to provide SSL acceleration. If this feature is available, then you should use it to offload the work of encryption from the DMZ servers and reduce the requirement for resources.

The load balancer pair in the intranet is configured with virtual hosts and services mapped to two partitioned server pools.

Oracle Collaboration Suite Duplicated Tiers: Clients

This section describes the following end-user devices supported by Oracle Collaboration Suite:

- Native Clients
- Web Clients
- External SMTP Servers
- External WAP Gateways
- Fax
- Telephone
- SMS-C

Native Clients The term "native client" refers to client devices such as PCs, Netscape Messenger, Oracle Corporate Time, and PDAs running client-side applications such as Microsoft Outlook.

Because native clients must communicate using application protocols (such as POP and IMAP) or proprietary protocols, typically, they are used only within the intranet, or outside the intranet through virtual private network (VPN) or intranet dial-up access.

Web Clients Oracle Collaboration Suite applications are served as markup-based applications to Web clients on PCs, PDAs, and mobile phones. For security, all Web clients should access only those published services that are provided over SSL.

External SMTP Servers These servers provide the connections by which Oracle Collaboration Suite exchanges e-mail with other sites.

External WAP Gateways External WAP gateways enable access to Oracle Collaboration Suite services through mobile phones and certain types of PDAs. These gateways are often deployed at mobile service provider sites. The type of access can be one of the following:

- Pull-type service, like a PC browser application
- Push-type service, like a WAP push operation

> **Note:** A WAP push operation can send an out-of-band message to a mobile device and present the user with an alert and the opportunity to log in to the application.

The Oracle Wireless and Voice application communicates principally with WAP gateways for mobile data access.

Fax When configured for Voice mail and Fax, fax machines can send pages to the Oracle Voicemail and Fax server. These pages are delivered as faxes to users' unified inboxes. When configured for wireless and voice services, the speech server can perform outbound operations such as sending e-mail or files to a fax machine.

Telephone When configured for voice mail and fax, telephones (mobile or landline) can be used to send and receive voice mail. When configured for wireless and voice services, you can use both speech recognition and speech synthesis to access a number of Oracle Collaboration Suite services. In addition, you can make outbound calls by using the Oracle Wireless and Voice component to deliver alerts to users.

SMS-C Mobile phone users can use the Oracle Wireless and Voice component to deliver text alerts. This component can respond to short text codes to access Oracle Collaboration Suite functionality.

Oracle Collaboration Suite Duplicated Tiers: DMZ Tier

The DMZ tier is exposed to allow services to be presented over the Internet. You must configure the DMZ firewall to allow SMTP, Web HTTP, and Web conferencing traffic.

This section describes the following elements of the DMZ tier:

- DMZ Firewalls
- DMZ Content Switches
- SMTP Gateways
- Anti Spam Server
- Web Caches
- Web Conferencing Application Servers

DMZ Firewalls The DMZ firewall permits only published services on the Internet to access the DMZ. This firewall must be configured to allow SMTP, Web over HTTP, and Web conferencing traffic. Two separate firewalls are used with a heartbeat mechanism running between them to ensure that failover takes place in the event of a firewall failure.

DMZ Content Switches Figure 3–6 shows two LBRs, one connected to the firewall and the other to the Oracle Collaboration Suite components in the DMZ. Like the firewalls, the LBRs are configured to monitor a heartbeat between them to ensure that failover takes place in the event of an LBR failure. The DMZ LBRs also provide service-level failover in the DMZ. The LBR must be configured for "sticky" sessions to the DMZ hosts.

SMTP Gateways The SMTP gateways relay e-mail into and out of the Oracle Collaboration Suite system. The SMTP gateways are hosts that run standard `sendmail`. These hosts are configured to relay e-mail addressed to users and domains served by Oracle Collaboration Suite and to the SMTP mail transfer agent located on the intranet. They can also be configured to relay e-mail from allowed hosts on the Internet. If you do not configure the SMTP relay to relay mail only from known allowed hosts, then your infrastructure may be compromised for use by spammers. You can also configure the SMTP relays to require authentication and to provide secure SMTP connections over SSL.

There are at least two SMTP relays in the DMZ, and the DMZ LBR balances the load across both SMTP mail relays. If one SMTP relay fails, then the surviving SMTP relay will continue to provide service. If the e-mail volume is very high, then you can incorporate additional SMTP relay servers into the DMZ tier to provide additional capacity.

Anti Spam Server The SMTP gateway relays incoming e-mail to the Anti Spam component. This component relays e-mail that is not identified as spam back to the SMTP gateway for delivery to the users and domains on the intranet. By deploying the Anti Spam server in the DMZ with (or on the same server as) the SMTP gateway, spam can be blocked at the earliest opportunity. You can also have an antispam solution in which a service entity on the Internet filters inbound e-mail for spam before relaying the e-mail to the SMTP gateway in the DMZ. In this case, spam never reaches the DMZ. If required, you can configure the Anti Spam server for redundancy or to scale up throughput.

Web Caches In the DMZ, the Web service is routed through the Web Cache instances. These Web Cache instances act as reverse proxies and caching servers for the Web servers that generate application content on the intranet. There are at least two Web Cache instances in the DMZ. These Web Cache instances provide load balancing and failover features.

Web Conferencing Application Servers If Oracle Web Conferencing is configured, then you must place a subset of the components, specifically the Web Conferencing application servers, within the DMZ. This would allow Internet attendees to participate in Web conferences and Web seminars.

Both Web over HTTP (to locate, join, or start meetings and seminars) and two ports for Web conferencing-specific protocols must be allowed to pass through the DMZ firewall. The protocols specific to Web Conferencing need not be routed through the DMZ LBR, because Web Conferencing has its own internal failover mechanism.

In addition, because Web Conferencing application servers require Oracle Internet Directory and Oracle Network Services, you must configure the intranet firewall to allow these protocols to be accessed only from the Web Conferencing application servers. There are at least two Web Conferencing application servers to provide for availability and capacity.

Oracle Collaboration Suite Duplicated Tiers: Intranet Tier

The Intranet tier hosts the core Oracle Collaboration Suite components. It is also assumed that the intranet is a secure and trusted network and that most users of Oracle Collaboration Suite are within the bounds of the intranet. The intranet is demarcated by the intranet firewall between the intranet and the DMZ. The users within the bounds of the intranet can be on the intranet, tunneled through by VPN servers, or connected through modem banks.

This section describes the following elements of the DMZ tier:

- Intranet Content Switches
- Oracle Internet Directory and Replica
- Enterprise Directory Information
- Oracle Calendar Server
- Oracle Voicemail and Fax Computer Telephony Servers
- Voice Servers

- Oracle Web Conferencing Voice and Conversion Servers
- Oracle UltraSearch Crawler Servers
- Oracle Collaboration Suite Server Pool
- AntiVirus Server

Intranet Content Switches The intranet LBRs are configured as a failover pair with heartbeat monitoring. They are also configured to distribute HTTP requests to one pool of application servers, and to distribute LDAP protocol requests to another pool that contains the core Oracle Collaboration Suite infrastructure components. The "sticky" session attribute must be set for Oracle Collaboration Suite services routed by the LBRs.

Configuring Oracle Internet Directory for serving the LDAP directory protocol involves a more detailed setup. As a preview, the Oracle service will be provided by at least two servers in an active-active configuration.

It is recommended that you partition Oracle Collaboration Suite services according to the specific LDAP Oracle Internet Directory server they access. To achieve this, you must configure three virtual hosts for LDAP service on the intranet LBRs. You must configure the first virtual host as a host/LDAP port that maps to the first LDAP server and fails over to the second LDAP server. The second virtual host must be configured as a host/LDAP port that maps to the second LDAP server and fails over to the first LDAP server. Note that these two virtual hosts are not configured to implement load balancing. The third virtual host must be configured to map to both LDAP servers and must provide load balancing between both servers.

Oracle Internet Directory and Replica Oracle Internet Directory is the core of the Oracle Collaboration Suite infrastructure, and is used by all the other Oracle Collaboration Suite components. It is accessed through the LDAP protocol. Because it performs a critical role, it must be configured for high availability. You can achieve this by first setting up IP/storage failover between a pair of servers in active/active configuration and then setting up replication between them. Each pair of servers manipulates its own infrastructure database replica, and each pair replicates to the other pair, bidirectionally, by using Oracle Advanced Replication.

A native client must be assigned an LDAP server host name and port. By using the LBR configuration discussed earlier in this document, you can assign native clients the host name and port of the virtual host on the LBR that is configured to provide load balancing across both LDAP servers.

Each replica can be configured to use Oracle9*i* Real Application Clusters. This is not shown in Figure 3–6.

Enterprise Directory Information Enterprise directory information can be provided by a source other than the directory infrastructure of Oracle Collaboration Suite. In such cases, you can bidirectionally populate and update the key directory elements of Oracle Collaboration Suite by using the Directory Integration Platform (DIP).

Oracle Calendar Server The Oracle Calendar server maintains its own data store for calendar information. To maintain availability, the core Oracle Calendar server components are configured to run on an IP/file system active/standby failover pair of physical servers. HTTP-based calendar services, such as the Web-based calendar application and SyncML services, run on different hosts. Native clients such as Outlook Connector and Corporate Time connect directly to the primary Oracle Calendar server.

Oracle Voicemail and Fax Computer Telephony Servers You must configure the Oracle Voicemail and Fax servers on the intranet and connect them to a PBX. Typically, the connection to the PBX is in the form of a T1/E1 or telephone line. To receive voice mail and faxes, you must configure the PBX to transfer busy or no-answer calls along with recipient information to the Oracle Voicemail and Fax servers. To achieve high availability, there is a pair of Oracle Voicemail and Fax servers. Each server is configured on the PBX so that if one fails, then calls are rerouted to the surviving server. You must configure the PBX to provide a dial-in number for telephone-based voice mail retrieval.

Voice Servers The voice servers must reside on the intranet. You must connect these servers to the PBX (typically through a T1/E1 or telephone line) in distinct "hunt groups". To provide speech recognition and speech synthesis interfaces over the telephone to e-mail, calendar, files, and directory services, you must configure the PBX to provide a dial-in access number that is distinct from the voice mail access number. The PBX must allow the voice server to make outbound calls for telephone-delivered alerts.

Oracle Web Conferencing Voice and Conversion Servers The Oracle Web Conferencing voice and conversion servers provide voice digitalization and presentation document conversion services. These servers are deployed in a failover pair and are located on the intranet. You must configure the Web Conferencing application servers in the DMZ so that they can communicate with all voice and conversion servers on the intranet. As mentioned earlier in this document, the Web Conferencing application servers communicate from the DMZ to the voice and conversion servers by using the port passed by the intranet firewall.

Oracle UltraSearch Crawler Servers If configured, you must deploy the Oracle UltraSearch crawler servers as a failover (IP/file system) pair. These servers must be made to share active/standby access to a database for Oracle UltraSearch. The crawler will access specified sites to build an intranet (and in some cases, Internet) search index.

Oracle Collaboration Suite Server Pool The mainstay of the intranet deployment is the pool of two or more servers, each of which runs all of the Oracle Collaboration Suite application protocols. The intranet LBR distributes requests to the servers in this pool according to protocol. The services provided include the following:

- SMTP for e-mail that is sent and received on the intranet
- POP3 and IMAP for native e-mail clients
- WebDAV, FTP, SMB, AFP, and NFS file access protocols
- The Web and Mobile XML user interfaces for Oracle9*i*AS Portal, Webmail, Web Calendar, SyncML, Oracle Files Web application, Oracle Wireless and Voice, and Oracle UltraSearch
- Oracle9*i*AS Single Sign-On services and self-service Oracle Delegated Administration Services

By configuring at least two hosts in the pool, you can ensure high availability for all application protocols. For scalability and enhanced throughput, you can add additional servers to this pool and update the LBR configuration. This configuration also ensures maximum use of resources in this pool across all application services.

You must follow the recommended method for configuring the application services to access directory services on each server in the pool. You must configure the SMTP MTA, Oracle Files, Oracle9*i*AS Portal, Oracle Wireless and Voice, Webmail, and Oracle Web Conferencing to access one of the virtual hosts on the LBR that routes requests to

only one of the LDAP servers. IMAP, POP, Oracle Delegated Administration Services, Oracle9*i*AS Single Sign-On, the Oracle Calendar server, and Oracle Voicemail and Fax must be configured to access the other virtual host on the LBR that maps to the second LDAP server. This form of partitioning offers the following benefits:

- **Directory updates are grouped**: Directory updates that might affect users, such as password updates, are grouped together. Therefore, users need not wait for directory replica propagation to complete before the update takes effect.
- **Requests for directory services are evenly distributed**: Typically, the SMTP MTA, Oracle9iAS Single Sign-On, IMAP, POP, and Oracle Calendar place a high load on directory services. The user interfaces for Oracle Files, Oracle9iAS Portal, Oracle Wireless and Voice, Webmail, and Oracle Web Conferencing do not. By partitioning, the traffic for directory services is evenly balanced across competing application services.

AntiVirus Server The AntiVirus server receives e-mail from all the SMTP MTAs and returns uninfected or cleaned e-mail. The AntiVirus server is placed in the intranet and not in the DMZ. This way, it can be used by the e-mail administrative components to scan e-mail in the mail store, which was not scanned by the AntiVirus server at the time it was delivered. You must ensure that the AntiVirus server has a steady connection to the Internet for receiving virus signature updates.

Oracle Collaboration Suite Duplicated Tiers: Database Tier

Although somewhat of a misnomer (since we have already discussed data stores for the directory, its replica, the Oracle Calendar server, and the Oracle UltraSearch crawler), in any deployment of Oracle Collaboration Suite, the majority of database storage will be dominated by Oracle Email and Oracle Files.

For the deployment architecture shown in Figure 3–6, the guideline for using different Oracle Email and Oracle Files databases must be followed on the assumption that both databases would be handling large workloads. In addition, both databases are configured for multiserver Oracle9*i* Real Application Clusters access. This feature enhances the availability and scalability of the database tier.

Oracle Files Store The Oracle Files store is implemented by at least two servers for active/active access to the databases containing user files and e-mail, respectively. These servers are configured for Oracle9*i* Real Application Clusters. In addition, there are redundant paths to the physical disk storage for the Oracle Files store, regardless of whether the connection to the storage is NAS or SAN. As mentioned earlier in this document, if you are using NAS storage, then the network bandwidth for this segment must be 1000 MBps. In addition, the Oracle Files store is directly connected to a backup server to allow for fast backups, perhaps not requiring direct processing by the database servers.

Message Store The setup for the Message Store is identical to the setup for the Oracle Files Store.

4

Oracle Collaboration Suite Deployment Examples

This chapter describes some real-life examples of Oracle Collaboration Suite deployments.

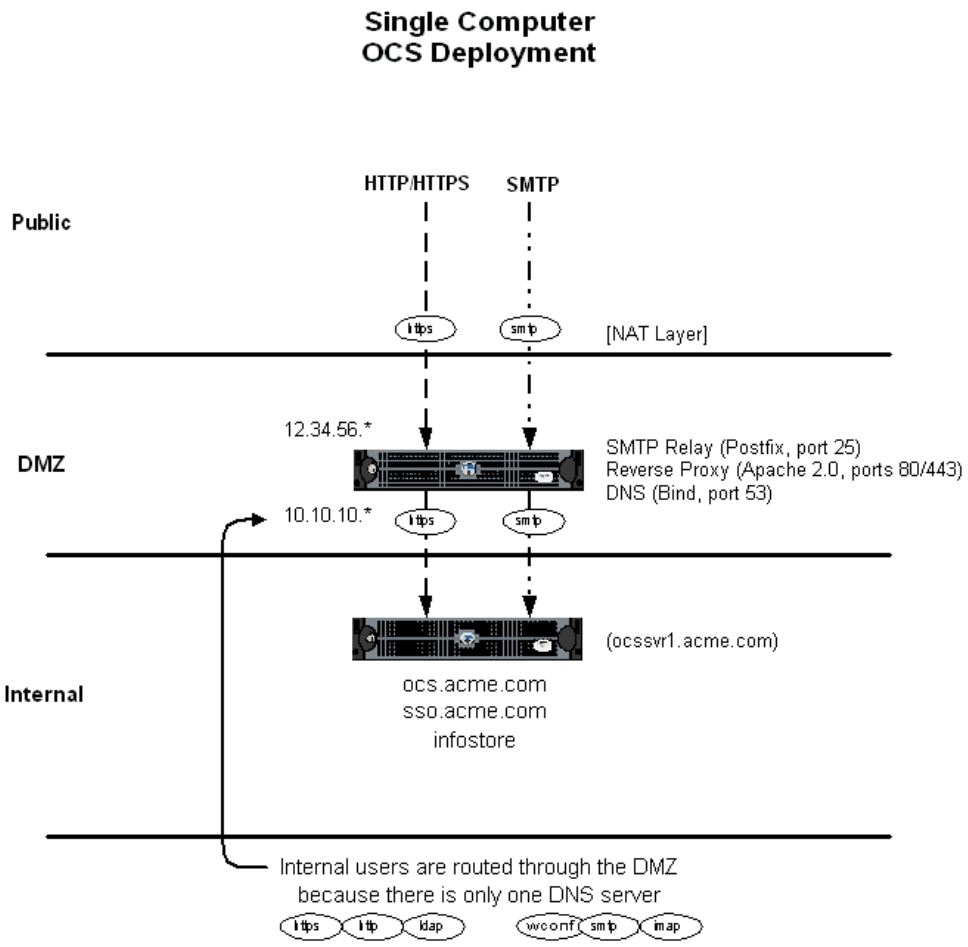
> **Note:** The examples provided in this chapter include references to third-party software and hardware. The examples given are provided for reference only, and may not reflect your organization's demands or architecture.

This chapter contains the following topics:

Oracle Collaboration Suite Single Computer Deployment (200 Users)

Figure 4–1 illustrates an example of Oracle Collaboration Suite deployed on one computer.

Figure 4–1 Oracle Collaboration Suite Single Computer Deployment for 200 Users



In this deployment, all three tiers are installed on a single internal server. Network services run on another server residing in the DMZ, including the Postfix mail relay on port 25, Apache 2.0 Reverse Proxy on ports 80 (HTTP) and 443 (HTTPS) and a single BIND DNS server on port 53.

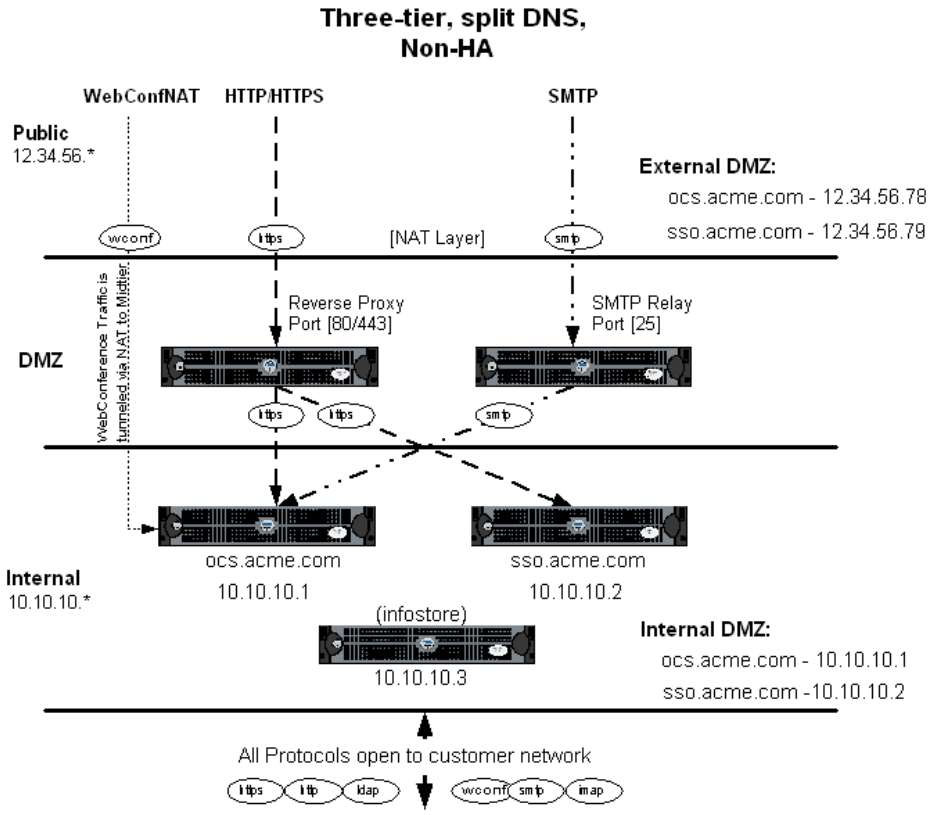
Internal users connect to Oracle Collaboration Suite through the DMZ because it contains the only DNS server. External users connect to the Oracle Collaboration Suite domain on the routable 12.34.56.78 IP address, and are served content by the proxy server, which communicates with Oracle Collaboration Suite through a firewall.

The interior network provides open access, 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 increases in bandwidth where necessary.

Oracle Collaboration Suite Simple Deployment (2000 - 4000 Users)

Figure 4–2 illustrates a single-box Oracle Collaboration Suite deployment for 2000 to 4000 users.

Figure 4–2 Oracle Collaboration Suite Simple Deployment (2000 - 4000 Users)



In this deployment, the three tiers each reside on their own server inside an internal network. NAT is used to tunnel Web Conferencing to the middle 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 allows 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.

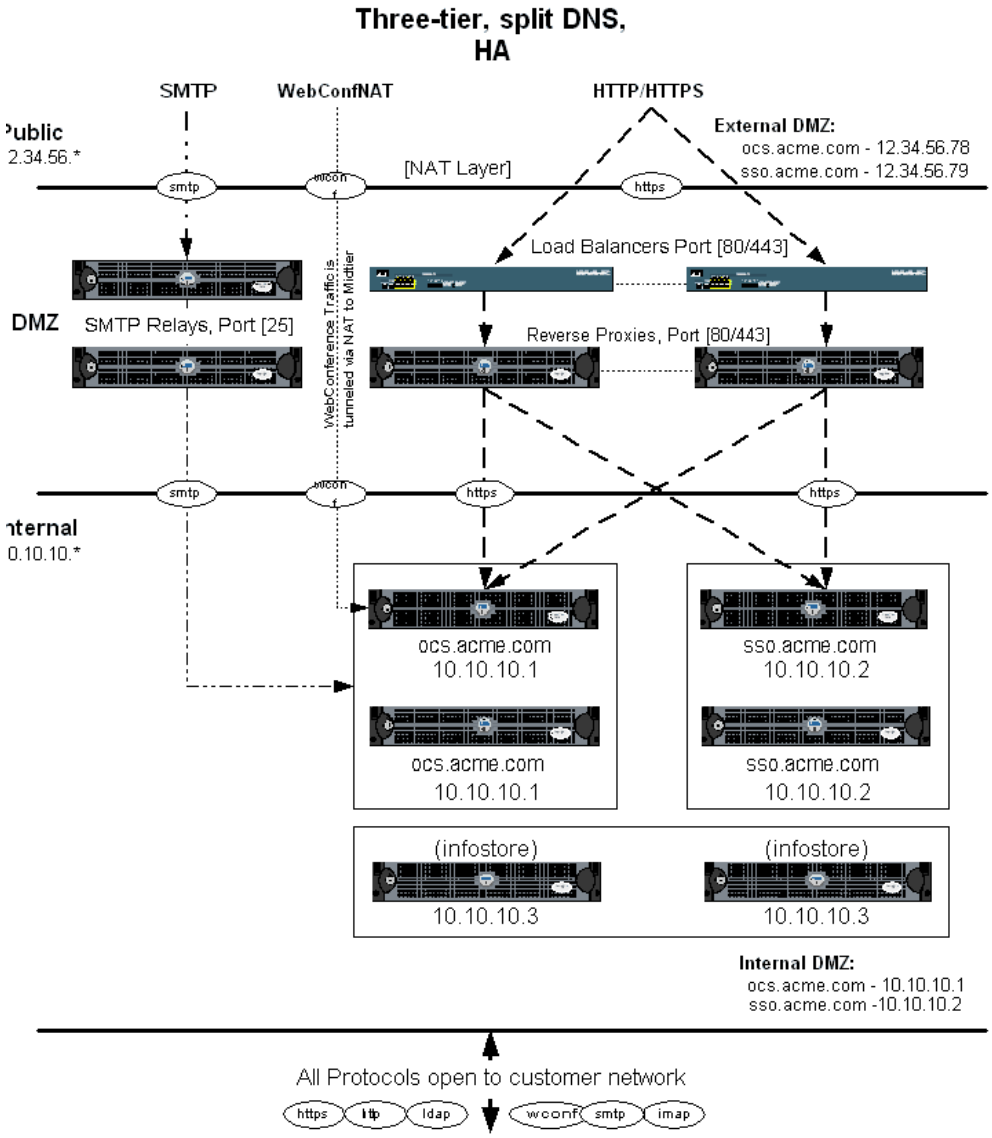
The internal network provides open access for its users, and is likely to be set up as a DMZ. The exterior network (the Internet) will have access to HTTPS, SMTP and Web Conferencing traffic. Web Conferencing and Files traffic are still being determined, and require appropriate increases in bandwidth where necessary.

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

Oracle Collaboration Suite High Availability Deployment (2,000 - 4,000 Users)

Figure 4–3 illustrates an example of a high availability deployment of Oracle Collaboration Suite.

Figure 4–3 Oracle Collaboration Suite High Availability Deployment (2,000 - 4,000 Users)



This deployment is similar to the previous example, Oracle Collaboration Suite Simple Deployment (2000 - 4000 Users), with the main difference being that the three tiers and network services servers are all duplicated. Load balancers are used to distribute HTTP and HTTPS traffic.

As in the previous example, NAT is used to tunnel Web Conferencing to the middle 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 allows 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

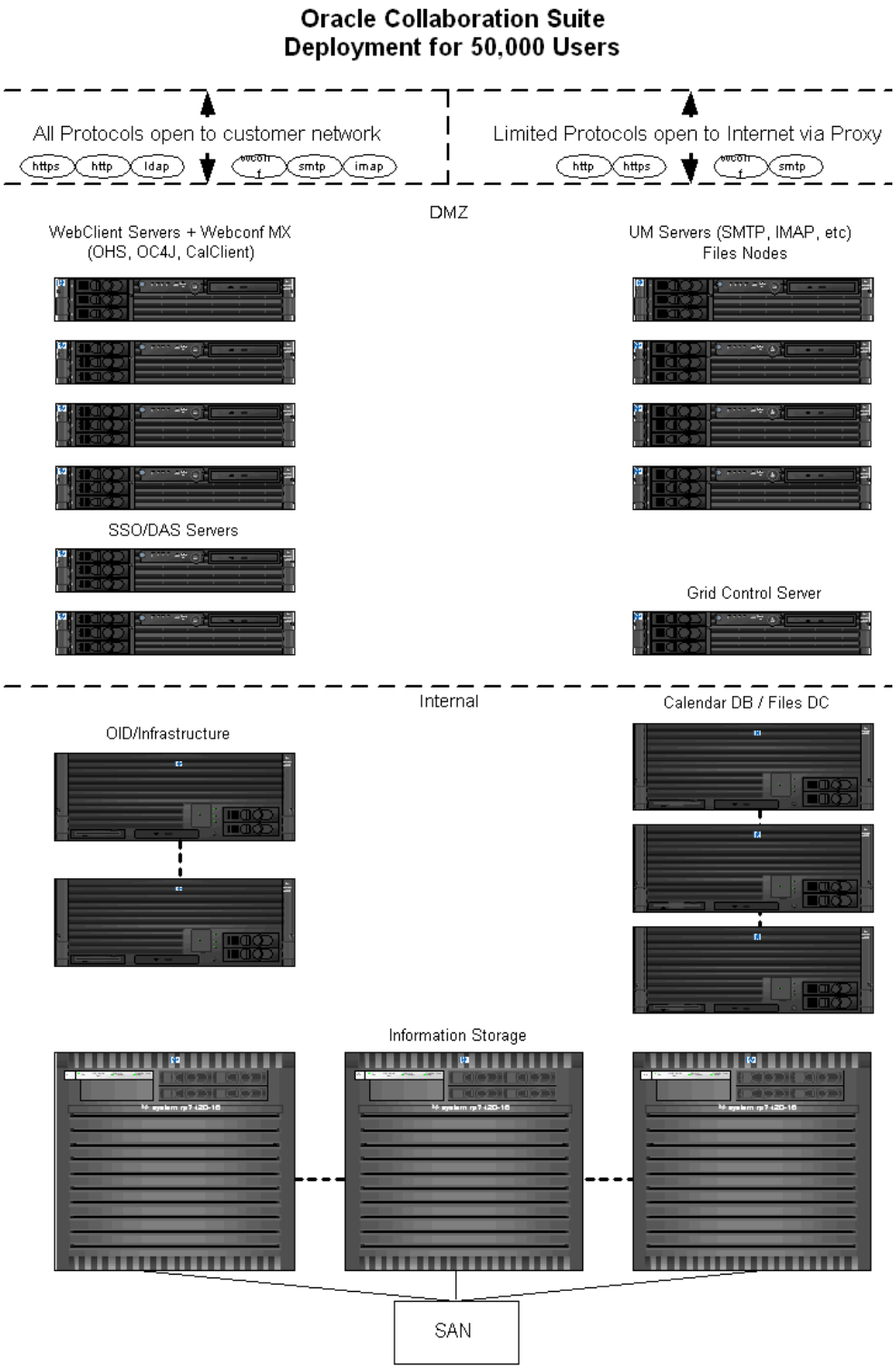
Conferencing and Files traffic are still being determined, and require appropriate increases in bandwidth where necessary.

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

Oracle Collaboration Suite Large Deployment (50,000 users)

Figure 4–4 illustrates an example of a large Oracle Collaboration Suite deployment.

Figure 4–4 Oracle Collaboration Suite Large Deployment (50,000 users)



This high-volume deployment uses dedicated 64-bit HP-UX servers. Because the internal user base is so large, it is set up to connect to the middle tier through secure means. Single-Sign On and Oracle Delegated Administration Services are broken out from Oracle Internet Directory, so that users cannot access the backend.

The use of Oracle Enterprise Manager Grid Control 10*g*, on its own server, is strongly recommended for a deployment of this size. Oracle Enterprise Manager Grid Control 10*g* provides insight into your architecture through the use of monitoring agents on all Oracle servers. Oracle Enterprise Manager Grid Control 10*g* is designed to interact with Oracle Collaboration Suite.

The Oracle Calendar database runs on a cold failover cluster of three dedicated servers to accommodate the large user base. Files Domain Controller runs on this as well, to take advantage of failover functionality.

Information storage uses Oracle Database 10*g* with Oracle9*i* Real Application Clusters, while Oracle Internet Directory uses 10*g* Infrastructure (active-active).

Index

O

P

R

S

T

V

W