Sun Java™ Enterprise System

# Java Enterprise System Telecommunications Provider Scenario

2005Q4

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-5485-10

# Contents

# List of Figures

# List of Tables

# Preface

This *Java Enterprise System Telecommunications Provider Scenario* describes how to install Sun Java™ Enterprise System (Java ES) components to implement a Java ES architecture that is suitable for a medium-sized telecommunications provider. The specific features provided by the deployment covered in the *Telecommunications Provider Scenario* are described in Chapter 2, “The Requirements” on page 19.

## Who Should Use This Book

This guide is intended for the following types of readers:

- System architects who are developing architectures that are similar to the architecture described in this guide. If you are an architect who has similar requirements, you can use the architecture described in this guide as the basis for your own architecture.
- System administrators and installation technicians who are deploying an architecture that is based on the architecture described in this guide. If you are deploying an architecture that is based on the architecture described in this guide, you can modify the installation specifications, installation plan, and detailed installation instructions in this guide and implement the architecture that was developed for your site.

This guide assumes you are familiar with the following:

- UNIX® operating system
- Internet protocol (IP) computer networks
- Installing enterprise-level software products

# Before You Read This Book

Before performing any of the tasks described in this guide, you should read *Java Enterprise System Release Notes*. Refer to "Java ES Documentation Set" for descriptions and links to the Java ES documentation set.

# How This Book Is Organized

This book describes a typical set of requirements for a telecommunications company that provides remote services for both consumers and businesses. It also describes a Java ES architecture that satisfies the requirements, an installation plan for implementing the architecture, and detailed procedures for installing and configuring the Java ES components used in the architecture.

This book is organized in the following chapters:

- Chapter 1, "Introduction," introduces the business problem that is addressed in this guide.
- Chapter 2, "The Requirements," describes Telco's business and technical requirements for the deployment.
- Chapter 3, "The Architecture," describes the Java ES architecture that Telco developed to meet the business and technical requirements.
- Chapter 4, "The Deployment Specifications," describes the detailed technical specifications developed from the deployment architecture.
- Chapter 5, "The Installation and Configuration Plan," describes the detailed installation and configuration plan developed from the deployment specifications.
- Chapter 6, "Software Installation and Configuration Procedures," describes the detailed procedures for installing and configuring Java ES software on Telco's network.

# Java ES Documentation Set

The Java ES documentation set describes deployment planning and system installation. The URL for system documentation is `http://docs.sun.com/coll/1286.1`. For an introduction to Java ES, refer to the books in the order in which they are listed in the following table.

**Table 1** Java ES Documentation

| Document Title | Contents |
|---|---|
| Sun Java Enterprise System 2005Q4 Release Notes | Contains the latest information about Java ES, including known problems. In addition, components have their own release notes. |
| Sun Java Enterprise System 2005Q4 Documentation Roadmap | Provides descriptions of all documentation related to Java ES, both as a system and for the individual components |
| Sun Java Enterprise System 2005Q4 Technical Overview | Introduces the technical and conceptual foundations of Java ES. Describes components, the architecture, processes, and features. |
| Sun Java Enterprise System 2005Q4 Deployment Planning Guide | Provides an introduction to planning and designing enterprise deployment solutions based on Java ES. Presents basic concepts and principles of deployment planning and design, discusses the solution life cycle, and provides high-level examples and strategies to use when planning solutions based on Java ES. |
| Sun Java Enterprise System 2005Q4 Installation Planning Guide | Helps you develop the implementation specifications for the hardware, operating system, and network aspects of your Java ES deployment. Describes issues such as component dependencies to address in your installation and configuration plan. |
| Sun Java Enterprise System 2005Q4 Installation Guide for UNIX | Guides you through the process of installing Java ES on the Solaris Operating System or the Linux operating system. Also shows how to configure components after installation and verify that they function properly. |
| Sun Java Enterprise System 2005Q4 Installation Reference | Gives additional information about configuration parameters, provides worksheets to use in your configuration planning, and lists reference material such as default directories and port numbers. |
| Sun Java Enterprise System 2005Q1 Deployment Example Series: Evaluation Scenario | Describes how to install Java ES on one system, establish a set of core, shared, and networked services, and set up user accounts that can access the services that you establish. |
| Sun Java Enterprise System 2005Q4 Upgrade Guide | Provides instructions for upgrading Java ES on the Solaris Operating System or the Linux operating environment. |
| Sun Java Enterprise System Glossary | Defines terms that are used in Java ES documentation. |

# Typographic Conventions

The following table describes the typographic changes that are used in this book.

**Table 2** Typographic Conventions

| Typeface | Meaning | Example |
|---|---|---|
| AaBbCc123 | The names of commands, files, and directories, and onscreen computer output | Edit your `.login` file.<br>Use `ls a` to list all files.<br>`machine_name% you have mail.` |
| **AaBbCc123** | What you type, contrasted with onscreen computer output | `machine_name% su`<br>`Password:` |
| *AaBbCc123* | A placeholder to be replaced with a real name or value | The command to remove a file is `rm` *filename*. |
| *AaBbCc123* | Book titles, new terms, and terms to be emphasized (note that some emphasized items appear bold online) | Read Chapter 6 in the *User's Guide*<br>A *cache* is a copy that is stored locally.<br>Do *not* save the file. |

## Shell Prompts in Command Examples

The following table shows default system prompts and superuser prompts.

**Table 3** Shell Prompts

| Shell | Prompt |
|---|---|
| C shell on UNIX and Linux systems | `machine_name%` |
| C shell superuser on UNIX and Linux systems | `machine_name#` |
| Bourne shell and Korn shell on UNIX and Linux systems | `$` |
| Bourne shell and Korn shell superuser on UNIX and Linux systems | `#` |
| Microsoft Windows command line | `C:\` |

## Symbol Conventions

The following table explains symbols that might be used in this book.

**Table 4** Symbol Conventions

| Symbol | Description | Example | Meaning |
|---|---|---|---|
| `[ ]` | Contains optional arguments and command options. | `ls [-l]` | The `-l` option is not required. |
| `{ \| }` | Contains a set of choices for a required command option. | `-d {y\|n}` | The `-d` option requires that you use either the `y` argument or the `n` argument. |
| `${ }` | Indicates a variable reference. | `${com.sun.javaRoot}` | References the value of the `com.sun.javaRoot` variable.</para> |
| - | Joins simultaneous multiple keystrokes. | Control-A | Press the Control key while you press the A key. |
| + | Joins consecutive multiple keystrokes. | Ctrl+A+N | Press the Control key, release it, and then press the subsequent keys. |
| `&rarr;` | Indicates menu item selection in a graphical user interface. | File > New > Templates | From the File menu, choose New. From the New submenu, choose Templates. |

# Accessing Sun Resources Online

The `http://docs.sun.com` web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to `http://www.sun.com`

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)

- Training
- Research
- Communities (for example, Sun Developer Network)

# Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

**NOTE** Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

# Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-5485-10.

Chapter 1

# Introduction

This document describes the architecture, installation and configuration plan, and installation and configuration procedures for a Java ES deployment that is suitable for a telecommunications provider.

The deployment described in this example is for an imaginary telecommunications provider named Telco. Telco provides telecommunications services to the following three classes of users:

- Telco employees
- Individual consumers
- Business users

The services available to each class of customer are listed in Table 1-1.

**Table 1-1** Services Provided by the Telco Deployment

| Service | Available to Consumer-class customers? | Available to Business-class Customers? | Available to Telco employees? |
|---|---|---|---|
| Email through web browser client | ✔ | ✔ | ✔ |
| Email through stand-alone email client | ✔ | ✔ | ✔ |
| Email through portal desktop | | ✔ | ✔ |
| Calendar through web browser client | | ✔ | ✔ |
| Calendar through portal desktop | | ✔ | ✔ |
| Remote file access | | ✔ | ✔ |
| Hosted domain service | | ✔ | |

These services are all available from a single, distributed Java ES deployment. The key features of Telco's deployment, which are described in this deployment example, are the following:

- Support for different classes of service on a single, distributed Java ES deployment.
- The use of Java ES components and services to support hosted domains.
- The security strategy used to secure a Java ES deployment that is accessible from the public Internet.

This deployment example describes Telco's Java ES deployment in the following chapters:

- Chapter 2, "The Requirements," describes Telco's business and technical requirements for the deployment.
- Chapter 3, "The Architecture," describes the Java ES architecture that Telco developed to meet the business and technical requirements.
- Chapter 4, "The Deployment Specifications," describes the detailed technical specifications developed from the deployment architecture.
- Chapter 5, "The Installation and Configuration Plan," describes the detailed installation and configuration plan developed from the deployment specifications.
- Chapter 6, "Software Installation and Configuration Procedures," describes the detailed procedures for installing and configuring Java ES software on Telco's network.

Chapter 2

# The Requirements

This chapter describes the business and technical requirements for Telco's Java ES deployment.

These requirements are one possible set of requirements for a medium-sized telecommunications service provider. These requirements might be similar to requirements developed by other telecommunications providers planning to deploy and use Java ES services. Compare the requirements information in this chapter with your own business requirements to determine points of similarity and points of difference, and to determine what aspects of the Telco deployment are applicable to your business requirements.

## Capacity Requirements

Telco is a medium-sized telecommunications company that provides regional telecommunication services. Telco provides email and calendar services to three classes of users. The services available to each class of users and the approximate number of users in each class are listed in Table 2-1.

**Table 2-1** Number of Users of Telco's Services

| Service Class | Services Provided | Number of Users |
|---|---|---|
| Internal User | Email, calendar, and file access | 1,000 |
| Business User | Email, calendar, and file access | 15,000 |
| Individual Consumer | Email | 250,000-300,000 |

The deployed system must be scalable to accommodate an increasing number of users. The growth rate for business users is expected to be 3-5% annually. The growth rate for consumer users is expected to be 7-10% annually.

# Detailed Service Requirements

Telco offers mail, calender, and file access services to its customers. The detailed requirements for these services, which must be met by the Java ES deployment, are listed in Table 2-2:

**Table 2-2** Detailed Service Requirements

| Service | Requirements |
|---|---|
| Email Service | 50MB default mailbox size |
| | User-controlled ability to increase mailbox capacity to the system-wide maximum size (subject to limits based on users's service class) |
| | Attachments up to 15 MB allowed |
| | Vacation message service |
| | Forwarding service |
| | A web browser-based client that provides the following features: send and receive mail, personal address books, group address books, spell check, message search, return receipts, multiple attachments, folder management, message signature, access to shared directory, change passwords |
| | Multi-language viewing capacity, with the display language selectable by the user; languages to include English, French, and Spanish |
| | Portal-based access to mail services (internal and business users only) |
| Address Book Requirements | The address book is completely integrated with the email and calendar features |
| | Address books can be created for and shared by defined groups or special interest groups |
| | User can resize column headings, to the extent of hiding and revealing columns |
| | Address data can be imported from thick-client address mail clients and other software packages |
| | User can print and export address book data |
| | User can upload photographs of contacts to the address book |
| | Customer can add customer-defined fields, display and sort the customer-defined fields |
| | Customer can set up email lists dependent on administration rights |
| | Customer can create mailing lists based on information in the user profile (for example, supply a department name and create a mailing list of all users in that department) |
| | Portal based access |

**Table 2-2** Detailed Service Requirements *(Continued)*

| Service | Requirements |
|---|---|
| Calendar Service (Available Only to Internal Users and Business Customers) | Support for the user's local time zone |
| | Display the calendar by month, week or day |
| | Summarize weekly and monthly calendars in easily printed formats |
| | Set reminders for calendar events |
| | Ability to share workgroup calendars |
| | Organize multiple calendars within the user's workgroup per user with various privacy options (for example, separate work and family calendars) |
| | Group and resource scheduling, including the ability to invite other users to events, accept or decline invitations to events, designate events as either public or private, view available times for potential invitees, and view group schedules within the user's assigned group |
| | Ability to propose meeting options based on invitees schedules |
| | Ability to schedule repeating meetings |
| | Send meeting invitations by email that are localized to time zones, including multiple time zones for a single invitation |
| | Meeting organizer can easily address memos to all invitees, invitees who have accepted the invitation, or invitees who have not responded to the invitation |
| | Event notification, with notification delivered by email, pager, wireless, or SMS (short message service) device |
| | Interoperable with approved desktop clients such as MS Outlook and selected mobile devices |
| | Portal-based access |
| File Access Service (available only to internal users and business customers) | Web access to file systems |
| | Drag and drop user interface |
| | User can select multiple files and send these files in a single e-mail as multiple attachments. |
| | User can delete and rename remote files |
| | User can search for files and display the list in a separate window. |
| | User can manage folders such as establish, delete, and assign folders rights to others in the same workgroup. |
| | 10MB shared storage per user in the customer group. This shared storage should be user-scalable to a preset default maximum. |
| | Administrator or user defined shared folders |
| | Administrator can limit the size of the upload |

# Customer Usage Patterns

Based on experience, Telco expects their business customers to be most active during the 8:00 a.m. to 5:00 p.m. working hours, although there will be some activity by business customers outside those hours.

Based on experience, Telco expects their residential customers to be most active during the evening hours, although there will be significant activity during daytime hours.

# Availability Requirements

Telco requires that the Java ES deployment be highly available. They specify 99.995 availability.

# Performance Requirements

Telco requires that the Java ES provide good response time. They specify 1-2 seconds response to a remotely installed thick client at peak load.

# Serviceability Requirements

An important aspect of Telco's Java ES deployment is that business customers be able to administer their own domains. An administrator at a business customer should be able to perform the system administration tasks listed in Table 2-3.

**Table 2-3** Serviceability Requirements

| Serviceability Category | Requirements |
|---|---|
| Business Customer System Administration | Provision account aliases and custom aliases, as permitted by domain or workgroup role<br>Add and delete users, increase mailbox size, change passwords, and other similar functions<br>Reroute mail from terminated or suspended accounts at the domain, delegate, and workgroup delegate levels<br>Create, modify, and delete domains<br>Create, modify, and delete mailing lists<br>Perform tiered or layered administration of the following<br>• User roles, groups, privileges, and access controls<br>• Web access to admin<br>• Single Sign On/Sign Off<br>• Display of services per user<br>• Migration tools/support<br>• Automatic settings for single or multiple customer users (privacy issues)<br>• Self up-selling – customer control for adjusting the tier of service at their domain |

# Scalability Requirements

As described in "Capacity Requirements" on page 19, Telco expects their user base to grow. For various reasons, Telco has adopted a strategy of horizontal scalability, or adding more computers to the system as user activity increases. The architecture for Telco's Java ES deployment must allow for horizontal scalability. The exact configuration of Java ES components that supports horizontal scalability will be developed when the deployment architecture is developed. For more information, see "Planning for Scalability in the Architecture" on page 41.

# Security Requirements

Security is an important consideration for a system accessed by a large number of users over the public Internet. Telco has developed the security requirements listed in Table 2-4.

**Table 2-4** Security Requirements

| Security Category | Requirements |
|---|---|
| Physical | Must be in controlled environment conditions within a core computer room.<br>Must be housed within a secure data centre which includes:<br>• Only authorized personnel are allowed access. Authorized personnel will only be granted access after fingerprint screening is verified<br>• All authorized personnel have undergone a security scrutiny |
| Firewall | Must have redundant firewall protection, for example, Cyber Guard UNIX firewalls.<br>Provide secure transfer and storage of data.<br>Provide administrative options to customize security settings (explicit policy control). |
| Transport | Compatible with SSL-enabled web browsers and Transport Layer Security (TLS)<br>Provide 128-bit encryption for mail transfer between client and server. |
| Virus and Spam Protection | Provide Server Side Virus Scanning<br>Provide unrequested bulk email (UBE) control including the ability to add server side spam control with tiers of administration of the tool down to the user level<br>Provide the ability for the user to establish e-mail filters on the server based on sender, subject, etc.<br>Provide the ability for the user to choose all spam automatically deleted or quarantined by an administrator/user for a set period of time in a spam/junk mail folder. This folder would automatically empty at the administrator and/or user defined periods.<br>Provide the ability to have content filtering including the ability to add server side content filtering with tiers of administration of the toll down to the user level<br>Provide the ability to manage e-mail with white and black list functionality. White list functionality allows only selected senders to send e-mail, the remaining are filtered. Black list functionality disallows selected senders<br>Provide the ability for the user to establish individual or specific filters. |

**Table 2-4** Security Requirements *(Continued)*

| Security Category | Requirements |
|---|---|
| Backup And Recovery | All software and configuration will be backed up weekly or nightly incremental backups |
| | The operating system will be backed up weekly |
| | Backups will be stored for 2 weeks |
| Disaster Recovery | Provide a distributed architecture that will be housed in multiple data centers with failover capability |
| | Provide for a 3 day recovery in a disaster situation |
| Privacy | All data must be stored in a manner that follows applicable regulations, Telco's company security policies, and adheres to Telco's privacy policy |

Chapter 3

# The Architecture

A Java ES architecture is a high-level technical description of a Java ES solution.You develop an architecture to identify the combination of Java ES components and other technologies that will deliver the services described in your requirements. The architecture described in this chapter is based on the requirements described in Chapter 2, “The Requirements” on page 19.

An architecture is developed in two stages:

1. The deployment scenario. The deployment scenario identifies the Java ES components that provide the services described in the requirements, and, separately, lists the quality of service requirements.
2. The deployment architecture integrates the information in the deployment scenario. Where the deployment scenario simply identifies the components, the deployment architecture specifies how many instances of each component must be installed and configured, with what redundancy strategies, on what kind of hardware, and how the instances are distributed across the network, in order to provide the required services at the required quality of service level.

This chapter describes the Java ES architecture that Telco developed to satisfy their business and technical requirements. This chapter contains the following sections:

# The Deployment Scenario

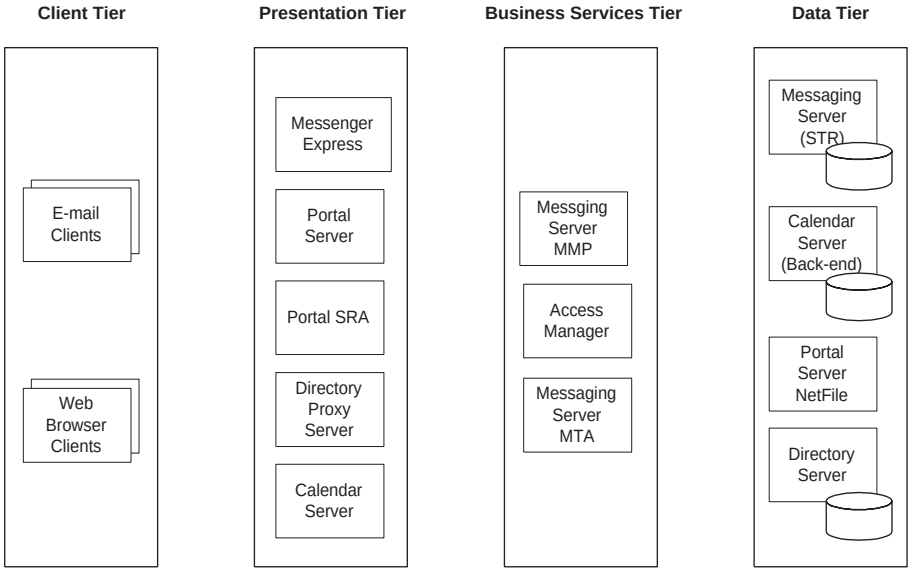
The deployment scenario for Telco's Java ES solution comprises the following:

- The logical architecture, which identifies the Java ES components needed to provide the services described in "Detailed Service Requirements" on page 20.
- The quality of service requirements, which specify the performance required from the Java ES component set.

## The Logical Architecture

The Java ES components needed to provide the services listed in "Detailed Service Requirements" on page 20 are displayed in Figure 3-1.

**Figure 3-1** Telco Deployment Logical Architecture

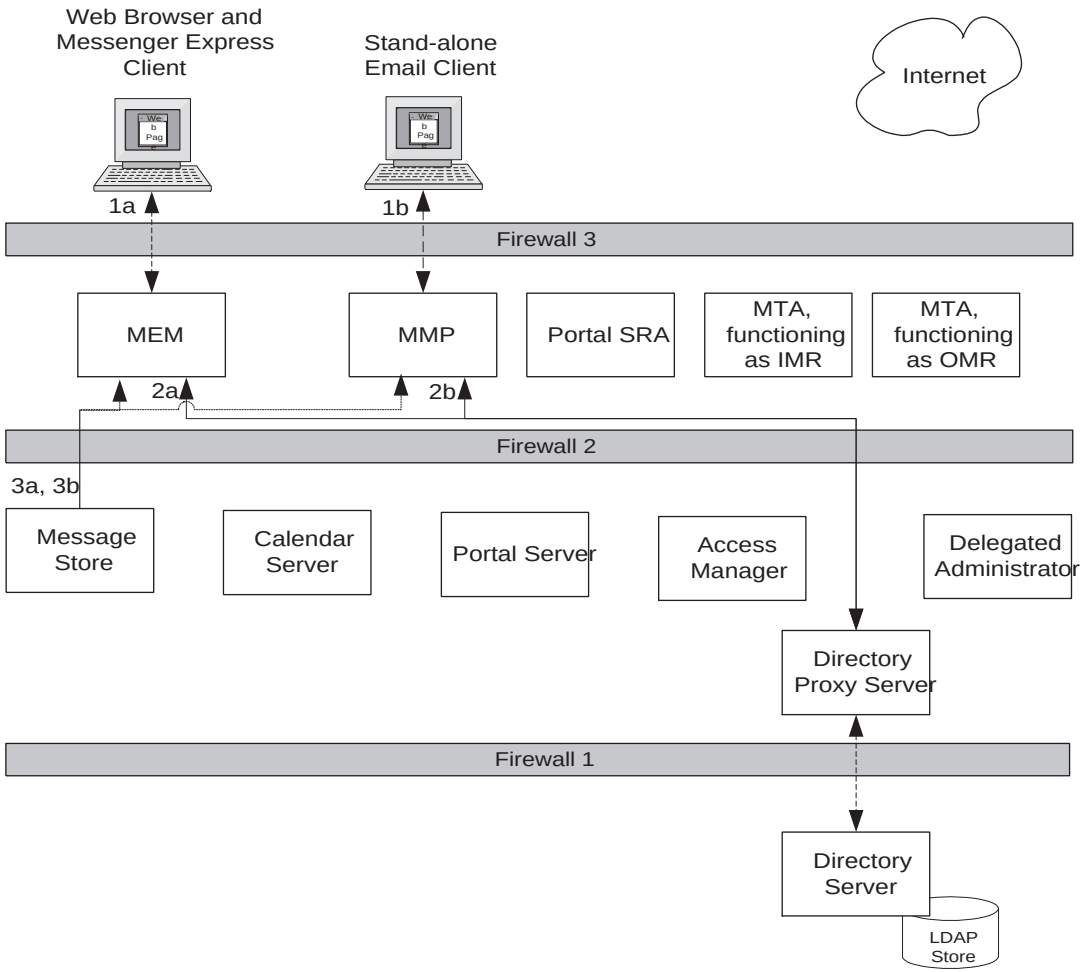



Notice that some basic design decisions are implied in Figure 3-1. The Messaging Server sub-components are to be deployed separately.

The main user interactions with this set of components are illustrated in Figure 3-2 on page 29, Figure 3-3 on page 31, Figure 3-4 on page 32, and Figure 3-5 on page 34. These figures show how the Java ES components in the proposed logical architecture deliver the specified services. As the design process continues, you analyze the component interactions represented in these figures, factor in the user base and usage patterns, and begin to make decisions about an architecture that supports these interactions with the specified quality of service.

Notice, too, that the security requirements are being considered at this stage of the analysis. The figures include proposed access zones for the deployment.

**Figure 3-2** User Login Interactions



The interactions shown in Figure 3-2 are the following:

**Step 1a** Messenger Express web browser-based client opens a connection to the Messenger Express Multiplexor (MEM). This is an HTTP connection. Notice that this is only for consumer-class customers; business-class customers have web browser access to email through the portal desktop. For more information see Figure 3-5 on page 34.

**Step 1b** Email client program opens a connection to Messaging Multiplexor (MMP). This is an IMAP connection.

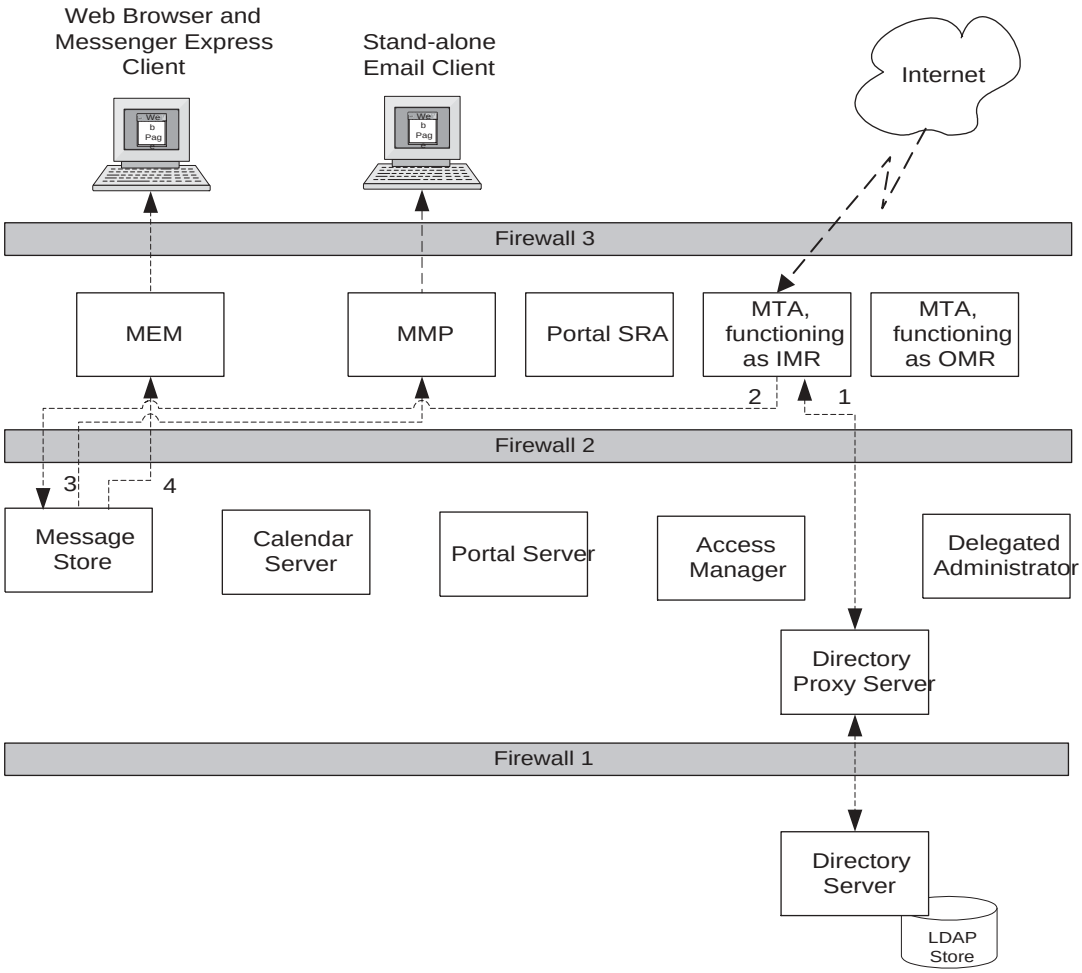
**Step 2a** The MEM connects to directory via directory proxy service and authenticates login ID and password against LDAP data.

**Step 2b** The MMP connects to directory via directory proxy service and authenticates login ID and password against LDAP data.

**Step 3a** If user is authenticated, the MEM connects to the HTTP server on the message store and transfers stored messages to the Messenger Express client.

**Step 3b** If user is authenticated, MMP connects to message store and transfers stored messages to the email client program.

**Figure 3-3** Incoming Mail Interactions




The interactions shown in Figure 3-3 are the following:

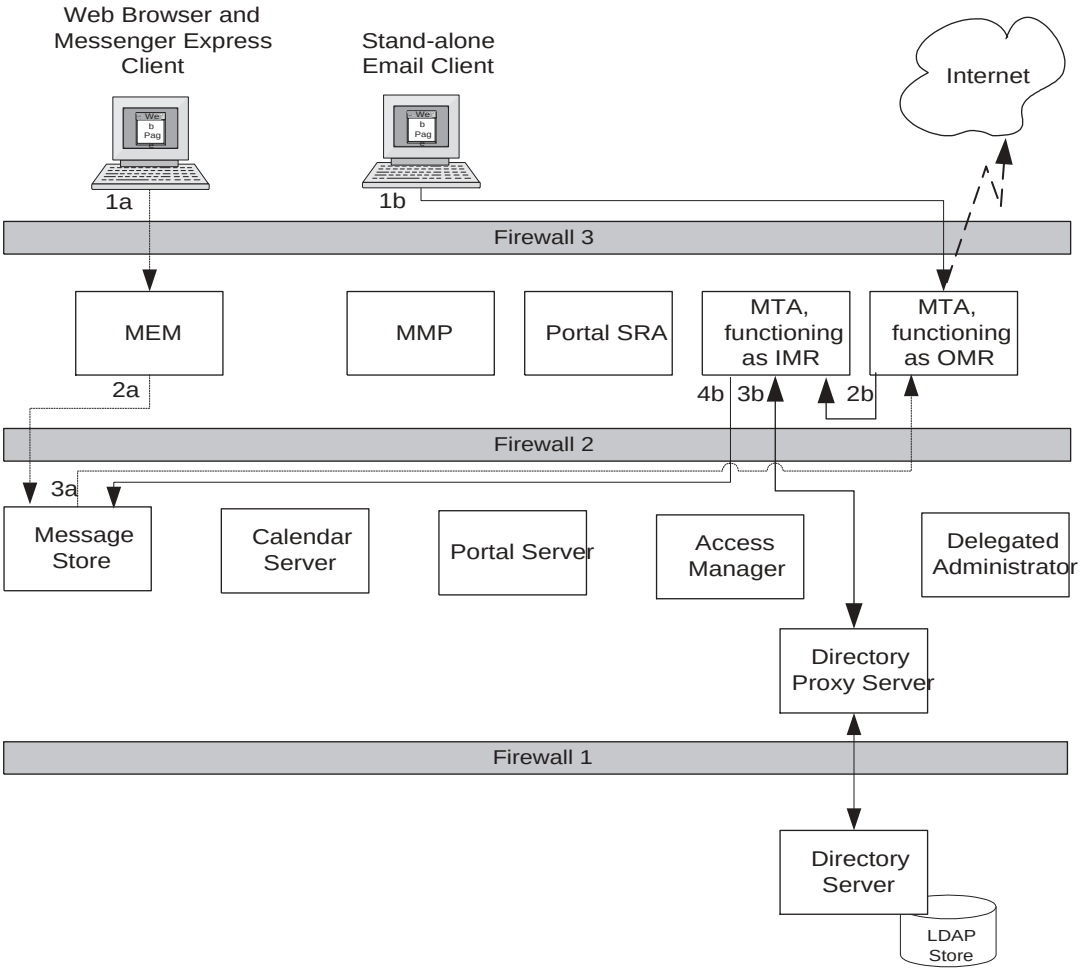
**Step 1** Incoming messages are delivered to an instance of the Messaging Server Message Transfer Agent (MTA) that is configured to serve as the incoming mail relay (IMR). The IMR verifies the addresses on incoming messages against the LDAP directory. The IMR also uses LDAP directory to determine correct message store instance for the address.

**Step 2** The IMR routes messages to the correct message store. This is a lightweight message transfer protocol (LMTP) connection.

**Step 3** If the user is logged in with an email client, the email client periodically polls the MMP to see if there are any new messages and fetches then into the client when requested to do so.

**Step 4** If the user is logged in with a web browser-based Messenger Express client, the MEM notifies the user when there are any new messages. The user can then view the message. The interaction between the web browser and the MEM is HTTP.

**Figure 3-4** Outgoing Mail Interactions



The interactions shown in Figure 3-4 are the following:

**Step 1a** The user composes a message in the Messenger Express mail client. The Messenger Express Client connects to the MEM. This is an HTTP connection.

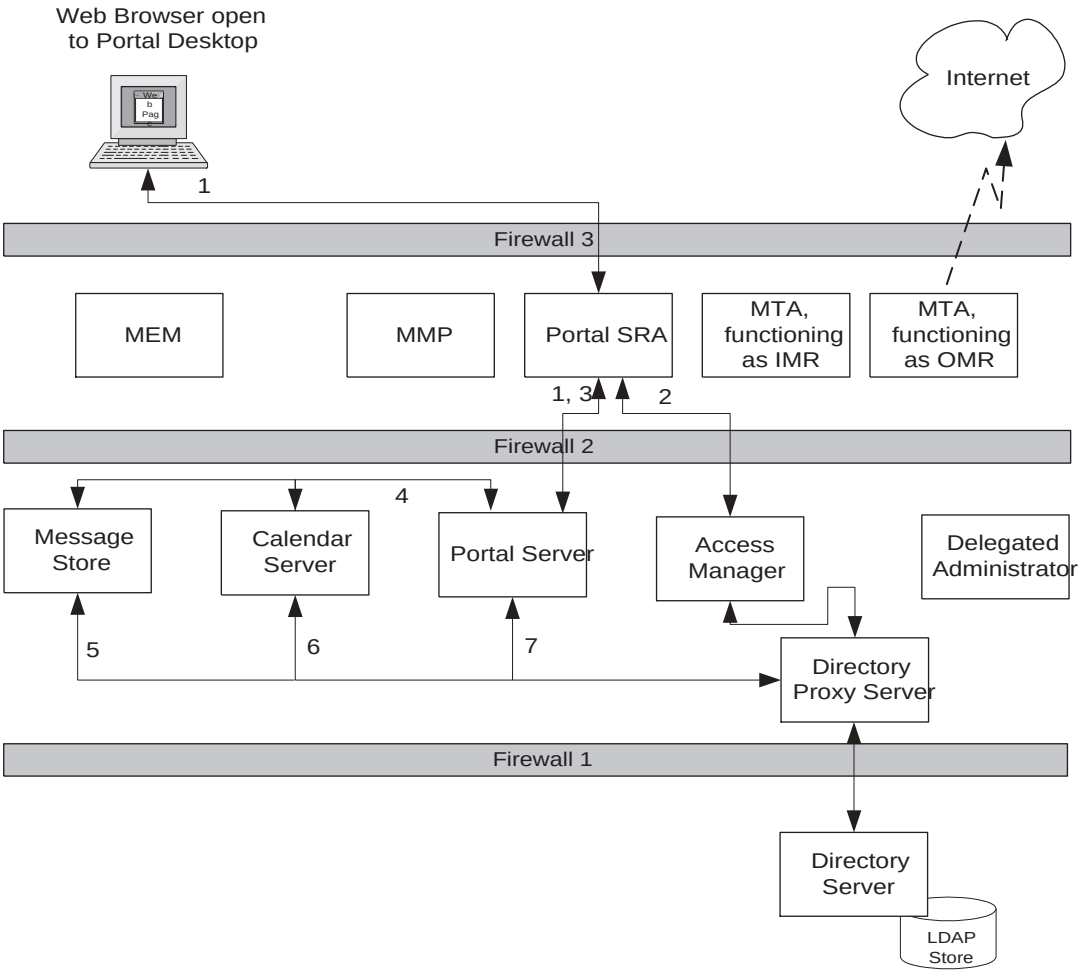
**Step 2a** The MEM routes the composed message to the HTTP server on the message store (the mshttpd).

**Step 3a** The HTTP server routes one copy of the message to the user's Sent folder and another copy to the Messaging Server Message Transfer Agent (MTA) that is configured to server as the outgoing mail relay (OMR). The OMR relays the message to the Internet.

**Step 1b** The user composes a message in the stand-alone email client program. The email client routes one copy of the composed message to the instance of the Messaging Server Message Transfer Agent (MTA) that is configured to server as the outgoing mail relay (OMR). This is an SMTP connection. The OMR relays the message to the Internet.

**Step 2b** The email client also routes another copy of the message, by way of the MMP, to the user's Sent mail folder.

**Figure 3-5** Portal Access Interactions




The interactions shown in Figure 3-5 are the following:

**Step 1** In a web browser, user opens the publicly accessible URL for portal desktop. This URL is actually a logical service name for the Portal Server Secure Remote Access service. Portal Server Secure Remote Access connects to Portal Server, obtains basic desktop page, relays basic desktop page to web browser. User sees User ID and password fields.

**Step 2** User supplies user ID and password. Portal Server Secure Remote Access connects to Access Manager for authentication. Access Manager connects to Directory Proxy Server service, and ultimately to Directory Server service, and authenticates the user ID and password. Access Manager returns single sign-on cookie to user's web browser session.

**Step 3** Portal Server Secure Remote Access contacts Portal Server with the single-sign on cookie.

**Step 4** In order to format user's desktop, Portal Server connects to Messaging Server and Calendar Server. Portal Server uses proxy authentication mechanism to open these connections.

**Step 5** Messaging Server obtains user's mail box location from LDAP directory. The Messaging Server also formats a summary display of the user's mail for the portal desktop mail channel. This is an IMAP and SMTP connection to the messaging back end.

**Step 6** Calendar Server obtains user's calendar preferences from LDAP directory. The Calendar Server also formats a summary display of the user's calendar for the portal desktop calendar channel. This is a WCAP connection.

**Step 7** Portal Server obtains user's display preferences from LDAP directory. Portal Server formats desktop page, relays desktop page to Portal Server Secure Remote Access, and ultimately, to user's web browser.

# The Quality of Service Requirements

The logical architecture identifies the Java ES components that provide the services specified in the requirements, but does not tell you how to install the components on your network. In a typical production deployment, quality of service requirements such as response time, service availability, and service reliability are satisfied by installing and configuring multiple instances of the components and distributing the components among several computers. For example, configuring two computers as cluster nodes, and then installing the Messaging Server back-end software on those computers provides fail-over capability and high availability for the messaging back-end service.

The quality of service requirements for the Telco deployment are described in the following sections:


- "Availability Requirements" on page 22
- "Performance Requirements" on page 22

# The Deployment Architecture

The deployment architecture integrates the information in the logical architecture and the quality of service requirements. The deployment architecture answers such questions as the following:

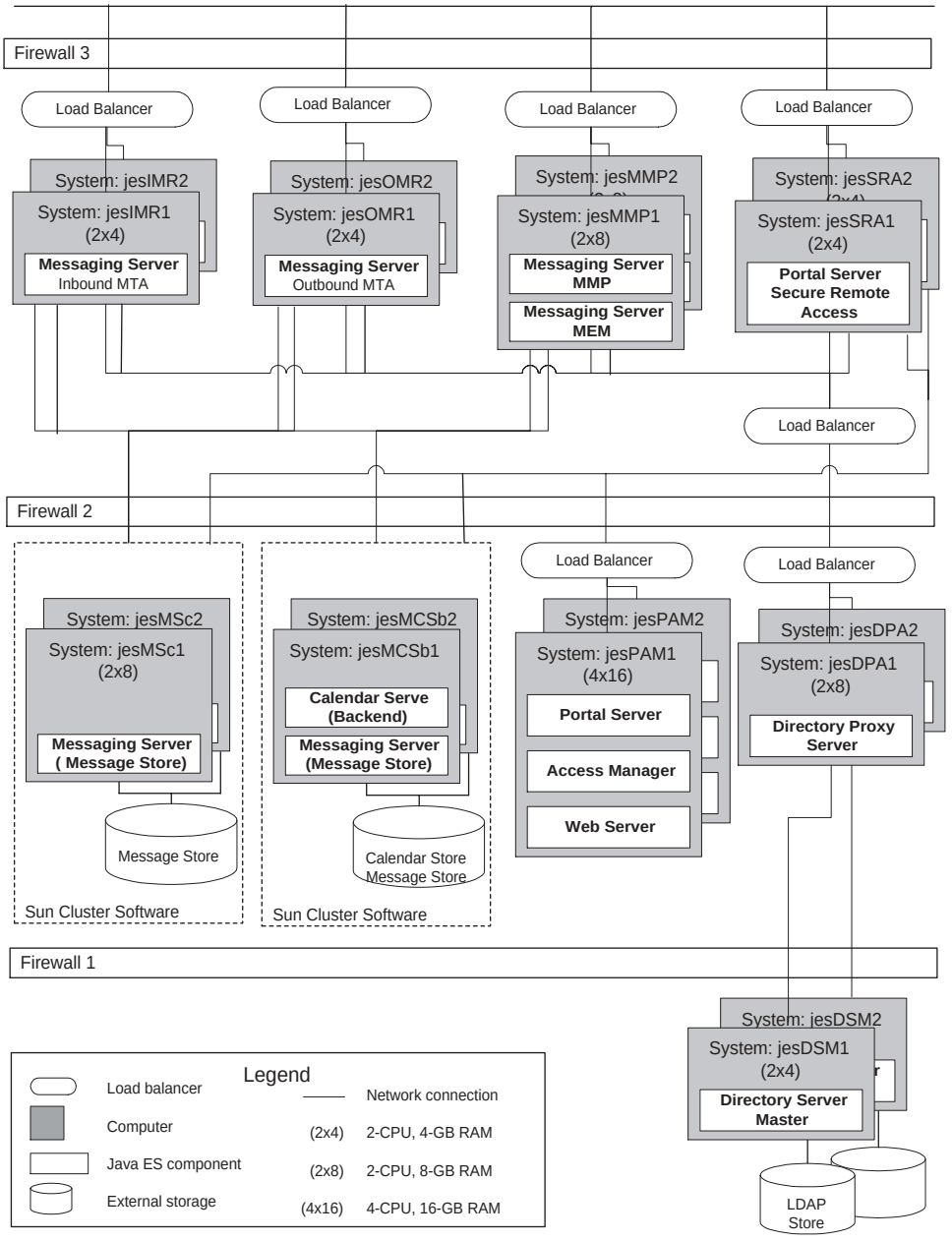
- Which redundancy strategies are you using to meet your availability and reliability requirements? (The main redundancy strategies available to you are installing and configuring multiple instances of a component and load balancing the instances to achieve availability and reliability, installing and configuring multiple instances of a component on Sun Cluster nodes to achieve availability and reliability, and using multiple instances of Directory Server that are synchronized through the multi-mastering and replication features to achieve availability and reliability.)
- How many instances of each component must be installed and configured in order to implement the redundancy strategies used in the solution?
- How are your component instances combined on your computers? For example, in a medium-sized solution, you could install and configure instances of both Messaging Server and Calendar Server on a single computer or cluster instance. In a larger solution with more user activity, you might install Messaging Server and Calendar Server on separate, dedicated computers to meet your performance requirements.
- How many CPUs are needed on each computer to achieve the performance specified in your quality of service requirements?

The answers to these questions lead to a deployment architecture for Telco.

The deployment architecture is the result of analyzing use cases and usage information and determining how the Java ES components can be installed to provide the specified services at the specified quality of services levels.

A deployment architecture is typically represented graphically, in a set of boxes that represent the computers in the deployment. Each box in the figure is labeled with the name of the computer and the components that are installed on the computer. The deployment architecture for the Telco deployment is illustrated in Figure 3-6.

**Figure 3-6** The Deployment Architecture



# Redundancy Strategies Used in the Architecture

The architecture in Figure 3-6 makes use of all three possible redundancy strategies for Java ES components. The redundancy strategies are chosen for the following reasons:

- Load balancing. This is the preferred solution for components that are stateless or mildly stateless, or for which instances of the component do not need to synchronize database updates. Load balancing uses redundant hardware and software components to distribute requests for a service among multiple components instances that provide the service, so that no single instance is overloaded. This redundancy also means that if any one instance of a components fails, other instances are available to assume a heavier load. Depending on the latent capacity built into this approach, failure might not result in significant degradation of performance. Load balancing is used for many components in the Telco architecture, for example the Portal Server and Access Manager components on jesPAM1 and jesPAM2.
- Sun Cluster software. This is the preferred solution for the back-end components that have read / write access to disk storage, namely the Messaging Server and Calendar Server components. In the Telco deployment, Sun Cluster software manages redundant hardware and software to provide failover for these components and for their access to disk storage. The Telco architecture makes use of Sun Cluster software on two separate back-end mail stores. The back-end mail store for business customers is on jesMCS1b and jesMCS2b, which function as a single logical host. The back-end mail store for consumer customers is on jesMS1c and jesMS2c, which also function as a single logical host.
- Directory Server Multimaster Replication. This is the preferred solution for Directory Server, which provides data that is crucial to the operation of the entire system. Multimaster replication is specifically designed for Directory Server and is therefore relatively easy to implement. The Telco architecture uses Directory Server multimaster replication for all Directory Server instances.

# Security Strategies Used in the Architecture

Telco provides mail and calendar services that are accessible to the public over the Internet. However, the network that provides mail and calendar services also runs other services that must not be compromised. The directory service, for example, has confidential data about Telco's employees, and similar confidential data about Telco's business and consumer class customers. (For more information, see."Security Requirements" on page 23.)

Telco's challenge is to develop an architecture that both provides the required publicly accessible services and secures the other services and resources that run on the same network. Telco assumes that the most significant threats would come from outside the local area network. Therefore, Telco's security strategy concentrates on preventing unauthorized outsiders from accessing the network at all, and preventing authenticated users from accessing any services or data they are not authorized to use.

The basic approach that Telco uses is to divide the network into access zones. The access zones are demarcated by firewalls. The firewalls and the access zones are shown in Figure 3-6.

In addition to the firewalls, Telco's plan includes a number of techniques and technologies that make it more difficult for would-be attackers to penetrate the firewalls and compromise the computers running the Java ES services.

The outermost zone in Figure 3-6 is the so-called de-militarized zone, or DMZ. The DMZ is reasonably secure. Each of the services behind the firewall can only be accessed at a specific URL. For example, business users who connect to the portal service access the service at https://www.telcomail.com:80. The firewall blocks all other ports and addresses. The firewall also imposes similar restrictions for accessing the other services in the DMZ, the messaging multiplexor and the mail relay services.

In addition to being deployed behind Firewall #3, the four Java ES services that are exposed to the internet are protected in the following ways:

- The services require users to authenticate themselves. For example, users who open www.telcomail.com in their web browsers are presented with a login page. The MMP and the mail relay services impose similar restrictions for access.
- The computers that provide these services are behind hardware load balancers. The load balancers provide a single point of contact for each service, regardless of how many component instances are running on how many computers. This means that for each service there is only one hole in the firewall, and all of the traffic for that service is routed through the load balancer.

- Access control features in the Java ES components. For example, access control rules are established for the Directory Proxy Server instances running on jesDPA1 and jesDPA2. Only traffic from the trusted proxy group (192.168.11.0 255.255.255.0 quad) is allowed to access the directory proxy servers through the load balancer. Any other traffic is blocked in the software.
- Not shown in Figure 3-6, but implied in the deployment architecture, is a network topology defined by private IP addresses. These private IP addresses define subnets that are invisible to the outside world. These subnets are connected only through the load balancers, further impeding the ability of intruders to see the actual computers behind the public URLs.
- Also not shown in Figure 3-6, the individual computers and running the Java ES services are hardened.

Figure 3-6 indicates where Firewalls 1 and Firewall 2 are placed in order to define the inner zones. Figure 3-6 also indicates some of the additional measures that Telco uses to further secure the inner zones.

- The only openings in Firewall 2 are those shown in Figure 3-6. Notice that these are connections from trusted private IP addresses.
- Firewall 2 is established with different hardware, from a different manufacturer, than Firewall 3. This ensures that an intruder who recognized Firewall 3, and was able to exploit a known weakness, would not be able to repeat the same exploit on Firewall 2.
- The actual portal service is provided by Portal Server instances in Zone 2. These instances are protected by the Portal Server Secure Remote Access service in Zone 3. All access to the portal service is through the Portal Server Secure Remote Access service. This aspect of the architecture allows the portal service to reside behind an additional firewall and an additional layer of hardware load balancers.
- The computers that provide these services in Zone 2 are also behind hardware load balancers, establishing a single point of contact for each service in Zone 2, a minimizing the openings in Firewall 2.
- The computers in Zone 2 are on a different subnet from the computers in Zone 3, which is defined by private IP addresses. The only bridges between the subnets are the hardware load balancers. The load balancers in zone 2 accept connections only from the load balancer in zone 3, and the firewall also rejects other connections.
- The individual computers running the Java ES services in Zone 2 are hardened.

Zone 1 is the most secure, and contains the directory service. In addition to Firewall 1, Zone 1 is protected by the following measures:

- There is no direct access to the Directory Server instances. All access is through the Directory Proxy Server instances in Zone 2. The directory service only accepts requests that originate with the directory proxy service.
- Firewall 1 only allows traffic from the Directory Proxy Server instances. All other traffic is blocked.
- Firewall 1 is established with different hardware, from a different manufacturer, than either Firewall 2 or Firewall 3.
- The individual computers running the directory services in Zone 1 are hardened.

For more information of the implementation of this security strategy see, "The Network and Connectivity Specification" on page 46.

# Planning for Scalability in the Architecture

The Messaging Multiplexor (MMP) and Messenger Express Multiplexor (MEM) are both capable of handling incoming client connections that are routed to multiple back-end mail stores. In the architecture illustrated in Figure 3-6, the MMP and MEM instances are co-located on computers jesMMP1 and jesMMP2. Depending on whether incoming client connections are business or consumer customers, they are routed to one of two back-end message stores.

This architecture could be scaled to handle more incoming connections in several ways:

- The user base is currently divided into business users and consumer users, and each group is assigned to its own message store. (Note that each message store is actually comprised of multiple instances represented by a logical host.) As the number of users grows, the user accounts could be divided into more groups (for example, divide the consumer users alphabetically or by location), and the number of computers running message store instances could be increased. The architecture would remain essentially the same, but the MMP and MEM would be distributing a greater number of incoming connections among a greater number of back-end message store instances. The load on each message store instance would remain constant.
- The MMP and MEM instances could be installed on separate computers, giving each instance more computing resources.

Chapter 4

# The Deployment Specifications

The deployment specifications comprise a technical description of a Java ES solution that is more detailed than the deployment architecture. The deployment specifications are based on the architecture, but they add more of the detailed information that is needed to install and configure the set of components identified in the architecture.

This chapter covers the deployment specifications for Telco's deployment in the following sections:



## The Computer Hardware and Operating System Specification

The computer hardware and operating system specification describes the operating system and hardware configuration required for each computer used in the deployment. The hardware chosen depends on the components installed on the computer and the level of performance required from the components. All computers used in the Telco deployment run the Solaris 10 operating system.

The computer hardware and operating system specification for Telco's deployment is shown in Table 4-1.

**Table 4-1** Computer Hardware and Operating System Specification

| Computer | Component Subsystem | Description | Hardware Model | Installation Module |
|---|---|---|---|---|
| jesDSM1 | Directory Server, Administration Server | Directory Server with Multimaster Replication | SunFire V240, 2 x 1GHz UltraSPARC III | 1A and 1B, in "Module #1: Directory Server with Multimaster Replication" |
| jesDSM2 | Directory Server, Administration Server | | SunFire V240, 2 x 1GHz UltraSPARC III | |
| jesDPA1 | Directory Proxy Server | Load Balanced Directory Proxy Server | SunFire V240, 2 x 1GHz UltraSPARC III | "Module #2 Directory Proxy Server" |
| jesDPA2 | Directory Proxy Server | | SunFire V240, 2 x 1GHz UltraSPARC III | |
| jesPAM1 | Portal Server, Access Manager, Web Server | Load Balanced Portal Server and Access Manager | SunFire V480, 2 x 1.05GHz UltraSPARC III | "Module #3: Portal Server and Access Manager on Web Server" |
| jesPAM2 | Portal Server, Access Manager, Web Server | | SunFire V480, 2 x 1.05GHz UltraSPARC III | |
| jesMCS1b | Messaging Server, Calendar Server, Administration Server, Sun Cluster software | Clustered Messaging Server and Calendar Server for business class customers | SunFire V480, 2 x 1.05GHz UltraSPARC III | "Module #5: Business-class Messaging Server and Calendar Server on Sun Cluster Nodes" |
| jesMCS2b | Messaging Server, Calendar Server, Administration Server, Sun Cluster software | | SunFire V480, 2 x 1.05GHz UltraSPARC III | |

**Table 4-1** Computer Hardware and Operating System Specification *(Continued)*

| Computer | Component Subsystem | Description | Hardware Model | Installation Module |
|---|---|---|---|---|
| jesMS1c | Messaging Server, Administration Server, Sun Cluster software | Clustered Messaging Server for consumer class customers | SunFire V480, 2 x 1.05GHz UltraSPARC III | "Module #6 Consumer-class Messaging Server on Sun Cluster Nodes" |
| jesMS2c | Messaging Server, Administration Server, Sun Cluster software | | SunFire V480, 2 x 1.05GHz UltraSPARC III | |
| jesSRA1 | Portal Server Secure Remote Access | Load balanced Portal Server Secure Remote Access | SunFire V480, 2 x 1.05GHz UltraSPARC III | "Module #7 Portal Server Secure Remote Access" |
| jesSRA2 | Portal Server Secure Remote Access | | SunFire V480, 2 x 1.05GHz UltraSPARC III | |
| jesADM | Delegated Administrator, Web Server | Delegated Administrator for user management | SunFire V240, 2 x 1GHz UltraSPARC III | "Module #8 Delegated Administrator Console on Web Server" |
| jesIMR1 | Messaging Server (MTA) | Load-balanced incoming message relay | SunFire V240, 2 x 1GHz UltraSPARC III | 9A, in "Module #9: Load Balanced Messaging Server MTA (Inbound and Outbound)" |
| jesIMR2 | Messaging Server (MTA) | | SunFire V240, 2 x 1GHz UltraSPARC III | |
| jesOMR1 | Messaging Server (MTA) | Load-balanced outgoing message relay | SunFire V240, 2 x 1GHz UltraSPARC III | 9B, in "Module #9: Load Balanced Messaging Server MTA (Inbound and Outbound)" |

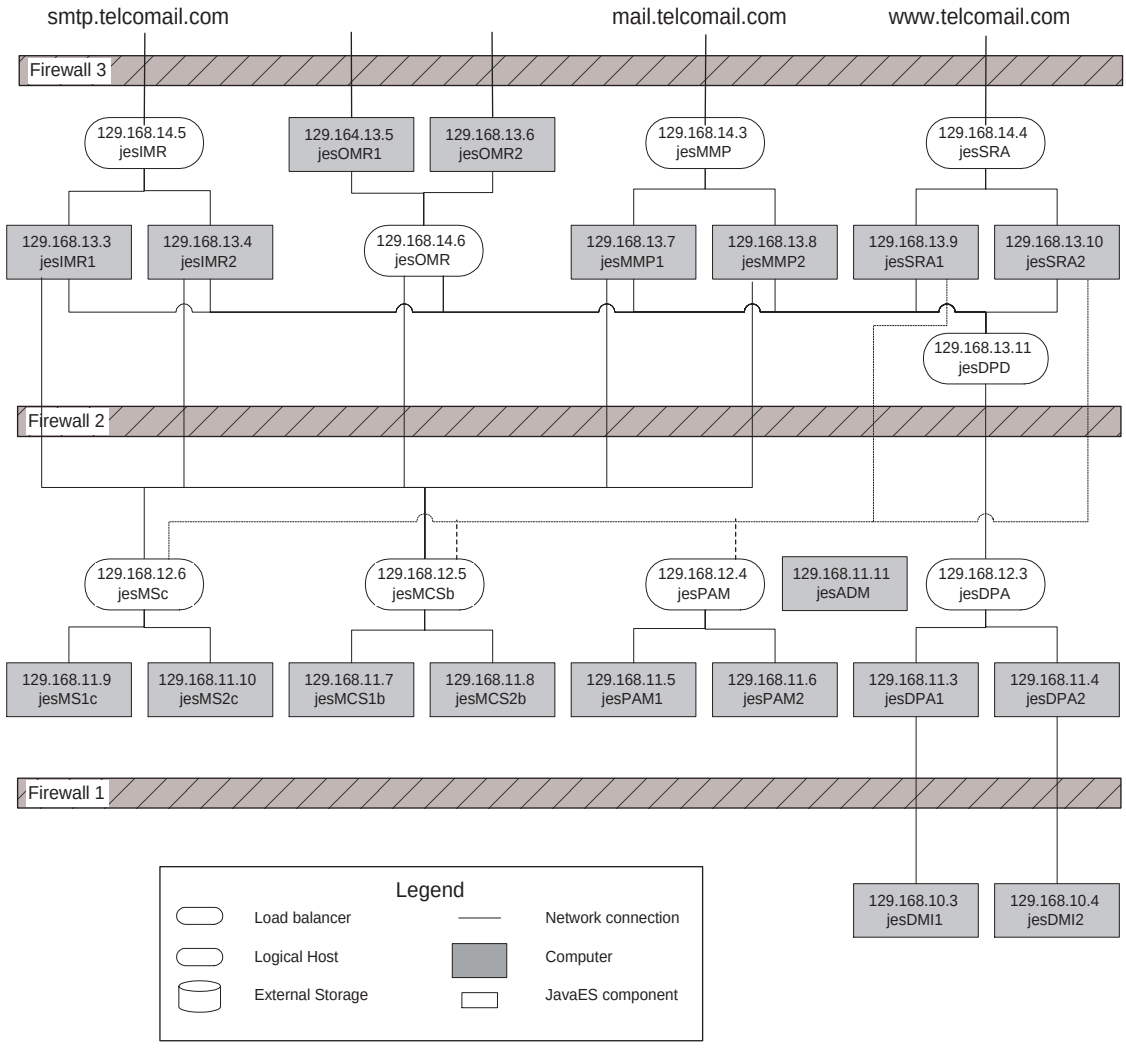
**Table 4-1** Computer Hardware and Operating System Specification *(Continued)*

| Computer | Component Subsystem | Description | Hardware Model | Installation Module |
|---|---|---|---|---|
| jesOMR2 | Messaging Server (MTA) | | SunFire V240, 2 x 1GHz UltraSPARC III | |
| jesMMP1 | Messaging Server (MMP) | Load-balanced MMP and MEM for mail client access | SunFire V240, 2 x 1GHz UltraSPARC III | "Module #10: Load Balanced Messaging Server MMP and MEM" |
| jesMMP2 | Messaging Server (MMP) | | SunFire V240, 2 x 1GHz UltraSPARC III | |

# The Network and Connectivity Specification

The network and connectivity specification describes all of the network connections needed to implement the architecture. The network and connectivity specification for Telco's deployment is displayed graphically in Figure 4-1.

**Figure 4-1** Network and Connectivity Specification




The network topology in Figure 4-1 implements the security strategy described in “Security Strategies Used in the Architecture” on page 39. Figure 4-1 shows the private IP addresses that establish the multi-layer network topology.

Each computer and load balancer tier is on separate sub-net. As shown in figure Figure 4-1 there are effectively 5 layers of computers.

In terms of access from the Internet only the load balancers in Zone 3 (sub net 129.168.14.x) are actually exposed, at the URLs shown in Figure 4-1. Everything else, according to the philosophy of minimizing the surface of attack, is hidden, through use of private IP addresses.

Since the DMZ contains the computers that are accessed by the public, the IP addressing scheme for the load balancers jesIMR, jesOMR, jesMMP and jesSRA are normal IP addresses, which are accessible from the Internet. The IP address shown for these load balancers in Figure 4-1 are 129.168.14.xx. When you set up these load balancers, however, you should replace these addresses with the real, publicly accessible, addresses for your company.

All of the other hardware is assigned 129.168.13.xx IP addresses, which are private addressees. These private addressees are not recognized by the Internet and are not routed outside.

The load balancers bridge the subnets, and route communications between the subnets. That means that the load balancers control the traffic between the sub nets. Therefore, if one layer is compromised there is no direct route to the next layer.

Web access is restricted to HTTPS (SSL) when accessing the load balancer for the SRA gateways. In practice proper certificates would be used rather than the self-signed, self-generated ones used in this example.

# The User Management Specification

Installing and configuring a Java ES solution establishes both the LDAP schema and the basic tree structure of the LDAP directory for the deployment. Specifications for the schema and the directory tree structure must be developed before installation begins, so that the correct values can be input during the installation and configuration process. This section specifies the schema and the directory tree for the Telco deployment. It also describes how the directory schema and the directory tree structure for the Telco deployment are established by the installation and configuration process.

# The LDAP Schema

The Java ES installation and configuration process both establishes the LDAP schema for the deployment. The LDAP schema is constructed in stages, by the Java ES installer, several of the configuration tools, and the Delegated Administrator administration tool.

With Java ES solutions in general, you need to specify the LDAP schema before you install and configure, so that you can select the correct installation and configuration parameters. This section describes the LDAP schema for the Telco deployment.

The schema for the Telco deployment must support the following services:

- Access Manager authentication and single sign-on
- Messaging, calendar, portal, and NetFile (file access) services
- Proxy authentication for business users who access mail and calendar through their portal desktops

The schema for the Telco deployment is constructed by the following steps of the installation and configuration process:

1. Apply schema 2 to the directory.

   Java ES solutions that use Directory Server can use either of two versions of a Sun standard LDAP schema for messaging and calendaring, which are known as Schema 1 and Schema 2. Schema 2 natively supports Access Manager and Access Manager's single sign-on feature.

   The Telco deployment uses Access Manager and the single sign-on feature, so the Directory Server instances in the deployment is configured for Schema 2.

   To configure a Directory Server instance for Schema 2, you do the following:

   a. Install and configure the necessary Directory Server instances.

   b. Install Access Manager and specify the Directory Server instance that Access Manager will be using. Installing Access Manager automatically updates the directory schema. Note that the Directory Server instances must be installed before Access Manager, and the Directory Server instances must be up and running while Access Manager is installed.

   c. Run the Directory Preparation Tool, and restart Directory Server instances. This completes the preparation of the overall schema.

2. Use the Delegated Administrator tool (either the console or the command line utility) to add object classes and attributes to the individual LDAP organizations that hold the user data (These organizations are described in "The Directory Tree Structure" on page 50.) Specifically, you add the following:

    a. To the LDAP organization for the business class customers, you add object classes and attributes that support messaging, calendar, portal and file access services.

    b. To the LDAP organization for the consumer class customers, you add object classes that support messaging services.

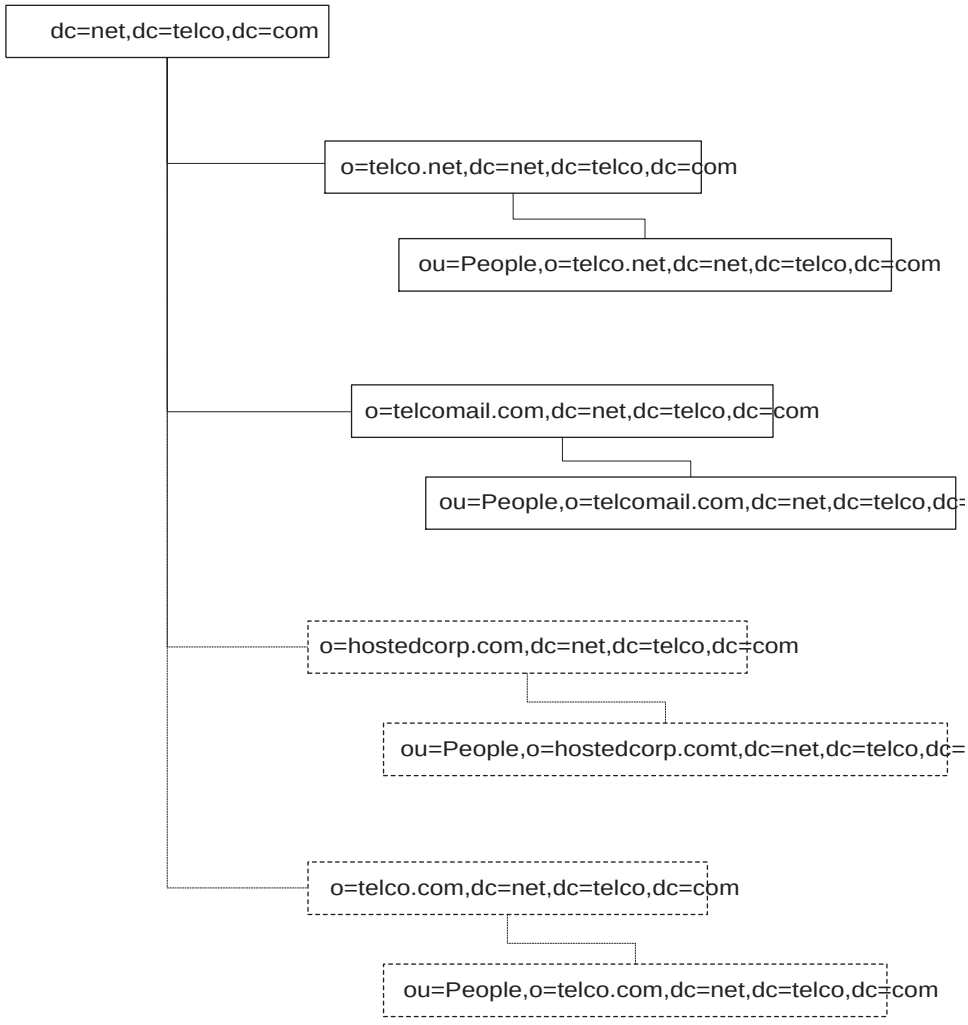
The installation and configuration plan for the Telco deployment includes all of these steps in the proper sequence. For more information, see "The Installation and Configuration Plan" on page 55.

# The Directory Tree Structure

The LDAP directory for a Java ES solution can be simple or complex, depending on the organization's needs for organizing user data. LDAP directories, are, by their nature, flexible in structure. Java ES does not require any particular structure, but you do use the installation and configuration process to implement the specified structure.

The LDAP directory for the Telco deployment must support Telco employees, consumer users, business users who use Telco's domain name, and business users that use the hosted domain service. The directory structure developed to support this requirement is illustrated in Figure 4-2.

**Figure 4-2** LDAP Directory Tree for the Telco Deployment




In Figure 4-2 the directory tree root is dc=net,dc=telco,dc=com. The tree has the following branches:

- **o=telco.net** This branch is for consumer class customers. This branch is provisioned for mail services only. The data for consumer class customers is stored in ou=People,o=telco.net,dc=net,dc=telco,dc=com.

- **o=telcomail.com** This branch is for business class customers that do not use the hosted domain service. This branch is provisioned for mail, calendar, portal, and file access services.
- **o=hostedcorp.com** This branch is for a business customer named hostedcorp that is using the hosted domain service. This branch is provisioned for mail, calendar, portal, and file access services.
- **o=telco.com** This branch is for Telco employees. This branch is provisioned for mail, calendar, portal, and file access services.

Chapter 5, "The Installation and Configuration Plan," explains how the installation and configuration process builds the directory tree. Chapter 6, "Software Installation and Configuration Procedures," contains instructions for creating and provisioning the o=telco.net and o=telcomail.com branches. The branches for hosted domains and internal users can be created by varying the instructions slightly.

## The Administrator Accounts

In addition to setting up the basic structure of the LDAP directory, installing and configuring a Java ES deployment establishes a number of administrator accounts. For each component that you install and configure, the installer or configuration program creates one or more administrator accounts.

The installation and configuration instructions in this document create the following administrator accounts:

- **Directory Server** The administrator account name is admin, and the administrator password is password. The LDAP DN for the administrator account is uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot. You also create a Directory Manager account. The Directory Manager account name is cn=Directory Manager and the password is password. Other components use the Directory Manager account to access the directory at installation or configuration time.
- **Administration Server** The administrator account name is admin, and the administrator password is password. The LDAP DN for the administrator account is uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot.
- **Access Manager** The administrator user account is amadmin, and the administrator password is password. The LDAP DN for the administrator account is uid=amadmin,ou=People,dc=net,dc=telco,dc=com.

- **Portal Server** The administrator account is amadmin and the password is password.
- **Portal Server Secure Remote Access** The Portal Server Secure Remote Access core runs on jesPAM1 and jesPAM2. The administrator account for this instance is amadmin and the password is password. The Portal Server Secure Remote Access gateway runs on jesSRA1 and jesSRA2.
- **Web Server** The administrator account name is admin, and the administrator password is password.
- **Messaging Server** There are two administrator accounts, one for the consumer class service and one for the business class service. The administrator account name for the consumer class service is admin_telco.net, and the administrator password is password. The LDAP DN for this administrator account is uid=admin_telco.net,ou=People,o=telco.net,dc=net,dc=telco,dc=com. The administrator account name for the business class service is admin, and the administrator password is password. The LDAP DN for this administrator account is uid=admin,ou=People,o=telcomail.com,dc=net,dc=telco,dc=com.
- **Calendar Server** The administrator account name is calmaster, and the administrator password is password. The LDAP DN for the administrator account is uid=calmaster,ou=People,o=telcomail.com,dc=net,dc=telco, dc=com.
- **Delegated Administrator** The Telco deployment installs the Delegated Administrator server-side component on jesPAM1. The administrator account ID is admin and the password is password. The Telco deployment also installs the Delegated Administrator console on jesADM. The administrator account name for this instance is admin and the administrator password is password.

Chapter 5, “The Installation and Configuration Plan,” explains how the installation and configuration process creates the administrator accounts. Chapter 6, “Software Installation and Configuration Procedures,” contains installation and configuration input values for creating the administrator accounts.

If you adapt the instructions in this document for your own solution, you should consider your security requirements and develop a plan for your administrator accounts and administrator passwords.

# The Delegated Administrator Instance

Delegated Administrator is the Java ES tool for managing the directory tree. Chapter 6, “Software Installation and Configuration Procedures,” contains instructions for using the Delegated Administrator server side component in command line mode to create the directory tree branches described in “The Directory Tree Structure” on page 50 and to create test user accounts.

This document also contains instructions for installing and configuring the Delegated Administrator console. For information on using the Delegated Administrator console, see the Delegated Administrator documentation.

Chapter 5

# The Installation and Configuration Plan

The goal of the installation and configuration process is the distributed system described in the deployment architecture. The distributed system is composed of component instances that run on multiple computers and interoperate with each other. To achieve a functioning distributed system, you must install the component instances on multiple computers and perform the basic configuration required to establish interoperation among the component instances.

To ensure that you achieve a functioning distributed system, you must develop an installation plan that uses the installer appropriately and considers the requirements of the components in the deployment. Your plan must describe the correct order for installing the component instances and performing basic configuration. The plan must also specify the configuration values that configure the components to interoperate.

This chapter describes the installation and configuration plan for the Telco deployment.

## Installation and Configuration Issues

You install Java ES components with the Java ES installer. The installer is able to configure some of the Java ES components at installation time. The other components are configured by running separate configuration tools after installation is complete.

Your installation and configuration procedures depend on the following factors:

- Installer Behavior
- Component Dependencies

- Distributed Subcomponents
- Component Redundancy
- LDAP Directory Tree

Each of these factors is described in the following sections.

# Installer Behavior

The Java ES installer uses Solaris pkgadd to transfer Java ES software to your computer system. The installer can install any number of Java ES components during a single installation session. The installer does not perform distributed installations. Therefore, to install and configure Java ES components on multiple computers, as called for in the Telco deployment architecture (Figure 3-6 on page 37), you must run the installer on each computer used in your deployment until all of the components have been installed and configured.

## Distributed Installations

The quality of service requirements for Java ES solutions lead to architectures that place component instances on more than one computer. For example, the Telco deployment achieves a reliable portal service by installing two instances of Portal Server on two computers (jesPAM1 and jesPAM2) and using a load balancer to establish a failover relationship between the two instances.

The Java ES installer, however operates on only one computer at a time. Therefore, when you install a distributed solution you must run the installer on every computer used in the solution.

In many cases you must install a component or components on a computer and then run a configuration tool to perform the basic configuration of the component. For example, in the Telco deployment, on the computer jesIMR1, you run the installer to install the Messaging Server software, and then you run a Messaging Server configuration program to configure an instance of the Message Transfer Agent.

## Configuring for Interoperation

The goal of the installation process is a set of interoperating component instances. When you install components and perform basic instance configuration, you supply configuration values that result in component instance interoperation.

The configuration values that result in interoperation include such values as the URLs or port numbers that one component instance uses to communicate with another component instance and the administrator account IDs and password that one component instance uses to gain access to another component instance. For example, in the Telco deployment, the Access Manager instances must communicate with the Directory Server instances, so you configure the Access Manager instances with the URLs, administrator account ID, and password for the directory service instances in the deployment.

When you run the Java ES installer, it does not know what components are installed on other computers used in the deployment. For example, when you install Access Manager, the installer does not know where the appropriate LDAP directory is located. To ensure the success of your installation and configuration process, you must plan ahead and develop the information that you need to configure each component instance. For example, when you configure the Access Manager instances on jesPAM1 and jesPAM2, you will need the URLs, administrator IDs, and administrator passwords for the jesDPA directory service.

## Configure Now and Configure Later

The Java ES installer is capable of configuring runnable instances of some components. To use the installer this way, you must run the installer in “configure now” mode and supply the necessary configuration values.

For components that cannot be configured at install time, you run the installer in configure later mode. After installation is complete, you run a configuration program for each component instance you are creating. For example, in the Telco deployment, on MCS1b, you run the installer in configure later mode to install Messaging Server and Calendar Server software. Then you run the Messaging Server configuration program to create an instance of the Message Store. Then you run the Calendar Server configuration program to configure and instance of the calendar store.

When you plan how to install and configure a solution, you need to plan the correct sequence of running the Java ES installer and running the configuration programs.

The installation and configuration plan for the Telco deployment uses the configure now option whenever it is possible to do so.

# Component Dependencies

Some Java ES components cannot be installed and configured unless other components are installed and configured first. Dependencies occur for several reasons:

- Some components cannot function unless certain other components are installed and configured. For example, Portal Server Secure Remote Access functions as a gateway for a specific Portal Server instance. The configuration process for Portal Server Secure Remote Access requires input of URLs that enable Portal Server Secure Remote Access to interoperate with an already functioning Portal Server. Because of this dependency, Portal Server must be installed, configured, and running before Portal Server Secure Remote Access is installed and configured. In the Telco installation plan, this type of dependency determines the installation sequence for the Portal Server and Portal Server Secure Remote Access instances.
- A number of components require an LDAP directory for authentication and authorization. When you install and configure instances of these components you input the URL for the LDAP directory service. Because of this dependency, Directory Server must be installed and configured before the components that use the LDAP directory service. In the Telco installation plan, Directory Server is the first component installed and configured.
- Some components modify the configuration of an existing component. For example, installing and configuring Access Manager modifies the LDAP directory schema. If your solution uses Access Manager, you must plan to install and configure Directory Server before you install and configure Access Manager. In the Telco installation plan, Access Manager instances are installed and configured after the Directory Server instances.
- A number of Java ES components are web applications. These components must be deployed into web containers to function. The Telco deployment uses Web Server as a web container. The Java ES installer can install Web Server and the web application component in one installation session and automatically deploy the component to Web Server. This is how the components on jesPAM1 and PAM2 are installed.
- Java ES components can be installed in a high-availability cluster provided by Sun Cluster software. The Sun Cluster software must be installed and running before the other components are installed and configured. Then, after the Java ES components are installed and configured, you must install and configure the appropriate Sun Cluster agents for the Java ES components. In the Telco installation plan, this is how the components on jesMCS1b, jesMCS2b, jesMS1c, and jesMS2c are installed and configured.

The Telco deployment has examples of all these types of dependency.

Notice that some of these dependencies are solution-wide and some are local. You consider solution-wide dependencies and local dependencies differently when you plan how to install and configure a solution. The difference is described in the following example:

- The dependency of Access Manager on Directory Server is a system-wide dependency. When you install Access Manager, you supply a URL for a directory service that is provided by one more instances of Directory Server. Once Directory Server is installed and configured, the directory service is available to all components in the solution. This type of dependency is determines the system-wide sequence for installing and configuring component instances: the computers running Directory Server are installed and configured before the computers running Access Manager. System-wide dependencies determine the overall sequence of installation and configuration steps.
- The dependency of Access Manager on a web container is a local dependency. To satisfy this dependency, a web container must be installed on the computer that runs Access Manager. This web container, however, does not provide services for the entire solution. In a distributed solution, web containers are typically installed on multiple computers. You do not install a single web container that supports the entire deployment. You install web container instances where they are needed locally. Each web container supports a different component locally. Therefore, in a distributed solution there is no single location for web container installation, and there is no single point in the installation procedure installing the web container.

To develop an installation plan, you analyze the deployment architecture and identify the dependencies among the components. Your plan must install and configure the components in a sequence that satisfies all of the dependencies. In general, you can develop an overall sequence of installation steps from the solution-wide dependencies. Then you consider the local dependencies that might exist on each computer.

## Distributed Subcomponents

Some Java ES components have subcomponents that can be separately installed and configured. For example, Messaging Server has four subcomponents, the Message Transfer Agent (MTA), the Message Multiplexor (MMP), Messenger Express Multiplexor (MEM), and Message Store. If the deployment architecture calls for these subcomponents to be installed on different computers, you must run the installer on each computer, in the correct sequence, and configure the subcomponents to interoperate.

The Telco deployment architecture places the Messaging Server subcomponents on separate computers to satisfy quality of service requirements. The Telco installation and configuration plan describes the correct sequence for installing and configuring these subcomponents.

## Component Redundancy

The sequence of installation sessions and configuration procedures depends on how redundancy is being used in a deployment architecture. Redundancy can be used to achieve high availability, scalability, serviceability, or any combination of these service qualities. There are three technologies for using redundant components in the Java ES Telecommunications Provider architecture: load balancing, Sun Cluster, and Directory Server multimaster replication. Each has recommended configuration procedures that affect the sequence of installation sessions, as outlined briefly in the following paragraphs:

- Load balancing is best set up by installing and configuring one instance of a load-balanced component, testing that the service provided by the instance is accessible through the load balancer, and then installing and configuring additional instances of the same component. This phased approach facilitates troubleshooting of configuration problems.
- Sun Cluster software is set up by first installing the Sun Cluster core software on all cluster nodes before installing other components. For the Telco architecture, for example, Sun Cluster core must be installed and configured before installing and configuring Messaging Server and Calendar Server on the cluster nodes. Likewise, Messaging Server and Calendar Server must be configured before Sun Cluster agents are configured.

- Directory Server multimaster replication is best implemented by first installing and configuring one of the multimaster replicas, then installing and configuring all components that depend on Directory Server. Once such installations and configurations are completed, replicas of Directory Server can be installed and the system configured to provide synchronization and failover.

Each of these redundancy implementations implies a specific scoping and sequencing of installation sessions and configuration procedures.

## LDAP Directory Tree

Installing and configuring a Java ES solution requires configuration values that establish the correct directory schema and directory tree structure. The schema and tree structure specified for the Telco deployment are described in "The User Management Specification" on page 48.

The installation and configuration plan contains the procedures for implementing the specified schema and directory tree.

# Installation and Configuration Plan for the Telco Deployment

This section summarizes the sequence of installation sessions and configuration procedures for the Telco deployment. The sequence is determined by considering all of the issues discussed in "Installation and Configuration Issues" on page 55.

The installation and configuration steps are grouped into modules. Each module contains the installation and configuration steps for one component subsystem in the Telco deployment architecture. The installation and configuration modules for the Telco deployment are listed in Table 5-1.

The configuration values that you input in each module are listed the detailed procedures for the modules, which are described in "Software Installation and Configuration Procedures" on page 69.

**Table 5-1** Telco Deployment Installation and Configuration Modules

| Module Number | Computers | Component Subsystem | Procedures |
|---|---|---|---|
| 1A | jesDSM1<br>jesDSM2 | Directory Server with multimaster replication | Install Directory Server and Administration Server |
| 2 | jesDPA1<br>jesDPA2 | Load-balanced Directory Proxy Server | Install Directory Proxy Server and Administration Server |
| 3 | jesPAM1<br>jesPAM2 | Load-balanced Portal Server and Access Manager | Install Portal Server, Access Manager, and Web Server |
| 4 | jesDSM1 | User Management | Prepare directory for Messaging Server and Calendar Server (run Directory Preparation Tool) |
| | jesPAM1 | | Install Delegated Administrator. Configure Delegated Administrator |
| | jesPAM1 | | Use Delegated Administrator command line to extend LDAP schema to support messaging and calendar services |
| | | | Run ldapmodify to add new user to directory |
| 5A | jesMCS1b<br>jesMCS2b | Clustered Business-class Messaging Server and Calendar Server | Install Sun Cluster software; configure both computers as Sun Cluster nodes |
| 5b | jesMCS1b<br>jesMCS2b | | Install Messaging Server and Calendar Server, configure Messaging Server, configure Calendar Server |
| 5c | jesMCS1b<br>jesMCS2b | | Install Sun Cluster agent software |
| 6A on page 125 | jesMS1c<br>jesMS2c | Clustered Consumer-class Messaging Server | Install Sun Cluster software; configure both computers as Sun Cluster nodes |
| 6b | jesMS1c<br>jesMS2c | | Install Messaging Server, configure Messaging Server |

**Table 5-1** Telco Deployment Installation and Configuration Modules *(Continued)*

| Module Number | Computers | Component Subsystem | Procedures |
|---|---|---|---|
| 6c | jesMS1c<br>jesMS2c | | Install Sun Cluster agent software |
| 7 | jesPAM1<br>jesPAM2 | Load balanced Portal Server Secure Remote Access | Install Portal Server Secure Remote Access core on both computers. |
| | jesSRA1<br>jesSRA2 | | Install Portal Server Secure Remote Access gateway on both computers |
| 8 | jesADM | Delegated Administrator Console | Install Delegated Administrator on computer. Configure Delegated Administrator. |
| 9A | jesIMR1<br>jesIMR2 | Load-balanced inbound message relay and outbound message relay | Install Messaging Server software on jesIMR1. Configure Messaging Server MTA on jesIMR1. Install Messaging Server software on jesIMR2. Configure Messaging Server MTA on jesIMR2. |
| 9B | jesORM1<br>jesOMR2 | | Install Messaging Server software on jesOMR1. Configure Messaging Server MTA on jesOMR1. Install Messaging Server software on jesOMR2. Configure Messaging Server MTA on jesOMR2. |
| 10 | jesMMP1<br>jesMMP2 | Load-balanced messaging multiplexor | Install Messaging Server software on jesMMP1. Configure Messaging Server MMP on jesMMP1. Install Messaging Server software on jesMMP2. Configure Messaging Server MMP on jesMMP2. |
| 1B | jesDMS1<br>jesDSM2 | Directory Server with multimaster replication | Activate multimaster replication (after all other installation and configuration steps are complete) |

The sequencing of the modules is described below. The sequence is determined by the issues described in "Installation and Configuration Issues" on page 55.

**Module 1a** The Directory Server module is first, because other components are dependent on the directory service. Notice this module is actually in two parts, with the multimaster replication being implemented in Module 1b after all other services have been installed and configured. For more information see "Component Redundancy" on page 60.

**Module 2** The Directory Proxy Server module comes next, because all other components access the directory through the directory proxy service.

**Module 3** The Portal Server and Access Manager module comes next, because Messaging Server and Calendar Server depend upon the directory schema (Schema 2) that Access Manager sets up in the directory.

**Module 4** Following the Directory Proxy Server module, a test user is created and a corresponding entry placed in the directory. A test user helps verify the remaining modules.

**Modules 5 and 6** The two Messaging Server and Calendar Server back end modules are next because these service are accessed by most of the remaining components. This module is also complicated, because it includes Sun Cluster, and should be done early on to reduce risk.

Following the first six modules, the ordering of the remaining modules is more arbitrary.

**Module 7** Portal Server Secure Remote Access.

**Module 8** Delegated Administrator Console.

**Modules 9 and 10** In these two modules, the various Message Transfer Agent instances are installed and configured. These instances are similar to each other. The have no dependencies on each other, so the order of these modules is not significant.

Each module, including its corresponding installation and configuration steps, is described more fully in "Software Installation and Configuration Procedures" on page 69.

# Configuring Single Sign-on

There are two mechanisms by which single sign-on behavior is achieved in the Telco deployment: Access Manager SSO and proxy authentication. Both of these mechanisms are activated by the installation and configuration process.

- **Access Manager SSO**. Access Manager SSO is a mechanism that supports single sign-on for all web-based services. When Access Manager authenticates an end user successfully, the end-user's browser gets a cookie. If that end user subsequently tries to access another service, the browser passes the cookie, after confirming with Access Manager that the user session is still open, and Access Manager provides access to the service in question. To set up Access Manager SSO for the Telco deployment, you have to configure Messaging Server and Calendar Server components to use Access Manager SSO instead of their legacy authentication mechanisms. For detailed instructions on configuring Access Manager SSO, see “Configure Messaging Server to support Access Manager single sign-on.” on page 119, and “Configure Calendar Server to support Access Manager single sign-on.” on page 122.

- **Proxy authentication.** Proxy authentication means that some proxy user is authenticated on behalf of an end user that has logged in to the system.

  Proxy authentication is used for populating the mail and calendar channels that appear in the portal desktop. A proxy user is authenticated by the Messaging Server and the Calendar Server on behalf of an end user who has logged in to Portal Server. For the Telco deployment, the proxy users are the Messaging Server administrator (`admin`) and the Calendar Server administrator (`calmaster`), respectively. To set up Portal Server proxy authentication, you use the Access Manager administration console to configure a Portal Server SSO adapter for each of these two Portal Desktop channels. You must also populate user entries with the attributes needed to support the Portal Server SSO adapter service. For detailed instructions on configuring proxy authentication, see “Set up the SSO Adapter for the portal mail channel.” on page 97, and “Set up the SSO Adapter for the portal calendar channel. In the Access Manager console:” on page 98.

  Proxy authentication is also used by the Messaging Server MEM component as an adjunct to Access Manager SSO. The user name is extracted from a valid cookie and access to Messaging Server is performed by the Messaging Server administrator (`admin`) on behalf of the user.

# Protocols and Port Numbers Used

The following table shows the protocols used in the Telco deployment.

**Table 5-2** Protocols Used by the Telco Deployment

| Service Provider | Protocol |
|---|---|
| Client facing | HTTP, HTTPS, IMAP, SMTP |
| Portal Server | HTTP, LDAP |
| Portal Server Secure Remote Access | HTTPS |
| Messaging Server (MMP)<br>Messaging Server (MEM) | IMAP, HTTP, LDAP |
| Messaging Server (MTA) | SMTP, LMTP, LDAP |
| Access Manager | HTTP, LDAP |
| Directory Server | LDAP |
| Messaging Server (Store) | HTTP, IMAP, SMTP, LMTP, LDAP |
| Calendar Server (Store) | HTTP, WCAP, LDAP |

When the Java ES installer requests that you enter a port number, the installer performs a runtime check on the ports in use and displays an appropriate default value. If the default port number is being used by another component or by another instance of the same component, the installer presents an alternative value.

The following table lists the Java ES components used in the Telco deployment, the port numbers that each component uses, and the purpose of each port used. Standard ports that are not used in the deployment, such as those for secure SSL protocols, are not included in the table.

**NOTE** Access Manager and Portal Server are not listed in this table because they use the port numbers of the web container into which they are deployed.

**Table 5-3** Telco Deployment Component Port Numbers

| Component | Port | Purpose |
|---|---|---|
| Administration Server | 390 | Standard HTTP port |
| Calendar Server | 82 | Standard HTTP port (changed from default value of 80) |
| | 57997 | ENS |
| Directory Server | 389 | Standard LDAP listener |
| Directory Proxy Server | 489 | Standard Directory Proxy Server listener |
| Messaging Server | 25 | Standard SMTP port |
| | 80 | Messaging MEM (HTTP) port |
| | 143 | Standard IMAP4 port / MMP IMAP Proxy |
| | 7997 | Event Notification Service port |
| | 27442 | Used by Job Controller for product internal communication |
| | 49994 | Used by the Watcher for internal product communication |
| Portal Server Secure Remote Access | 80 | Standard HTTP Port |
| | 443 | HTTP over SSL |
| | 10443 | Rewriter Proxy port |
| | 10555 | Netlet Proxy port |
| | 49916 | Secure Mode, Netlet outgoing port |
| | 49917 | Secure Mode, Netlet incoming port |
| Web Server | 80 | Standard HTTP port |
| | 8888 | Standard Administration port |

Chapter 6

# Software Installation and Configuration Procedures

This chapter describes the procedures for implementing the architecture that is described in Chapter 3, “The Architecture” on page 27. The implementation procedures are based on the specifications described in Chapter 4, “The Deployment Specifications” on page 43 and the installation plan described in Chapter 5, “The Installation and Configuration Plan” on page 55.

The installation and configuration procedures are described in two sections, as follows:

- “System Preparation” on page 70

  This section describes the software installations and hardware configurations needed to prepare the network and the individual computers for installation of the Java ES components. deployment components. This section includes such tasks as installing and configuring the operating system on each computer, setting up the Domain Name Service, and configuring the load balancers.

- “Installing and Configuring the Java ES Software Components” on page 77

  This section describes procedures for installing and configuring the Java ES components instances identified in the architecture. It describes how to install and configure the instances so that they interact properly with each other and provide all of the services described in the requirements.

# System Preparation

To fully deploy the Telco architecture, or a similar architecture that you develop, you must do more than install and configure the Java ES components. This section describes some other tasks you are likely to perform as part of deploying a Java ES system based on the Telco architecture. The tasks are described in a general way, that can be adapted to the specific hardware or software you may be using.

In general, Java ES components are installed on a set of networked computers, and both the individual computers and the network must be properly prepared before you begin to install the Java ES components. The network connections must be complete before you begin to install the Java ES components. Figure 4-1 on page 47 illustrates the network connections required for the Telco deployment.

This section describes:

- Setting up a Domain Name Service (DNS)
- Configuring the load balancers used in the deployment

You set up the DNS first, since you will need the DNS for name/IP address resolution when you install the Solaris operating system on the computers used in the deployment.

## Setting Up a Domain Name Service

A Domain Name Service (DNS) is maps host names to IP addresses, making it possible to access remote computers by host names. in Java ES deployments like the Telco deployment, the DNS also makes it possible to specify networked services by host names. When you install and configure the Java ES components, you configure component instances to interoperate with other component instances by specifying the named networked services provided by the other component instances. You also establish some named services that are accessible to remote users.

### The DNS Mappings for the Telco Deployment

For the purpose of the Telco deployment a new domain called net.telco.com was established. The hostnames for all of computers implementing the deployment architecture belong to the net.telco.com domain.

The entries in the DNS specify the IP address and host name for each computer in the system. The host names and corresponding IP addresses for the Telco deployment are shown in Figure 4-1 on page 47.

In addition to the host names and IP addresses shown in Figure 4-1, the Telco deployment uses a set of virtual host names and virtual IP addresses to reference the networked services provided by the components in the deployment.

Notice that the networked services provided by the component instances in the Telco deployment are logical services. Logical service are networked services provided by several distributed, redundant component instances but represented by a single host name defined in the DNS. Clients of the service address their requests to the logical host name; the requests are to delivered to one of the distributed instances that comprises the logical service.

Logical services are established to satisfy quality of service requirements such as availability, reliability, and network isolation (security). For example, the Telco deployment uses load balancers to distribute requests for a service between two component instances that provide a service, which increases both the availability and reliability of the service. Figure 4-1 shows the network connections between the load balancers and the component instances.

When you use load balancers in this way, you establish a logical service by mapping the logical service name to the load balancer. Then you configure clients of the service to address their requests for the service to the logical service name (the load balancer), which distributes the requests to the real instances that provide the service. For example, components that need directory services are configured to address requests to `jesDPA.net.telco.com`. Figure 4-1 shows you that the name `jesDPA.net.telco.com` is mapped to a load balancer that distributes the requests between to instances of Directory Proxy Server.

Table 6-1 lists the DNS entries that are needed to define the logical services in the Telco deployment. The DNS entries for the logical services must match the virtual host names and virtual IP addresses that you establish for the load balancers. For more information on configuring the load balancers, see “Configuring the Load Balancers” on page 73.

**Table 6-1** Virtual Host Names and IP Addresses for Logical Services

| Logical Service | Virtual Host Name | Virtual IP Address |
|---|---|---|
| Zone 2 | | |
| Directory Proxy Server | jesDPA.net.telco.com | 192.168.12.3 |
| Portal/Access Manger | jesPAM.net.telco.com | 192.168.12.4 |
| Messaging & Calendar Business class Cluster logical host | jesMCSb.net.telco.com | 192.168.12.5 |
| Messaging Consumer class Cluster logical host | jesMSc.net.telco.com | 192.168.12.6 |

**Table 6-1** Virtual Host Names and IP Addresses for Logical Services *(Continued)*

| Logical Service | Virtual Host Name | Virtual IP Address |
|---|---|---|
| Zone 3 | | |
| Messaging Server: MMP | mail.telcomail.com | 192.168.14.3 |
| Portal: SRA gateway | www. telcomail.com | 192.168.14.4 |
| Messaging Server: MTA inbound | smtp. telcomail.com | 192.168.14.5 |
| Messaging Server: MTA outbound | smtpout.telcomail.com | 192.168.14.6 |
| Messaging Server: MMP | mail.telco.net | 192.168.14.7 |
| Messenger Express: MEM | www.telco.net | 192.168.14.8 |
| Messaging Server: MTA inbound | smtp.telco.net | 192.168.14.9 |
| Messaging Server: MTA outbound | smtpout.telco.net | 192.168.14.10 |

## The DNS Architecture for the Telco Deployment

A DNS consists of both server and client components. In the Telco deployment, the DNS server component runs on a SunFire V240 Server (jesADM.net.telco.com). In The DNS server software was co-located with the Delegated Administrator component, as this computer has the least average usage.

Security considerations normally dictate separate DNS servers for the public, client-facing computers and load balancers and the protected computers and load balancers. The DNS server for the public, client-facing computers is typically located in the DMZ, while the DNS server for the internal, protected hardware is located on one of the protected computers, such as jesADM.net.telco.com.

Notice that "The DNS Mappings for the Telco Deployment" on page 70 only describes the contents of the internal DNS server.

If greater security is needed, the internal DNS service can be placed in the innermost access zone. In this case, the integrity of the firewalls could be maintained by having load balancers in the other zones that provide virtual extensions of the DNS service.

DNS client components are needed on all other computers in the deployment. The client components are configured to point to the internal DNS server component. Alternatively the naming service could be changed to LDAP instead of DNS, for the internal hostname-to-IP address translation.

# Configuring the Load Balancers

The load-balancers in the Telco deployment serve a number of purposes, which are described in "Redundancy Strategies Used in the Architecture" on page 38, and "The Network and Connectivity Specification" on page 46.

Before you can install, configure, and use any of Telco's Java ES services, you must configure the load balancers to achieve the correct routing of network traffic.

## Configuring Virtual Service Addresses

Figure 4-1 on page 47 illustrates the physical connections in the Telco deployment between the load balancers and the computers running the Java ES components. For example, there is a load balancer, jesDPA.net.telco.com that is placed in front of two computers, jesDPA1.net.telco.com and jesDPA2.net.telco.com that are running Directory Proxy Server instances. The goal is to have the load balancer distribute requests for directory proxy services between the Directory Proxy Server instances running on jesDPA1 and jesDPA2. This section describes how to configure the load balancer to provide this function.

The mechanism for providing this function is the virtual service and the virtual IP address (VIP). You choose a virtual (logical) name, such as jesDPA.net.telco.com, for a service that is, in reality, provided by a number of component instances. You then configure the load balancer to map the virtual service name and virtual IP address to the component instances that actually provide the service. The configured load balancer appears to the clients of the service as a single device that provides the service, but it is actually the load balancer distributing the requests among the component instances that provide the service.

The basic configuration steps, which should apply to whatever load balancing hardware you are using, are the following:

1. Identify the real hosts to which the load balancer routes requests. These real hosts are the computers running the Java ES component instances. You typically identify the real hosts by adding their IP addresses to the load balancer's hosts table. For example, when you configure the load balancer for the `jesDPA` service, you add the IP addresses for `jesDPA1.net.telco.com` and `jesDPA2.net.telco.com` to the load balancer's host table.

2. Identify the real services to which the load balancer will be routing requests. The real services are the server application instances running on the host computers that you identified in Step 1. In the Telco deployment, the real services are the Java ES component instances. You typically identify a real service by its IP address and port. For example, when you configure the load balancer for the `jesDPA.net.telco.com` service, you identify the Directory Proxy Server instances at `129.138.11.3:489` and `129.138.11.4:489`.

3. Define the service groups. The service groups are sets of the real services that you defined in Step 2. The real services in the group must be capable of fulfilling the same type of request. The load balancer will distribute requests among the real services in the service group. For example, when you define the service group for the `jesDPA.net.telco.com`, you add the real services that specify the Directory Proxy Server instances, `129.138.11.3:489` and `129.138.11.4:489`.

4. Define the virtual (also called logical) service. The virtual service definition includes the outward facing IP address and port at which the load balancer accepts requests for a service. The definition of the virtual service also maps the virtual service to the service group (defined in Step 3) that actually handles the requests. The load balancer will accept requests at the virtual service address and distribute them among the service group. For example, the virtual service definition for the directory proxy service maps the virtual name `jesDPA.net.telco.com` and the virtual IP address 192.168.12.3:389, to the service group that includes the real services`129.138.11.3:489` and `129.138.11.4:489`.

Once the load balancer is configured, you configure the client components, such as the components that use the directory proxy service, to address their requests to the virtual service, rather than to a specific Directory Proxy Server instance. The requests are delivered to the load balancer, which distributes the requests between the Directory Proxy Server instances.

The configuration of virtual service IP addresses must be coordinated with the configuration of your DNS servers. For example, in the Telco deployment, the externally accessible DNS server maps the URL `www.telcomail.com` to the virtual service address for the load balancer in front of the Portal Server Secure Remote Access instances running on jesSRA1 and jesSRA2. The internal DNS server maps the hostname `jesSRA.net.telco.com` to the same virtual service address. This load balancer is configured to distribute requests for portal access between the two Portal Server Secure Remote Access instances.

## SSL Termination

In the Telco deployment, users access portal services through the Portal Server Secure Remote Access gateway, over HTTPS connections. The problem that arises when HTTPS connections are used, is that any session persistence cookies you are using are encrypted when the traffic passes through the load balancers.

- The preferred way of implementing HTTPS secure session is to terminate the SSL connection at the load balancer and have the load balancer do all the encryption and decryption work, rather than computers running the Portal Server Secure Remote Access instances. This produces much better performance. However, not all load balancers have this feature.

- If the load balancer does not decrypt requests, HTTPS sessions pass through the load balancer, and the Portal Server Secure Remote Access instance does the encrypting and decrypting. In this case, the load balancer must still identify the user session and route the requests to the correct Portal Server Secure Remote Access instance. To accomplish this, you configure the load balancer to make routing decisions based on the SSL session ID. Configuring the load balancer to use the session cookie, as described in "Configuring for Session Persistence" on page 75, is not possible.

If the load balancers in your deployment support encrypting and decrypting of SSL requests, you should use this feature. If not, configure the load balancers to route base on the SSL session ID.

## Configuring for Session Persistence

This section describes your options for configuring your load balancers to use session cookies to maintain session persistence. These options are available if you are able to terminate you HTTPS sessions at your load balancers. (These options are also available if you choose to use HTTP instead of HTTPS.)

The Telco deployment uses the Access Manager single sign-on mechanism, which adds the concept of state to the otherwise stateless HTTP protocol. When a user logs in through the Portal Server Secure Remote Access gateway, Access Manager creates a session, which is maintained until the user logs out. You can think of Access Manager sessions in much the same way that you think of the `javax.servlet.http.HttpSession` object.

In the Telco deployment, both portal and access manager services are provided by a service group that is comprised of the component instances running on two load-balanced computers, `jesPAM1` and `jesPAM2`. When a user logs in, the request is routed to the instances on one computer, and the new session is established with the instances on that computer. The problem that arises is tracking the user's session so that additional requests from the same user are routed to the instances to which the user originally connected.

To maintain the user's session, you must configure the load balancer's virtual service definition to support session persistence. You can do this is in either of the following two ways:

- Define and set a session cookie in Access Manager.

  **a.** To define the session cookie, edit the Access Manager configuration file (`/etc/opt/SUNWam/config/AMConfig.properties`) and add the following lines:

  ```
  com.iplanet.am.lbcookie.name=pamlbcookie
  com.iplanet.am.lbcookie.value=101  (on jesPAM1)
  ```

  or

  ```
  com.iplanet.am.lbcookie.name=pamlbcookie
  com.iplanet.am.lbcookie.value=102 (on jesPAM2)
  ```

  The value of the cookie identifies the computer on which the user's session was established.

  **b.** To use the cookie, you configure the load balancer to read the cookie and route requests to the real host identified in the cookie. You typically accomplish this by establishing object and forwarding rules based on the HTTP Request and Response header predicate COOKIE. For example:

  ```
  {COOKIE has pamlbcookie eq 101}
  ```

  This technique makes use of the load balancer's *cookie persistence mechanism* or *level 7 stickiness*. With this technique the load balancer knows exactly where to direct a user HTTP request.

  If you are using load balancers that do not support level 7 stickiness, you can use level 4 stickiness.

- Set the session cookie with the load balancer.

  Some load balancers have their own cookie persistence mechanisms. In this case you can implement session persistence without defining any extra cookies in Access Manager. If your load balancer supports its own persistence mechanism, follow the instructions in the load balancer documentation. Setting the cookie in Access Manager is a more general solution for load balancers that do not have their own cookie persistence mechanism.

# Installing and Configuring the Java ES Software Components

This section describes how to install and configure the Java ES software component instances. The procedures in this section are developed from the following information, which appears earlier in this document:

- The requirements are described in Chapter 2, “The Requirements” on page 19.
- The architecture is described in Chapter 3, “The Architecture” on page 27.
- The detailed specifications are described in Chapter 4, “The Deployment Specifications” on page 43.
- The installation plan, which explains the sequencing and content of the modules, is described in Chapter 5, “The Installation and Configuration Plan” on page 55.

## Module #1: Directory Server with Multimaster Replication

In Module #1, you install and configure two instances of Directory Server. These two instances will serve as master replicas. However, you do not implement multimaster replication immediately. You implement multimaster replication only after you install and configure all of the other component instances.

Implementing multimaster replication as the last step of your installation and configuration process has an important benefit. When you install and configure component instances in modules 2-10, the component instances write their configuration data to the directory. If you write all of these changes to a single Directory Server instances, you can ensure that all of the configuration data is recorded correctly. After you install and configure the other components, you implement multimaster replication, which replicates the component configuration data to the second Directory Server instance.

When you implement multimaster replication as the last step of your installation and configuration process, you must re-create the directory indexes that support the Java ES components. You must create these indexes need in the second Directory Server instance by hand.

Because you implement multimaster replication as the last step of your installation and configuration process, this module is divided into two parts. Part A describes the basic Directory Server installation and configuration. Part B describes how to implement multimaster replication. You perform the procedures in Part B after you complete module 10, after all other component instances are installed and configured.

## Installation and Configuration Summary

The installation and configuration procedures, detailed in the following sections, consist of the following steps:

**Part A: Basic Directory Server Setup**

1. "Install Java ES software on `jesDSM1`." on page 78
2. "Start Directory Server on `jesDSM1`." on page 81
3. "Verify the operation of Directory Server on `jesDSM1`." on page 81
4. "Repeat Step 1- Step 3 on jesDSM2, with the following differences." on page 81

**Part B: Multimaster Replication**

1. "Set up multimaster replication between `jesDSM1` and `jesDMS2`." on page 82
2. "Verify replication behavior." on page 84
3. "Set the Directory Server tuning parameters." on page 85

## Procedure, Part A: Basic Directory Server Setup

1. Install Java ES software on `jesDSM1`.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Directory Server
      - Administration Server

   b. Enter the Directory Server configuration parameter values shown in the following table:

**Table 6-2** Directory Server Configuration Parameters

| Parameter | Value |
|---|---|
| Directory Preparation Tool Installation Directory | `/global/jesDSM1/opt/SUNWcomds` |
| **Common Configuration Settings** | |
| Host Name | `jesDSM1` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.10.3` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **General Settings** | |
| Directory Server Admin User | `admin` |
| Directory Server Admin Password | `password` |
| Directory Server Manager | `cn=Directory Manager` |
| Directory Server Password | `password` |
| **Server Settings** | |
| Directory Server Root (installation directory) | `/global/jesDSM1/var/opt/mps/serverroot` |
| Directory Server Identifier | `jesDSM1` |
| Directory Server Port | `389` |
| Directory Server Root Suffix | `dc=net,dc=telco,dc=com` |
| Directory Server Administration Domain | `net.telco.com` |
| System User | `root` |
| System Group | `root` |
| **Configuration Directory Settings** | |
| New instance will be configuration Directory Server | `1 (Yes)` |
| Configuration Directory Host | `jesDSM1.net.telco.com` |
| Configuration Directory Port | `389` |
| Configuration Directory Admin User | `cn=Directory Manager` |

**Table 6-2** Directory Server Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| Configuration Directory Password | password |
| **Data Storage Settings** | |
| Store user data in new DS instance | 1 (Yes) |
| User Directory Host | jesDSM1.net.telco.com |
| User Directory Port | 389 |
| User Directory Admin User | admin |
| User Directory Admin Password | password |
| Directory Server Suffix | dc=net,dc=telco,dc=com |
| **Populate Data Settings** | |
| Populate with user data? | 4 (No) |
| Disable Schema Checking? | No |

**c.** Enter the Administration Server configuration parameter values shown in the following table:

**Table 6-3** Administration Server Configuration Parameters

| Parameter | Value |
|---|---|
| **Server Settings** | |
| Admin Server Root | /global/jesDSM1/var/opt/mps/serverroot |
| Admin Server Port | 390 |
| Admin Server Administration Domain | net.telco.com |
| System User | root |
| System Group | root |
| **Configuration Directory Settings** | |
| Configuration Directory Admin User ID | admin |
| Configuration Directory Admin Password | password |
| Configuration Directory Host | jesDSM1.net.telco.com |
| Configuration Directory Port | 389 |

2. Start Directory Server on jesDSM1.

```
# /usr/sbin/directoryserver start
```

3. Verify the operation of Directory Server on jesDSM1.

   a. Enter the following commands:

```
# cd /global/jesDSM1/opt/jes/mps/serverroot/shared/bin
```

```
# ./ldapsearch -b "dc=net,dc=telco,dc=com" -h jesDSM1 -p 389 \
   -D "cn=Directory Manager" -w password "objectClass=*"
```

   b. Check for the following results:

```
version: 1
```

```
dn: dc=net,dc=telco,dc=com
objectClass: top
objectClass: domain
dc: net
```

```
dn: cn=Directory Administrators, dc=net,dc=telco,dc=com
objectClass: top
objectClass: groupofuniquenames
cn: Directory Administrators
```

4. Repeat Step 1- Step 3 on jesDSM2, with the following differences.

   a. When installing enter the following parameter values shown in the following table:

**Table 6-4** Directory Server Configuration Parameters

| Parameter | Value |
|---|---|
| **Configuration Directory Settings** | |
| Use an Existing Configuration Directory Server | 2 |

   b. When installing enter the configuration parameter values shown in the following table:

**Table 6-5** Administration Server Configuration Parameters

| Parameter | Value |
|---|---|
| **Configuration Directory Settings** | |
| Configuration Directory Host | jesDSM1.net.telco.com |

## Procedure, Part B: Multimaster Replication

The following steps are performed only after completing Modules 2 through 8.

**1.** Set up multimaster replication between `jesDSM1` and `jesDMS2`.

Before replication agreements can be configured, replication must first be enabled on both Directory Server instances.

Replication is achieved by using the Administration Server Console to configure one master instance (`jesDSM1`) and then replicating all the data to the other Directory Server instance (`jesDSM2`).

**a.** Enable replication for Directory Server on `jesDSM1`.

- Start the Administration Server

```
# /usr/sbin/mpsadmserver start
```

- Start the Administration Server Console

```
# /usr/sbin/mpsadmserver startconsole
```

- Set the replication flag for the five root suffixes in the directory:

```
dc=net,dc=telco,dc=com
o=comms-config
o=NetscapeRoot
o=pab
o=PiServerDb
```

**b.** Add the `o=NetscapeRoot` suffix to Directory Server on `jesDSM2`.

Use the Administration Server Console that your started in Step a.

**c.** Add schema extensions and indexes for Messaging Server and Calendar Server to the Directory Server instance on `jesDSM2`.

- Change directory on `jesDSM2` to the location of the Directory Preparation Tool.

```
# cd /global/jesDSM2/opt/SUNWcomds/sbin
```

- Run the Directory Preparation Tool.

```
# perl comm_dssetup.pl
```

- Provide the following parameters requested by the script:

**Table 6-6** Directory Server Preparation Tool Parameters

| Parameter | Value |
|---|---|
| Directory Server Root | /global/jesDSM2/var/opt/mps/serverroot |
| Directory Server Instance | slapd-jesDSM2 |
| Directory Manager DN | cn=Directory Manager |
| Directory Manager Password | password |
| Users/Groups Directory | Yes |
| User/Group Base Suffix | dc=net,dc=telco,dc=com |
| Schema Type | 2 |
| Update Schema | Yes |
| Add New Indexes | Yes |
| ReIndex New Indexes Now | Yes |

The Directory Preparation Tool adds schema extensions and indexes to the directory, including adding the following root suffixes:

- o=pab (for personal address books)
- o=PiServerDb (for personal address books)
- o=comms-config (for mapping the functions of Delegated Administrator, used to populate user data for Messaging Server and Calendar Server)

**d.** Add indexes for Access Manager to the Directory Server instance on jesDSM2.

- Log in on jesDPA.net.telco.com.
- 
```
# ./ldapmodify -D "cn=Directory Manager" -w password -c
-a -h "jesDSM2" -p "389"
-f "/etc/opt/SUNWam/config/ldif/index.ldif"
```

**e.** Create replication agreements for the Directory Server instance on jesDSM1.

**f.** Repeat Step a for the Directory Server instance on jesDSM2.

**g.** From the Directory Server instance on jesDSM1, initialize the remote Directory Server on jesDSM2 for each of the root suffixes.

**h.** Repeat Step e for the Directory Server instance on `jesDSM2`.

**i.** Reindex all the suffixes on `jesDSM1` and then on `jesDSM2`.

Use the Administration Console to perform the reindexing.

**j.** Set the replication agreements on `jesDSM1` and `jesDSM2` for continuous refresh.

**2.** Verify replication behavior.

**a.** Insert a test organization entry in Directory Server on `jesDSM1`.

```
# ./ldapmodify -a -h jesDSM1 -p 389 -D "cn=Directory Manager"
   -w password

dn: o=testOrg, o=data
objectClass: top
objectClass: organization
o: testOrg
```

**b.** Query Directory Server on `jesDSM2` for the new entry.

```
# ./ldapsearch -b "dc=net,dc=telco,dc=com" -h jesDSM2 -p 389
   -D "cn=Directory Manager" -w password "objectClass=*"
```

**c.** Check for the following results:

```
version: 1
...
dn: o=testOrg, dc=net,dc=telco,dc=com
objectClass: top
objectClass: organization
```

3. Set the Directory Server tuning parameters.

   Set the parameters shown in Table 6-7.

**Table 6-7** Directory Server Tuning Parameters

| Parameter | Value |
|---|---|
| Database Cache Size | 200 MB |
| **Entry Cache Size** | |
| dc=net,dc=telco,dc=com | 100 MB |
| o=comms-config | 20 MB |
| o=NetscapeRoot | 10 MB |
| o=pab | 30 MB |
| o=PiServerDb | 30 MB |
| **Client Control Parameters** | |
| Size Limit: | unlimited |
| Look-through Limit: | unlimited |
| Time-Limit: | unlimited |
| Idle-Timeout: | 1200 secs<br>(20 mins when load balancer timeout set to 30 mins) |

# Module #2 Directory Proxy Server

In this module you install Directory Proxy Server instances and configure the instances for load balancing.

## Procedure, Part A: Directory Proxy Server in DMZ1 Layer

Directory Proxy Server set up.

1. Install Java ES software on `jesDPA1`.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Administration Server
      - Directory Proxy Server

**b.** Select Remote Directory Installation

Specify the existing Directory Server instance on `jesDS1`.

**c.** Enter the Directory Proxy Server configuration parameter values shown in the following table:

**Table 6-8** Directory Proxy Server Configuration Parameters

| Parameter | Value |
|---|---|
| Target Installation Directory | `/global/jesDPA1` |
| **Common Configuration Settings** | |
| Host Name | `jesDPA1` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.3` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **Administration Server: Server Settings** | |
| Server Root | `/global/jesDPA1/var/opt/mps/serverroot` |
| Administration Port | `390` |
| Administration Domain | `net.telco.com` |
| System User | `root` |
| System Group | `root` |
| **Configuration Directory Settings** | |
| Directory Server Admin User | `admin` |
| Directory Server Admin Password | `password` |
| Configuration Directory Host | `jesDSM1.net.telco.com` |
| Configuration Directory Port | `389` |
| Directory Proxy Server Port | `489` |

2. Start the Directory Proxy Server on `jesDPA1`.

   ```
   cd /global/jesDPA1/var/opt/mps/serverroot/dps-jesDPA1
   ./start-dps
   ```

3. Verify the operation of Directory Proxy Server on `jesDPA1`.

   a. Query Directory Server on `jesDSM1` via the Directory Proxy Server.

      # ldapsearch -b “dc=net,dc=telco,dc=com” -h jesDPA1 -p 489
      -D “cn=Directory Manager -w password “objectClass=*”

   b. Check for the following results:

      ```
      ldap_simple bind: Insufficient access
      ldap_simple bind: additional info: Not permitted to bind
      ```

      This result indicates that the directory proxy has not yet been configured to allow access to the Directory Server.

4. Configure Directory Proxy Server using the Directory Proxy Server console.

   a. Open `jesDPA1` configuration.

   b. Select Network Groups.

   c. Select Group Configuration.

   d. Select Edit.

   e. Rename the Network Group from `network-group-1` to `trusted_zone_group`.

   f. In the Group panel go the Network option.

   g. Set the client binding criteria:

      ```
      162.168.11.0/255.255.255.0 quad mask
      ```

   h. In the Forwarding option, go to Operations.

      Allow all operations.

   i. Save the configuration and exit the Group panel.

   j. Select Properties.

   k. Select Ldap Server

   l. Select ldap-server-1

**m.** Select Edit.

Change the property name to `jesDSM1`.

Set the host to `jesDSM1.net.telco.com`.

**n.** Save your changes.

**5.** Restart Directory Proxy Server.

Use the Tasks menu on the Directory Proxy Server console.

**6.** Verify the operation of Directory Proxy Server.

**a.** Query Directory Server on `jesDSM1` via the Directory Proxy Server.

```
# ldapsearch -b “dc=net,dc=telco,dc=com” -h jesDPA1 -p 489
-D “cn=Directory Manager -w password “objectClass=*”
```

**b.** Check for the following results:

```
version:1
dn: dc=net,dc=telco,dc=com
objectClass: top
objectClass: domain
dc: net
```

**7.** Repeat Step 1 through Step 6 on `jesDPA2`.

When you repeat, note the following changes:

- In Step 4m replace `jesDSM1` with `jesDSM2`.
- In Step 6a replace `jesDPA1` with `jesDPA2`.

**8.** Configure the load balancer `jesDPA` in zone 2 (192.168.12.3) to balance http requests between the two Directory Proxy Server instances `jesDPA1` (192.168.11.3) and `jesDPA2` (192.168.11.4). For more information see “Configuring the Load Balancers” on page 73.

**9.** Shut down the Directory Proxy Server on `jesDPA2`.

10. Verify the operation of Directory Proxy Server on jesDPA1.

    a. Insert into the LDAP directory an o=id root suffix. Set the value to jesDSM1:

    ```
    # ldapmodify -a -h jesDSM1 -p 389 -D cn=Directory Manager -w
    password
    dn: o=id
    objectClass: top
    objectClass: organization
    description: jesDSM1
    ```

    b. Query the Directory Server instance on jesDSM1 via the Directory Proxy Server logical URL:

    ```
    # ldapsearch -b o=id -h jesDPA -p 389 -D cn=Directory Manager
    -w password objectClass=*
    ```

    c. Check for the following results:

    ```
    dn: o:=id
    objectClass: top
    objectClass:organization
    description: jesDSM1
    ```

    This result verifies that the load balancer, Directory Proxy Server, and Directory Server are all working.

11. Shut down the Directory Proxy Server on jesDPA1.

12. Verify the operation of Directory Proxy Server on jesDPA2.

    a. Insert into the LDAP directory an o=id root suffix. Set the value to jesDSM2:

    ```
    # ldapmodify -a -h jesDSM2 -p 389 -D cn=Directory Manager -w
    password
    dn: o=id
    objectClass: top
    objectClass: organization
    description: jesDSM2
    ```

    b. Query the Directory Server on jesDSM2 via the Directory Proxy Server logical URL:

    ```
    # ldapsearch -b o=id -h jesDPA -p 389 -D cn=Directory Manager
    -w password objectClass=*
    ```

**c.** Check for the following results:

```
dn: o:=id
objectClass: top
objectClass:organization
description: jesDSM2
```

This verifies that the load balancer, Directory Proxy Server, and Directory Server are all working.

# Module #3: Portal Server and Access Manager on Web Server

In this module you install Portal Server and Access Manager instances and configure these instances for load balancing. For Access Manager, you run the Java ES installer in configure now mode, and the installer configures Access Manager, which includes extending the directory schema to support Access Manager. Configuring Access Manager for load balancing, however, is a procedure you must perform by hand.

## Installation and Configuration Summary

The installation and configuration procedure, detailed in the following section, consists of the following steps:

1. “Install Java ES software on jesPAM1.” on page 91
2. “Start Web Server on jesPAM1. Starting Web Server automatically starts Access Manager.” on page 94
3. “Verify the operation of Access Manager on jesPAM1.” on page 94
4. “Install Java ES software on jesPAM2.” on page 95
5. “Start Web Server on jesPAM2. Starting Web Server automatically starts Access Manager.” on page 96
6. “Verify the operation of Access Manager on jesPAM2.” on page 96.
7. “Log in to the Access Manager console on jesPAM1.” on page 96.
8. “In the Access Manager console, navigate:” on page 96
9. “On both jesPAM1 and jesPAM2, edit the Access Manager configuration file and add an fqdnmap entry.” on page 97
10. “Restart the Web Server instances on jesPAM1 and jesPAM2.” on page 97

11. "Set up the SSO Adapter for the portal mail channel." on page 97
12. "Set up the SSO Adapter for the portal calendar channel. In the Access Manager console:" on page 98

## Procedure

1. Install Java ES software on `jesPAM1`.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Web Server
      - Access Manager
      - Portal Server

   b. Select the following Access Manager sub-components:

      - Identity Management and Policy Services Core
      - Access Manager Administration Console
      - Common Domain Services for Federation Management
      - Access Manager SDK

   c. Specify that Access Manager will use a remote Directory Server instance.

   d. Enter the configuration parameter values shown in the following table:

**Table 6-9** Portal Server, Access Manager and Web Server Configuration Parameters

| Parameter | Value |
|---|---|
| **Installation Directories** | |
| Access Manager | `/global/jesPAM1/opt` |
| Web Server | `/global/jesPAM1/opt/SUNWwbsvr` |
| Portal Server | `/global/jesPAM1/opt` |
| **Common Configuration Settings** | |
| Host Name | `jesPAM1` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.5` |
| Administrator User ID | `admin` |

**Table 6-9** Portal Server, Access Manager and Web Server Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| Administrator Password | password |
| System User | root |
| System Group | root |
| **Web Server: Administration** | |
| Server Admin User ID | admin |
| Admin User's Password | password |
| Host Name | jesPAM1.net.telco.com |
| Administration Port | 8888 |
| Administration Server User ID | root |
| **Default Web Server Instance** | |
| System User ID | root |
| System Group | root |
| HTTP Port | 80 |
| Content Root | /global/jesPAM1/opt/SUNWwbsvr/docs |
| Do you want to automatically restart Web Server when system restarts? | Yes |
| **Access Manager: Administration** | |
| Administrator User ID | amAdmin |
| Administrator Password | password |
| LDAP User ID | amldapuser |
| LDAP Password | password1 |
| Password Encryption Key | password |
| Install Type | legacy |
| **Access Manager: Web Container** | |
| Web container in which to deploy | 2. Web Server |

**Table 6-9** Portal Server, Access Manager and Web Server Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| **Access Manager: Web Server** | |
| Host Name | jesPAM1.net.telco.com |
| Web Server Instance Directory | /global/jesPAM1/opt/SUNWwbsvr/https-jesPAM1.net.telco.com |
| Web Server Port | 80 |
| Document Root Directory | /global/jesPAM1/opt/SUNWwbsvr/docs |
| Secure Server Instance Port | No |
| **Web Container for Running Access Manager Services** | |
| Host Name | jesPAM1.net.telco.com |
| Services Deployment URI | amserver |
| Common Domain Deployment URI | amcommon |
| Cookie Domain | .net.telco.com |
| Administration Console | Yes |
| Console Deployment URI | amconsole |
| Password Deployment URI | ampassword |
| **Access Manager: Directory Server** | |
| Directory Server Host | jesDPA.net.telco.com |
| Directory Server Port | 389 |
| Directory Root Suffix | dc=net,dc=telco,dc=com |
| Directory Manager DN | cn=Directory Manager |
| Directory Manager Password | password |
| **Access Manager: Directory Server Data** | |
| Is Directory Server provisioned[1] | No |
| **Portal Server: Web Container** | |
| Web Container | 2. Sun Java System Web Server |

**Table 6-9** Portal Server, Access Manager and Web Server Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| **Portal Server: Web Server** | |
| Installation Directory | /global/jesPAM1/opt/SUNWwbsvr |
| Server Instance | jesPAM1.net.telco.com |
| Server Instance Port | 80 |
| Instance Port Secure | No |
| Document Root | /global/jesPAM1/opt/SUNWwbsvr/docs |
| **Portal Server: Web Container Deployment** | |
| Load Balancer | Yes |
| Load Balancer Protocol | 1. HTTP |
| Load Balancer Host | jesPAM.net.telco.com |
| Load Balancer Port | 80 |
| Deployment URI | /portal |
| Install Sample Portal | Yes |

1. Value of No indicates that schema extensions and directory entries should be made. A Value of Yes means changes have already been made by installation or configuration of Java ES components, even if users have not yet been provisioned.

2. Start Web Server on jesPAM1. Starting Web Server automatically starts Access Manager.

```
# cd /global/jesPAM1/opt/SUNWwebsvr/https-jesPAM1.net.telco.com
# ./start
```

3. Verify the operation of Access Manager on jesPAM1.

   - `# /usr/bin/ps -ef | grep webservd`

     and look for running Web Server processes.

     or, in a web browser:

   - `http://jesPAM1.net.telco.com/amconsole`

     and log in as the Access Manager administrator, amadmin.

4. Install Java ES software on `jesPAM2`.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Web Server
      - Access Manager
      - Portal Server

   b. Select the following Access Manager sub-components:

      - Identity Management and Policy Services Core
      - Access Manager Administration Console
      - Common Domain Services for Federation Management
      - Access Manager SDK

   c. Specify that Access Manager will use a remote Directory Server instance.

   d. Enter the same configuration parameter values that you used for the `jesPAM1` installation, with the exceptions shown in the following table:

**Table 6-10** Access Manager and Web Server Configuration Parameters

| Parameter | Value |
|---|---|
| **Access Manager: Directory Server Data** | |
| Is Directory Server provisioned[1] | `Yes` |
| Organization Marker Object Class | `sunISManagedOrganization` |
| Organization Naming Attribute | `o` |
| User Marker Object Class | `inetorgperson` |
| User Naming Attribute | `uid` |

1. Value of No indicates that schema extensions and directory entries should be made. A Value of Yes means changes have already been made by installation or configuration of Java ES components, even if users have not yet been provisioned.

5. Start Web Server on jesPAM2. Starting Web Server automatically starts Access Manager.

   ```
   # cd /global/jesPAM1/opt/SUNWwebsvr/https-jesPAM2.net.telco.com
   # ./start
   ```

6. Verify the operation of Access Manager on jesPAM2.

   ```
   # /usr/bin/ps -ef | grep webservd
   ```

   and look for running Web Server processes.

   or, in a web browser:

   `http://jesPAM1.net.telco.com/amconsole`

   and log in as the Access Manager administrator, `amadmin`.

7. Log in to the Access Manager console on jesPAM1.
   a. `http://jesPAM1.net.telco.com/amconsole`
   b. For user ID, use amadmin, for password use password.

8. In the Access Manager console, navigate:
   a. Click the Configuration tab.
   b. Select Authentication Modules / System Properties.
   c. Select Platform
   d. Select Site Name.
   e. To specify the load balancer, enter the following value

      `http://jesPAM.net.telco.com:80|10`

   f. Click Add.
   g. In the Server List, locate Instance Name. Do the following:
      - Add `jesPAM2.net.telco.com:80|02|10`
      - Add `jesPAM1.net.telco.com:80|01|10`
      - Remove `jesPAM1.net.telco.com:80|01`
      - Remove `jesPAM2.net.telco.com:80|02`
      - Click Save.

9. On both jesPAM1 and jesPAM2, edit the Access Manager configuration file and add an fqdnmap entry.

   a. In a text editor, open /etc/opt/SUNWam/config/AMConfig.properties.

   b. Add the following line:

      ```
      com.sun.identity.server.fqdnMap[jesPAM.net.telco.com]=jesPAM.net
      .telco.com
      ```

10. Restart the Web Server instances on jesPAM1 and jesPAM2.

11. Set up the SSO Adapter for the portal mail channel.

    a. In your web browser, log in to the Access Manager console. Open the following URL:

       ```
       http://jesPAM.net.telco.com/amconsole
       ```

    b. Type the user ID (amadmin) and password (password).

    c. Click the Service Configuration tab.

    d. In the left pane, locate the SSO adapter service. Click the arrow for the adapter service.

    e. In the right pane, Locate the SUN-ONE-MAIL service. Click Edit Properties.

    f. Set the property values shown in the following table:

**Table 6-11** Sun One Mail Server SSO Adapter Service Properties

| Property | Value |
|---|---|
| **Access Manager: Directory Server Data** | |
| Protocol | imap |
| ClientProtocol | http |
| EnableProxyAuth | TRUE |
| ProxyAdminUid | admin |
| ProxyAdminPassword | password |
| EnablePerRequestConnection | true |
| UserAttribute | uid |
| Host | jesMCSb.net.telco.com |
| Port | 143 |
| ClientPort | 80 |

**Table 6-11** Sun One Mail Server SSO Adapter Service Properties

| Property | Value |
|---|---|
| SmtpServer | jesMCSb.net.telco.com |
| smtpPort | 25 |
| ServerSSOEnabled | TRUE |

**g.** Save the parameter settings. Do not close the Access Manager console.

**12.** Set up the SSO Adapter for the portal calendar channel. In the Access Manager console:

**a.** Click the Service Configuration tab.

**b.** In the left pane, locate the SSO adapter service. Click the arrow for the adapter service.

**c.** In the right pane, Locate the SUN-ONE-CALENDAR service. Click Edit Properties.

**d.** Set the property values shown in the following table:

**Table 6-12** Sun One Calendar Server SSO Adapter Service Properties

| Property | Value |
|---|---|
| **Access Manager: Directory Server Data** | |
| Protocol | http |
| ClientProtocol | http |
| EnableProxyAuth | TRUE |
| ProxyAdminUid | calmaster |
| ProxyAdminPassword | password |
| UserAttribute | uid |
| Host | jesMCSb.net.telco.com |
| Port | 82 |
| ClientPort | 82 |
| ServerSSOEnabled | TRUE |

**e.** Save the property settings.

# Module #4: User Management

In this module you prepare the LDAP directory for the different classes of user that Telco supports. You set up two email domains, `telcomail.com` and `telco.net`. You also add two branches to the LDAP directory tree, `o=telcomail.com` and `o=telco.net`, which group the user entries for the two mail domains. Business class users who do not have hosted domain support are added to the `telcomail.com` email domain, and their account data is stored in the `o=telcomail.com` branch of the directory tree. Consumer class users are added to the `telco.net` email domain, and their account data is stored in the `o=telco.net` branch of the directory tree.

This specific tasks described in this module are the following:

- Preparing the LDAP directory for mail and calendar services.
- Creating the `telcomail.com` and `telco.net` email domains and the corresponding branches in the LDAP directory tree.
- Adding attributes to each branch of the LDAP tree so that the user accounts in each branch are provisioned for the correct services.
- Adding a test user to each branch.

The tool that you use for most of these tasks is Delegated Administrator.

Delegated Administrator consists of server-side components and client-side components. This module explains how to install and configure the server-side components of Delegated Administrator. These components use the Access Manager SDK and must be deployed in the same web container as Access Manager.

This module also describes how to use the client-side command line utility (the `commadmin` command) to add the email domains, add the LDAP branches, and provision the test users.

This document describes using the Delegated Administrator command line utility, because the command line examples clearly show you the changes that you make to the directory. In a production environment you probably would use the Delegated Administrator console for many of these administration tasks. For the procedures that install and configure the Delegated Administrator console, see "Module #8 Delegated Administrator Console on Web Server" on page 139.

To add more email domains, such as a hosted domain for hostedcorp.com, repeat Step 9 through Step 14, changing the command line arguments for the email domains and LDAP branches you are creating.

## Installation and Configuration Summary



## Procedure

1. Prepare the directory for Messaging Server and Calendar Server.

   a. On jesDSM1, change directory to the location of the Directory Preparation Tool.

   ```
   # cd /global/jesDSM1/opt/SUNWcomds/sbin
   ```

   b. Run the Directory Preparation Tool.

   ```
   # perl comm_dssetup.pl
   ```

   The script prompts you for configuration parameters.

   c. Enter the parameter values listed in the following table:

**Table 6-13** Directory Server Preparation Tool Parameters

| Parameter | Value |
|---|---|
| Directory Server Root | /global/jesDSM1/var/opt/mps/serverroot |
| Directory Server Instance | slapd-jesDSM1 |
| Directory Manager DN | cn=Directory Manager |
| Password | password |
| Directory Server Used for Users/Groups? | Yes |
| Users/Groups Base Suffix | dc=net,dc=telco,dc=com |
| Schema Type | 2 |
| Update the Schema Files? | Yes |
| Configure New Indexes? | Yes |
| Reindex the New Indexes Now? | Yes |

The Directory Preparation Tool adds schema extensions to the directory, including adding the following root suffixes:

- o=pab (for personal address books)
- o=PiServerDb (for personal address books)
- o=comms-config (for mapping the functions of Delegated Administrator, used to populate user data for Messaging Server and Calendar Server)

Notice that the Directory Preparation Tool operates on the base suffix for the Telco deployment, dc=net,dc=telco,dc=com.

**2.** Install Delegated Administrator software on jesPAM1.

**a.** Use the Configure Later option of the Java ES installer.

**b.** Select the following components:

- Communications Services Delegated Administrator

**c.** Specify that Delegated Administrator will use a remote Directory Server instance. Use the configuration parameter values shown in the following table:

**Table 6-14** Delegated Administrator Installation Parameters

| Parameter | Value |
|---|---|
| Target Installation Directory | /global/jesPAM1/opt/SUNWcomm |

**3.** Configure Delegated Administrator on jesPAM1.

**a.** Run the Delegated Administrator configuration program.

```
# cd /global/jesPAM1/opt/SUNWcomm/sbin
# ./config-commda -nodisplay
```

**b.** Supply the parameters listed in the following table (notice that this operation creates the o=telcomail.com domain):

**Table 6-15** Delegated Administrator Configuration Parameters

| Parameter | Value |
|---|---|
| Directory for the Configuration and Data Files | /global/jesPAM1/var/opt/SUNWcomm |
| Component Selection | 1 Delegated Administrator Utility<br>3 Delegated Administrator Server |
| Hostname | jesPAM1.net.telco.com |
| Port | 80 |
| Default Domain | net.telco.com |
| Default SSL Port | 443 |
| Access Manager Base Directory | /global/jesPAM1/opt/SUNWam |
| Web Server Root Directory | /global/jesPAM1/opt/SUNWwbsvr |
| Web Server Instance Identifier | jesPAM1.net.telco.com |
| Virtual Server Identifier | https-jesPAM1.net.telco.com |
| Web Server HTTP Port | 80 |
| LDAP (Directory Server) URL | ldap://jesDPA.net.telco.com:389 |
| Bind as | cn=Directory Manager |

**Table 6-15** Delegated Administrator Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| Password | password |
| Access Manager Admin User | amadmin |
| Access Manager Admin Password | password |
| Access Manager LDAP Authentication User | amldapuser |
| Access Manager Internal LDAP Authentication Password | password1 |
| Organization DN | o=telcomail.com,dc=net,dc=telco,dc=com |
| Default Organization Top Level Administrator | admin |
| Top Level Administrator Password | password |
| Load sample service packages? | Yes |
| Load sample organizations? | No |

4. Restart Web Server.

```
# cd /global/jesPAM1/opt/SUNWwbsvr/https-jesPAM1.net.telco.com
# ./stop
# ./start
```

5. Modify the telcomail.com domain.

   Use Delegated Administrator to add object classes and attributes that support Messaging Server and Calendar Server to the telcomail.com domain.

```
# ./commadmin domain modify -D admin -w password -n net.telco.com
  -d o=telcomail.com,dc=net,dc=telco,dc=com -S mail,cal
```

   When prompted, enter the domain's mailhost: jesMCSb.net.telco.com

6. Verify the telcomail.com domain.

   a. Query the list of domains:

```
# ./commadmin domain search -D admin -w password
```

**b.** Confirm that you receive the following response:

```
OK
dn: o=telcomail.com,dc=net,dc=telco,dc=com
preferredmailhost: jesMCSb.net.telco.com
o: telcomail.com
```

**7.** Add a user account in the `telcomail.com` domain.

The following commands also provision the user account for Messaging Server, Calendar Server, and Portal Server.

**a.** Create a user entry for `buser0001`.

```
# ./commadmin user create -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -F user -L buser0001 -W password
```

**b.** Provision `buser0001` for mail and calendar services:

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -S mail,cal
```

`-S mail,cal` means add mail and calendar support for the user.

**c.** Provision the user for the Portal Server SSO adapter service.

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -A +objectclass:sunssoadapterperson
```

**d.** Provision the user for Portal Server Portal Desktop service.

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -A +objectclass:sunportaldesktopperson
```

**e.** Set the mail host for the user to `jesMCSb.net.telco.com`.

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -A mailhost:jesMCSb.net.telco.com
```

**f.** Provision the user for the Netfile service.

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -A +objectclass:sunportalnetfileservice
```

**g.** Provision the user for the portal gateway access service.

```
# ./commadmin user modify -D admin -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com”
   -d “o=telcomail.com,dc=net,dc=telco,dc=com”-l buser0001
   -A +objectclass:sunportalgatwayaccessservice
```

**8.** Verify `buser0001`.

**a.** Query the directory for business class users:

```
# ./commadmin user search -D “admin” -w password
   -n “o=telcomail.com,dc=net,dc=telco,dc=com“
   -d “o=telcomail.com,dc=net,dc=telco,dc=com“
```

**b.** Confirm the following response:

```
dn:
uid=buser0001,ou=People,o=telcomail.com,dc=net,dc=telco,dc=com
uid: buser0001
mail: buser0001@telcomail.com
mailhost: jesMCSb.net.telco.com
...
```

**9.** Create the `telco.net` domain.

```
# ./commadmin domain create -D admin -w password
   -n o=telcomail.com,dc=net,dc=telco,dc=com

   Enter DNS Domain Name: telco.net
   OK
```

**10.** Add Messaging Server support to the `telco.net` domain.

```
# ./commadmin domain modify -D admin -w password
   -n o=telcomail.com,dc=net,dc=telco,dc=com
   -d o=telco.net,dc=net,dc=telco,dc=com, -S mail

Enter domain’s mailhost: jesMSc.net.telco.com
```

**11.** Verify the `telco.net` domain.

**a.** Query the list of domains:

```
# ./commadmin domain search -D admin -w password
   -n o=telcomail.com,dc=net,dc=telco,dc=com
```

**b.** Confirm that you receive the following response:

```
OK
dn: o=telco.net,dc=net,dc=telco,dc=com
preferredmailhost: jesMSc.net.telco.com
o: telcomail.com
```

**12.** Add an administrator account for the `telco.net` domain.

**a.** Create the `admin_telco.net` account.

```
# ./commadmin user create -D admin -w password
-n o=telcomail.com,dc=net,dc=telco,dc=com
-d o=telco.net,dc=net,dc=telco,dc=com
-l admin_telco.net -F Default  -L Administrator -W password
```

**b.** Add the `admin_telco.net` account as an administrator for the `telco.net` domain.

```
# ./commadmin admin add -D admin -w password
-n o=telcomail.com,dc=net,dc=telco,dc=com
-d o=telco.net,dc=net,dc=telco,dc=com
-l  admin_telco.net
```

**13.** Add a user account to the `telco.net` domain.

The following command uses the `admin_telco.net` account to create a user account and provision the user account for Messaging Server. Compare this sequence of commands to Step 7, which provisions a business class user account for more services.

**a.** Create a user entry for `cuser0001`.

```
# ./commadmin user create -D admin_telco.net -w password
   -n o=telco.net,dc=net,dc=telco,dc=com
   -d o=telco.net,dc=net,dc=telco,dc=com -l cuser0001
   -F user -L cuser0001 -W password
```

**b.** Provision cuser0001 for mail service:

```
# ./commadmin user modify -D admin_telco.net -w password
   -n o=telco.net,dc=net,dc=telco,dc=com
   -d o=telcomail.com,dc=net,dc=telco,dc=com-l cuser0001
   -l cuser0001 -S mail
```

`-S mail` means add mail support for the user.

**c.** Set cuser0001's mailhost to jesMSc.net.telco.com.

```
# ./commadmin user modify -D admin_telco.net -w password
   -n o=telco.net,dc=net,dc=telco,dc=com
   -d o=telco.net,dc=net,dc=telco,dc=com -l cuser0001
   -A mailhost:jesMSc.net.telco.com
```

**14.** Verify cuser0001.

**a.** Query the directory for consumer class users:

```
# ./commadmin user search -D admin_telco.net -w password
   -n o=telco.net,dc=net,dc=telco,dc=com
   -d o=telco.net,dc=net,dc=telco,dc=com
```

**b.** Confirm the following response:

```
dn: uid=cuser0001,ou=People,o=telco.net,dc=net,dc=telco,dc=com
uid: cuser0001
mail: cuser0001@telco.net
mailhost: jesMSc.net.telco.com
```

# Module #5: Business-class Messaging Server and Calendar Server on Sun Cluster Nodes

In module 5 you set up the Messaging Server and Calendar Server instances that support the `telcomail.com` email domain for business-class users. You install and configure these instances to run on Sun Cluster nodes. The messaging and calendar services thereby become resources managed by Sun Cluster software. The installation and configuration procedure is relatively complex, and requires you to run the Java ES installer three times on each computer. The procedure is divided into the following three parts:

**Part A.** Install Sun Cluster software and set up the global file system and cluster nodes. This must be done before Messaging Server and Calendar Server are installed.

**Part B.** Install and configure Messaging Server and Calendar Server. Messaging Server and Calendar Server are installed in the global file system on the logical host that represents the Sun Cluster nodes.

After you install Messaging Server and Calendar Server, you configure them as follows:

1. Run the Directory Preparation Tool to extend the LDAP schema to support Messaging Server and Calendar Server configuration. Notice that in the Telco installation, you performed this step in Module 4. For more information, see "Module #4: User Management" on page 99.
2. Run the Messaging Server configuration program. Configure the Messaging Server instance to support the `telcomail.com` email domain.
3. Run the Calendar Server configuration program. Configure Calendar Server to use the `telcomail.com` email domain.

**Part C.** Install the Sun Cluster agents and configure the Messaging Server and Calendar Server resources. This makes it possible for the Sun Cluster software to manage the Messaging Server and Calendar Server instances.

## Installation and Configuration Summary

The installation and configuration procedures are divided into three parts. The procedures are summarized as follows:

**Part A: Set Up Sun Cluster Nodes and Global File System**

1. "Install Java ES software on `jesMCS1b`." on page 110.
2. "Prepare system for configuring Sun Cluster software." on page 110

3. “Configure Sun Cluster software on jesMCS1b.” on page 111
4. “Repeat Step 1 - Step 3 on jesMCS2b.” on page 112
5. “Complete the configuration of Network Timing Protocol (NTP).” on page 112
6. “Add a quorum disk to the cluster.” on page 113.
7. “Set up cluster disk meta sets and mirroring.” on page 113
8. “Create new cluster file systems and mount corresponding global directories.” on page 115
9. “Create a cluster resource group. The resource group must be associated with a virtual host name and IP address and then brought on line.” on page 115
10. “Test failover of the cluster resource group.” on page 116

**Part B: Install and Configure Messaging Server and Calendar Server**

1. “Disable the Solaris sendmail service on jesMCS1b.” on page 116
2. “Install Java ES software on jesMCS1b.” on page 116
3. “Configure Messaging Server.” on page 118.
4. “Start the Messaging Server” on page 119
5. “Verify that Messaging Server is properly configured.” on page 119
6. “Configure Calendar Server.” on page 120
7. “Start the Calendar Server.” on page 122
8. “Verify that Calendar Server is properly configured.” on page 122

**Part C: Configure Sun Cluster Resources**

1. “Install Java ES software on jesMCS1b.” on page 123
2. “Configure the Messaging Server resource.” on page 123
3. “Configure the Calendar Server resource.” on page 124

## Procedure, Part A: Set Up Sun Cluster Nodes and Global File System

1. Install Java ES software on `jesMCS1b`.

   Use the Configure Later option of the Java ES installer.

   Select the Sun Cluster core component for installation.

2. Prepare system for configuring Sun Cluster software.

   Create new file systems on `jesMCS1b` and mount directories in preparation for configuring Sun Cluster software.

   a. Create new file systems on `jesMCS1b`. The following example uses meta devices created using Solaris Volume Manager. d0 is a mirrored, encapsulated system disk and the slice 4 partition will be mounted as a `/globaldevices` mount point.

      ```
      # newfs /dev/md/rdsk/d0
      # newfs /dev/rdsk/c1t0d0s4
      ```

   b. Edit the table of file system defaults (`vfstab`) to include the new file systems and mount points:

      ```
      #device   device    mount   FS   fsck    mount mount
      #to mount to fsck point type pass at boot options
      # fd - /dev/fd fd - no -
      /proc - /proc proc - no -
      /dev/dsk/c1t0d0s1 - - swap - no -
      /dev/md/dsk/d0 /dev/md/rdsk/d0 / ufs 1 no -
      swap - /tmp tmpfs - yes -
      /dev/dsk/c1t0d0s4 /dev/rdsk/c1t0d0s4 /globaldevices ufs 1 yes -
      ```

   c. Create and mount the directories included in the `vfstab` in the previous step.

      ```
      # cd /
      # mkdir /globaldevices
      # mount /globaldevices
      ```

      The `/globaldevices` mount point is required for configuring Sun Cluster software.

3. Configure Sun Cluster software on `jesMCS1b`.

   a. Run the Sun Cluster configuration program.

   ```
   # cd /net/installserver/export/jes4/Solaris_sparc/
   Product/sun_cluster/Solaris_10/Tools
   # ./scinstall
   ```

   Choose to add `jesMCS1b` as the first node of a new cluster.

   b. Enter the configuration parameter values shown in the following table:

**Table 6-16** Cluster Node Configuration Parameters

| Parameter | Value |
|---|---|
| Cluster Name | `ha_jesMCSb` |
| Cluster Nodes | `jesMCS1b, jesMCS2b` |
| DES authentication to add nodes | `no` |
| Default network address for cluster transport | `yes` |
| Default Network mask for cluster transport | `yes` |
| Use interconnect cluster transport junction | `no` |
| 1st interconnect cluster transport adapter name | `ce1` |
| 2nd interconnect cluster transport adapter name | `ce5` |
| File system default name (/globaldevices) | `yes` |
| Automatic reboot | `no` |

**c.** Reboot jesMCS1b.

Sun Cluster software creates cluster metadevices that correspond to each of the disks seen by jesMCS1b.

In addition, it replaces the following jesMCS1b mounted file system

```
/dev/dsk/c1t0d0s4 mounted on /globaldevices
```

with

```
/dev/did/dsk/d2s4 mounted on /global/.devices/node@1
```

where d2 is the cluster meta device that corresponds to c1t0d0 on jesMCS1b.

**4.** Repeat Step 1 - Step 3 on jesMCS2b.

When running the scinstall program in Step 3, choose to add jesMCS2b as a node in an existing cluster. Sun Cluster software, as in the case of jesMCS1b, creates cluster metadevices that correspond to each of the disks seen by jesMCS2b. However the storage array disks that are dual ported to both jesMCS1b and jesMCS2b are each assigned only a single cluster metadevice, signifying that Sun Cluster software will regard these as replicated devices corresponding to the same logical device.

In addition, it replaces the following jesMCS2b mounted file system

```
/dev/dsk/c1t0d0s4 mounted on /globaldevices
```

with

```
/dev/did/dsk/d27s4 mounted on /global/.devices/node@2
```

where d27 is the cluster meta device that corresponds to c1t0d0 on jesMCS2b. The scinstall configuration program also configures the private interconnect between jesMCS1b jesMCS2b.

Running the ifconfig command on either node will show the ce1 and ce5 internet adapter in addition to the public internet connection on ce0.

**5.** Complete the configuration of Network Timing Protocol (NTP).

NTP is used to synchronize the time on all cluster nodes. The scinstall configuration program sets up NTP clients for up to 16 cluster nodes. The extra NTP clients can be removed as follows (on both jesMCS1b and jesMCS2b):

**a.** Edit the cluster configuration file:

```
# vi /etc/inet/ntp.conf.cluster
```

**b.** Remove the following entries:

```
peer clusternode3-priv
peer clusternode4-priv
...
peer clusternode16-priv
```

**6.** Add a quorum disk to the cluster.

Sun Cluster software uses quorum vote counts to determine when a cluster is viable. Each functioning node or device gets a vote. To be viable, the cluster must have at least one node and one disk storage device functioning. To set this up, you have to add a quorum disk to the cluster.

**a.** Enter the following command on either `jesMCS1b` or `jesMCS2b`:

```
# /usr/cluster/bin/scsetup
```

**b.** Specify that you want to add a quorum disk.

**c.** The Telco deployment uses `d18` as the global device to use for quorum counts. This cluster meta device on the storage array will be used for the Messaging Server store. Note that the quorum count is set to 2 by default because there are two cluster nodes.

**7.** Set up cluster disk meta sets and mirroring.

Execute the following commands on `jesMCS1b` to set up disk sets that store Messaging Server data (ms_data) and Calendar Server data (cs_data) as mirrored sets.

**a.** Add root to the administrative group.

```
# vi /etc/group and change sysadmin::14: to sysadmin::14:root.
```

**b.** Add the following entries in the /etc/hosts file:

```
192.168.11.7 jesMCS1b.net.telco.com jesMCS1b loghost

192.168.12.5 jesMCSb.net.telco.com jesMCSb
192.168.11.8 jesMCS2b.net.telco.com jesMCS2b
```

**c.** Set up the meta set hosts

```
# metaset -s ms_data -a -h  jesMCS1b jesMCS2b
# metaset -s cs_data -a -h jesMCS1b jesMCS2b
```

**d.** Set up the meta set definitions. In the following example, d18, d19, d20, and d21 are located on storage array A and d22, d23, d24, and d25 are located on storage array B. Two disks on each storage array are used for ms_data and two are used for cs_data.

storage array A:

```
# metaset -s ms_data -a /dev/did/rdsk/d18 /dev/did/rdsk/d19
# metaset -s cs_data -a /dev/did/rdsk/d20 /dev/did/rdsk/d21
```

storage array B:

```
# metaset -s ms_data -a /dev/did/rdsk/d22 /dev/did/rdsk/d23
# metaset -s cs_data -a /dev/did/rdsk/d24 /dev/did/rdsk/d25
```

**e.** Set up disk concatenations corresponding to the meta set definitions.

Note that slice 0 is the only partition used on the disks in our setup.

```
# metainit -s ms_data d71 1 2 /dev/did/rdsk/d18s0
/dev/did/rdsk/d19s0

# metainit -s ms_data d72 1 2 /dev/did/rdsk/d22s0
/dev/did/rdsk/d23s0

# metainit -s cs_data d81 1 2 /dev/did/rdsk/d20s0
/dev/did/rdsk/d21s0

# metainit -s cs_data d82 1 2 /dev/did/rdsk/d24s0
/dev/did/rdsk/d25s0
```

**f.** Set up mirroring between the disk sets on the two storage arrays.

```
# metainit -s ms_data d70 -m d71 d72
# metainit -s cs_data d80 -m d81 d82
```

**g.** Set up dual string mediators. In a two-node cluster, with two external storage disk arrays (two strings of disks, hence the name dual string mediators), a quorum mechanism is needed to determine the viability of disk storage in case of failure. Dual string mediators play a role in that mechanism. (Solaris Volume Manager)

```
# metaset -s ms_data -a -m jesMCS1b jesMCS2b
# metaset -s cs_data -a -m  jesMCS1b jesMCS2b
```

8. Create new cluster file systems and mount corresponding global directories.

   a. Create new cluster file systems.

      These file systems use the mirrored meta sets created in the previous steps.

      ```
      # newfs -f 4096 /dev/md/ms_data/rdsk/d70

      # newfs -f 4096 /dev/md/cs_data/dsk/d80
      ```

   b. Edit the table of file system defaults (`vfstab`) on both `jesMCS1b` and `jesMCS2b` to include the new file systems and mount points:

      ```
      /dev/md/ms_data/dsk/d70 /dev/md/ms_data/rdsk/d70
      /global/jesMCSb/ms_data ufs 1 yes global
      /dev/md/cs_data/dsk/d80 /dev/md/cs_data/rdsk/d80
      /global/jesMCSb/cs_data ufs 1 yes global
      ```

   c. Create and mount the directories included in the `vfstab` in the previous step.

      ```
      # cd /
      # mkdir -p /global/jesMCSb/ms_data
      # mkdir /global/jesMCSb/cs_data
      # chmod 777 /global/jesMCSb/ms_data  /global/jesMCSb/cs_data
      # mount /global/jesMCSb/ms_data
      # mount /global/jesMCSb/cs_data
      ```

9. Create a cluster resource group. The resource group must be associated with a virtual host name and IP address and then brought on line.

   a. Create a resource group called `IMS-RG` and make it visible on `jesMCS1b` and `jesMCS2b`.

      ```
      # cd /usr/cluster/bin
      # ./scrgadm -a -g IMS-RG -h jesMCS1b jesMCS2b
      ```

   b. Identify the resource group with a virtual host name.

      ```
      # ./scrgadm -a -L -g IMS-RG -l jesMCSb
      ```

   c. Bring the resource group online.

      ```
      # ./scswitch -Z -g IMS-RG
      ```

10. Test failover of the cluster resource group.

    a. Check which cluster node is currently active.

    ```
    # ./scstat
    ```

    b. Perform failover.

    Assuming that jesMCS1b is currently active, enter the following command:

    ```
    # ./scswitch -z -g IMS-RG -h  jesMCS2b
    ```

    c. Check which node is currently active.

    ```
    # ./scstat
    ```

## Procedure, Part B: Install and Configure Messaging Server and Calendar Server

1. Disable the Solaris `sendmail` service on `jesMCS1b`.

   The Solaris `sendmail` service is a message transfer agent that listens on port 25, the standard SMTP port (see Table 5-3 on page 67). If not disabled, `sendmail` would conflict with Messaging Server's MTA component. Use the following procedure on the Solaris 10 platform:

   a. Look for the sendmail process:

   ```
   # svcs | grep -i sendmail
   ```

   b. You receive a response similar to the following.

   ```
   online Nov_21 svc:/network/smtp:sendmail
   ```

   c. Disable the service.

   ```
   # svcadm disable svc:/network/smtp:sendmail
   ```

2. Install Java ES software on `jesMCS1b`.

   Use the Configure Later option of the Java ES installer.

   a. Select the following components:

   - Messaging Server
   - Calendar Server
   - Administration Server

**b.** Specify that Administration Server will use a remote Directory Server instance.

**c.** Enter the Messaging Server and Calendar Server installation parameter values shown in the following table:

**Table 6-17** Messaging Server and Calendar Server Parameters

| Parameter | Value |
|---|---|
| Messaging Server Installation Directory | `/global/jesMCSb/ms_data/opt/SUNWmsgsr` |
| Calendar Server Installation Directory | `/global/jesMCSb/cs_data/opt` |
| **Common Configuration Settings** | |
| Host Name | `jesMCS1b` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.7` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **Administration Server: Server Settings** | |
| Admin Server Installation Directory | `/global/jesMCSb/ms_data/var/opt/mps/serverroot` |
| Admin Server Port | `390` |
| Admin Server Administration Domain | `net.telco.com` |
| System User | `root` |
| System Group | `root` |
| **Administration Server: Configuration Directory Settings** | |
| Configuration Directory Admin User ID | `admin` |
| Configuration Directory Admin Password | `password` |
| Configuration Directory Host | `jesDPA.net.telco.com` |
| Configuration Directory Port | `389` |

**3.** Configure Messaging Server.

**a.** Modify the /etc/hosts file on jesMCS1b to include the following entries:

```
192.168.12.5     jesMCSb.net.telco.com jesMCSb
192.168.11.7     jesMCS1b.net.telco.com jesMCS1b loghost
192.168.11.8       jesMCS2b.net.telco.com jesMCS2b
```

**b.** Run the Messaging Server configuration program.

```
# cd /global/jesMCSb/ms_data/opt/SUNWmsgsr/sbin
# ./configure -nodisplay
```

**c.** Provide the following parameters requested by the configuration program:

**Table 6-18** Messaging Server Configuration Parameters

| Parameter | Value |
|---|---|
| Fully Qualified Host Name | jesMCS1b.net.telco.com |
| Directory for configuration and data files | /global/jesMCSb/ms_data/var/opt/SUNWmsgsr |
| Component Selection | Message Transfer Agent (MTA)<br>Message Store<br>Messenger Express (MEM) |
| Administrator Username | mailsrv |
| Administrator Unix group | mail |
| LDAP configuration directory URL:port | ldap://jesDPA.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| LDAP user/group directory URL:port | ldap://jesDPA.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| Postmaster email address | root@jesMCSb.net.telco.com |
| Password | password |
| Email default domain | telcomail.com |
| Organization DN | o=telcomail.com,dc=net,dc=telco,dc=com |

**d.** Set configuration parameters and files to the virtual jesMCSb IP address rather than the physical IP address.

- Run the ha_ip_config script to set configure the dispatcher.cnf and job_controller.cnf files for high availability and to set a number of configutil parameters.

  ```
  # ./ha_ip_config
  ```

  Provide the following parameters as requested:

  ```
  Logical IP address: 192.168.12.5
  iMS server root: /global/jesMCSb/ms_data/opt/SUNWmsgsr
  ```

- Modify two additional configutil parameters by hand:

  ```
  # cd /global/jesMCSb/ms_data/opt/ms_data/SUNWmsgsr/sbin
  # ./configutil -o local.hostname -v jesMCSb.net.telco.com
  # ./configutil -o local.servername -v jesMCSb.net.telco.com
  ```

**e.** Configure Messaging Server to support Access Manager single sign-on.

Set the following Messaging Server configutil parameters to enable support for Access Manager's cookie-based single sign-on when messaging services are accessed in a web browser.

```
# cd /global/jesMCSb/ms_data/opt/ms_data/SUNWmsgsr/sbin

# ./configutil -o local.webmail.sso.amnamingurl
   -v http://jesPAM.net.telco.com/amserver/namingservice

# ./configutil -o local.webmail.sso.amcookiename
   -v iPlanetDirectoryPro

# ./configutil -o local.webmail.sso.amloglevel -v 5

# ./configutil -o local.webmail.sso.singlesignoff -v 1
```

**4.** Start the Messaging Server

```
# cd /global/jesMCSb/ms_data/opt/ms_data/SUNWmsgsr/sbin
# ./start-msg
```

**5.** Verify that Messaging Server is properly configured.

- Start the web browser.
- Connect to http://jesMCSb.net.telco.com. Note that the jesMCSb.net.telco.com virtual service must be configured at this point.

- Log in to mail server as user=admin, password=password.
- Send a test email message to Store.Administrator@telcomail.com.
- Check that a new mail arrives in the inbox.

**6.** Configure Calendar Server.

**a.** Run the Calendar Server configuration program on jesMCS1b.

```
# cd /global/jesMCSb/cs_data/opt/SUNWics5/cal/sbin
# sh ./csconfigurator.sh -nodisplay
```

**b.** Provide the following parameters requested by the configuration program:

**Table 6-19** Calendar Server Configuration Parameters

| Parameter | Value |
|---|---|
| LDAP Server Host Name | jesDPA.net.telco.com |
| LDAP Server Port | 389 |
| Directory Manager DN | cn=Directory Manager |
| Directory Manager Password | password |
| Base DN | o=telcomail.com,dc=net,dc=telco,dc=com |
| Calendar Server administrator | calmaster |
| Calendar Server administrator password | password |
| Email Alarms | Enabled |
| Administrator Email Address | root@jesMCS1b.net.telco.com |
| SMTP Host Name | jesMCSb.net.telco.com |
| Service Port | 82 |
| Maximum Sessions | 5000 |
| Maximum Threads | 20 |
| Number of server processes | 4 |
| Runtime User ID | icsuser |
| Runtime Group ID | icsgroup |

**Table 6-19** Calendar Server Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| Start After Successful Configuration | Yes |
| Start on System Startup | Yes |
| Config Directory | /global/jesMCSb/cs_data/etc/opt/SUNWics5/config |
| Database Directory | /global/jesMCSb/cs_data/var/opt/SUNWics5/csdb |
| Logs Directory | /global/jesMCSb/cs_data/var/opt/SUNWics5/logs |
| Temporary Files Directory | /global/jesMCSb/cs_data/var/opt/SUNWics5/tmp |
| Enable Archiving | Yes |
| Path Where You Want Archives to be Stored | /global/jesMCSb/cs_data/var/opt/SUNWics5/csdb/archive |
| Min Number of Days to Keep Hot Backups | 3 |
| Max Number of Days to Keep Hot Backups | 6 |
| Do You Want to Enable Hot Backup | No |

**c.** Set configuration parameters and files to the virtual `jesMCSb` IP address rather than the physical IP address.

Edit the Calendar Server configuration file, `/global/jesMCSb/cs_data/etc/opt/SUNWics5/config/ics.conf`, as follows:

- Add the following parameters:

```
local.server.ha.enabled = "yes"
local.server.ha.agent = "SUNWscics"
```

- Rename the `service.listenaddr` parameter to `service.http.listenaddr` and then set the parameter to the IP address of the virtual host:

```
service.http.listenaddr = 192.168.12.5
```

- Change all parameters that refer to a local host name to the virtual host name:

```
local.hostname = "jesMCSb"
local.servername = "jesMCSb"
service.ens.host = "jesMCSb"
service.http.calendarhostname = "jesMCSb"
```

**d.** Configure Calendar Server to support Access Manager single sign-on.

Set the following Calendar Server parameters to enable support for Access Manager's cookie-based single sign-on when calendar services are accessed in a web browser. Set the following parameters in the `/global/jesMCSb/cs_data/etc/opt/SUNWics5/config/ics.cnf` file:

```
local.calendar.sso.amnamingurl="http://jesPAM.net.telco.com/amserver/naмingservice"

local.calendar.sso.amcookiename=iPlanetDirectoryPro

local.calendar.sso.logname=am_sso.log

local.calendar.sso.singlesignoff=true

sso.enable = "0"

service.http.allowadminproxy="yes"

service.http.ipsecurity="no"
```

(Setting `sso.enable` to `0` turns off Calendar Server's legacy Trusted Circle single sign-on mechanism and permits Access Manager single sign-on. Setting `allowadminproxy` and `ipsecurity` enables the Portal Server SSO adapters to operate.)

**7.** Start the Calendar Server.

```
# cd /global/jesMCSb/cs_data/opt/SUNWics5/cal/sbin
# ./start-cal
```

**8.** Verify that Calendar Server is properly configured.

- Start browser.
- Connect to `http://jesMCSb.net.telco.com:82`
- Log in as user=`calmaster`, password=`password`.
- Check that the calendar page comes up.

**9.** Create a Calendar Server user, user group, and directory on `jesMCS2b.net.telco.com`.

(The configuration program did this automatically on `jesMCS1b`.)

```
# groupadd -g 103 icsgroup
# useradd -u 104 -g 103 -d /home/icsuser icsuser
# cd /home
# mkdir icsuser
# chown icsuser icsuser
```

## Procedure, Part C: Configure Sun Cluster Resources

**1.** Install Java ES software on `jesMCS1b`.

Use the Configure Later option of the Java ES installer.

Select the following components:

- Sun Cluster Agent for Messaging Server
- Sun Cluster Agent for Calendar Server

**2.** Configure the Messaging Server resource.

**a.** Register the Messaging Server cluster agent.

```
# cd /usr/cluster/bin/
# ./scrgadm -a -t SUNW.ims
```

`SUNW.ims` is the Messaging Server cluster agent.

**b.** Create a Messaging Server resource and add it to the cluster resource group.

```
# ./scrgadm -a -j ims-rs -t SUNW.ims -g IMS-RG \
   -x IMS_serverroot=/global/jesMCSb/ms_data/opt/SUNWmsgsr \
   -y Resource_dependencies=jesMCSb
```

`ims-rs` is the name of the Messaging Server resource.

**c.** Enable the Messaging Server resource.

```
# ./scswitch -e -j ims-rs
```

**d.** Test failover of the Messaging Server resource from `jesMCS1b` to `jesMCS2b`.

```
# ./scswitch -z -g IMS-RG -h jesMCS2b
```

On `jesMCS1b`, you see the following messages written to the console:

```
Connecting to watcher ...
shutting down all servers...
Stopping job_controller server 2468 .... done
Stopping dispatcher server 2464 ... done
Stopping sched server 2462 ... done
Stopping http server 2460 ... done
Stopping pop server 2457 ... done
Stopping imap server 2454 ... done
Stopping store server 2451 .... done
Stopping ens server 2450 .... done
stopping watcher process 2443 ... done
Oct 13 08:25:22 jesMCS1b ip: TCP_IOC_ABORT_CONN: local =
129.148.008.109:0, remote = 000.000.000.000:0, start = -2, end = 6
Oct 13 08:25:22 jesMCS1b ip: TCP_IOC_ABORT_CONN: aborted 2 connections
```

On `jesMCS2b`, you see the following messages written to the console:

```
Starting the watcher....
Connecting to watcher ...
Launching watcher ...
Oct 13 08:25:42 jesMCS2B SC[SUNW.ims,IMS-RG,ims-rs,ims_svc_start]:
Starting the rest of the messaging services....
Connecting to watcher ...
Starting ens server .... 7950
Starting store server .... 7951
checking store server status ..... ready
Starting imap server ...... 7953
Starting pop server .... 7956
Starting http server .... 7959
Starting sched server .... 7961
Starting dispatcher server .... 7963
Starting job_controller server .... 7969
```

**3.** Configure the Calendar Server resource.

**a.** Register the Calendar Server cluster agent.

```
# cd /usr/cluster/bin/
# ./scrgadm -a -t SUNW.scics
```

`SUNW.scics` is the Calendar Server cluster agent.

**b.** Create a Calendar Server resource and add it to the cluster resource group.

```
# ./scrgadm -a -j scics-rs -t SUNW.scics -g IMS-RG \
   -x Confdir_list=/global/jesMCSb/cs_data \
   -y Resource_dependencies=jesMCSb -y Port_list=82/tcp
```

`scics-rs` is the name of the Calendar Server resource.

**c.** Enable the Calendar Server resource.

```
# ./scswitch -e -j scics-rs
```

**d.** Check the status of the Sun Cluster resource group.

```
# ./scstat
```

The output from this command is displayed and described in "Sample User Provisioning Script" on page 161.

# Module #6 Consumer-class Messaging Server on Sun Cluster Nodes

In this module you set up the Messaging Server instances that support the `telco.net` email domain for consumer-class users. These instances are installed and configured to run on Sun Cluster nodes. The messaging service thereby becomes a resource managed by the Sun Cluster software. The procedure is similar to the procedure for the business-class messaging and calendar services that is described in "Module #5: Business-class Messaging Server and Calendar Server on Sun Cluster Nodes" on page 108. The procedure is relatively complex, and requires you to run the Java ES installer three times on each computer.

## Installation and Configuration Summary

The installation and configuration procedures are divided into three parts. The procedures are summarized as follows:

**Part A: Basic Sun Cluster Setup**

1. Repeat the steps in "Procedure, Part A: Set Up Sun Cluster Nodes and Global File System" on page 110.

**Part B: Install and Configure Messaging Server**

1. "Disable the Solaris `sendmail` service on `jesMS1c`." on page 126
2. "Install Java ES software on `jesMS1c`." on page 126

3. “Configure Messaging Server.” on page 128.
4. “Start the Messaging Server” on page 129
5. “Verify that Messaging Server is properly configured.” on page 129

**Part C: Configure Sun Cluster Resources**

1. “Install Java ES software on jesMS1c.” on page 130
2. “Configure the Messaging Server resource.” on page 130

## Procedure, Part A: Set Up Sun Cluster Nodes and Global Filesystem

Setting up Sun Cluster nodes and global filesystems on jesMS1c and jesMS2c is almost identical to the procedure for the business class service.

1. Repeat Step 1 through Step 10 in “Procedure, Part A: Set Up Sun Cluster Nodes and Global File System” on page 110 on jesMS1c and jesMS2c. Modify the hostnames and other parameter whenever it is necessary.

## Procedure, Part B: Install and Configure Messaging Server

1. Disable the Solaris sendmail service on jesMS1c.

   The Solaris sendmail service is a message transfer agent that listens on port 25, the standard SMTP port. If not disabled, sendmail would conflict with Messaging Server’s MTA component. Use the following procedure on the Solaris 10 platform:

   a. Identify the sendmail service.

      ```
      # svcs | grep -i sendmail
      ```

   b. You receive a response similar to the following.

      ```
      online Nov_21 svc:/network/smtp:sendmail
      ```

   c. Disable the service.

      ```
      # svcadm disable svc:/network/smtp:sendmail
      ```

2. Install Java ES software on jesMS1c.

   Use the Configure Later option of the Java ES installer.

   a. Select the following components:

      - Messaging Server
      - Administration Server

**b.** Specify that Administration Server will use a remote Directory Server instance.

**c.** Enter the Messaging Server installation parameter values shown in the following table:

**Table 6-20** Messaging Server Installation Parameters

| Parameter | Value |
|---|---|
| Messaging Server Installation Directory | `/global/jesMSc/ms_data/opt/SUNWmsgsr` |
| **Common Configuration Settings** | |
| Host Name | `jesMS1c` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.9` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **Administration Server: Server Settings** | |
| Admin Server Installation Directory | `/global/jesMSc/ms_data/var/opt/mps/serverroot` |
| Admin Server Port | `390` |
| Admin Server Administration Domain | `net.telco.com` |
| System User | `root` |
| System Group | `root` |
| **Administration Server: Configuration Directory Settings** | |
| Configuration Directory Admin User ID | `admin` |
| Configuration Directory Admin Password | `password` |
| Configuration Directory Host | `jesDPA.net.telco.com` |
| Configuration Directory Port | `389` |

**3.** Configure Messaging Server.

**a.** Modify the /etc/hosts file on jesMS1c to include the following entries:

```
192.168.12.6     jesMSc.net.telco.com jesMSc
192.168.11.9     jesMS1c.net.telco.com jesMS1c loghost
192.168.11.10       jesMS2c.net.telco.com jesMS2c
```

**b.** Run the Messaging Server configuration program.

```
# cd /global/jesMSc/ms_data/opt/SUNWmsgsr/sbin
# ./configure -nodisplay
```

**c.** Provide the following parameters requested by the configuration program:

**Table 6-21** Messaging Server Configuration Parameters

| Parameter | Value |
|---|---|
| Fully Qualified Host Name | jesMS1c.net.telco.com |
| Directory for configuration and data files | /global/jesMSc/ms_data/var/opt/SUNWmsgsr |
| Component Selection | Message Transfer Agent (MTA)<br>Message Store<br>Messenger Express (MEM) |
| Administrator Username | mailsrv |
| Administrator Unix group | mail |
| LDAP configuration directory URL | ldap://jesDPA.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| LDAP user/group directory URL | ldap://jesDPA.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| Postmaster email address | root@jesMSc.net.telco.com |
| Password | password |
| Email default domain | telco.net |
| Organization DN | o=telco.net,dc=net,dc=telco,dc=com |

**d.** Set configuration parameters and files to use the virtual service IP address jesMSc rather than the physical IP address.

- Run the ha_ip_config script to set configure the dispatcher.cnf and job_controller.cnf files for high availability and to set a number of configutil parameters.

```
# ./ha_ip_config
```

Provide the following parameters as requested:

```
Logical IP address: 192.168.12.6
iMS server root: /global/jesMSc/ms_data/opt/SUNWmsgsr
```

- Modify two additional configutil parameters by hand:

```
# cd /global/jesMSc/ms_data/opt/ms_data/SUNWmsgsr/sbin
# ./configutil -o local.hostname -v jesMSc.net.telco.com
# ./configutil -o local.servername -v jesMSc.net.telco.com
```

**e.** Configure Messaging Server to support Access Manager single sign-on.

For Messaging Server to support cookie-based single sign-on by way of Access Manager from a browser, the following configutil parameters need to be set.

```
# cd /global/jesMSc/ms_data/opt/ms_data/SUNWmsgsr/sbin

# ./configutil -o local.webmail.sso.amnamingurl
   -v http://jesPAM.net.telco.com/amserver/namingservice

# ./configutil -o local.webmail.sso.amcookiename
   -v iPlanetDirectoryPro

# ./configutil -o local.webmail.sso.amloglevel -v 5

# ./configutil -o local.webmail.sso.singlesignoff -v 1
```

**4.** Start the Messaging Server

```
# cd /global/jesMSc/ms_data/opt/ms_data/SUNWmsgsr/sbin
# ./start-msg
```

**5.** Verify that Messaging Server is properly configured.

- Start the web browser.
- Connect to http://jesMSc.net.telco.com
- Log in to mail server as user=admin, password=password.
- Send a test email message to Store.Administrator@telco.net.

## Procedure, Part C: Configure Sun Cluster Resources

**1.** Install Java ES software on `jesMS1c`.

Use the Configure Later option of the Java ES installer.

Select the following components:

- Sun Cluster Agent for Messaging Server

**2.** Configure the Messaging Server resource.

**a.** Register the Messaging Server cluster agent:

```
# cd /usr/cluster/bin/
# ./scrgadm -a -t SUNW.ims
```

where `SUNW.ims` is the Messaging Server cluster agent.

**b.** Create a Messaging Server resource and add it to the cluster resource group:

```
# ./scrgadm -a -j ims-rs -t SUNW.ims -g IMS-RG \
   -x IMS_serverroot=/global/jesMSc/ms_data/opt/SUNWmsgsr \
   -y Resource_dependencies=jesMSc
```

where `ims-rs` is the name of the Messaging Server resource.

**c.** Enable the Messaging Server resource.

```
# ./scswitch -e -j ims-rs
```

**d.** Test failover of the Messaging Server resource from `jesMS1c` to `jesMS2c`.

```
# ./scswitch -z -g IMS-RG -h jesMS2c
```

On `jesMS1c`, you see the following messages written to the console:

```
Connecting to watcher ...
shutting down all servers...
Stopping job_controller server 2468 .... done
Stopping dispatcher server 2464 ... done
Stopping sched server 2462 ... done
Stopping http server 2460 ... done
Stopping pop server 2457 ... done
Stopping imap server 2454 ... done
Stopping store server 2451 .... done
Stopping ens server 2450 .... done
stopping watcher process 2443 ... done
Oct 13 08:25:22 jesMS1c ip: TCP_IOC_ABORT_CONN: local =
129.148.008.109:0, remote = 000.000.000.000:0, start = -2, end = 6
Oct 13 08:25:22 jesMS1c ip: TCP_IOC_ABORT_CONN: aborted 2 connections
```

On jesMS2c, you see the following messages written to the console:

```
Starting the watcher....
Connecting to watcher ...
Launching watcher ...
Oct 13 08:25:42 jesMS2c SC[SUNW.ims,IMS-RG,ims-rs,ims_svc_start]:
Starting the rest of the messaging services....
Connecting to watcher ...
Starting ens server .... 7950
Starting store server .... 7951
checking store server status ..... ready
Starting imap server ...... 7953
Starting pop server .... 7956
Starting http server .... 7959
Starting sched server .... 7961
Starting dispatcher server .... 7963
Starting job_controller server .... 7969
```

# Module #7 Portal Server Secure Remote Access

In this module you install and configure Portal Server Secure Remote Access. You run the Java ES installer twice on each computer. First you install the Portal Server Secure Remote Access core on jesPAM1 and jesPAM2. Then you install the Portal Server Secure Remote Access gateway on jesSRA1 and jesSRA1. The gateway instances on jesSRA1 and jesSRA2 are load-balanced, and appear to the outside world as a single logical service named jesSRA.

## Installation and Configuration Summary

The installation and configuration procedures are summarized as follows:



## Procedure

1. Install Java ES software on jesPAM1.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Portal Server Secure Remote Access

**b.** Select the following sub-components of Portal Server Secure Remote Access:

- Secure Remote Access Core

**c.** Enter the configuration parameter values shown in the following table:

**Table 6-22** Portal Server Secure Remote Access Configuration Parameters

| Parameter | Value |
|---|---|
| Portal Server Secure Remote Access Installation Directory | `/global/jesPAM1/opt` |
| Portal Server Installation Directory | `/global/jesPAM1/opt` |
| **Common Configuration Settings** | |
| Host Name | `jesPAM1` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.5` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **Portal Server Secure Remote Access: Access Manager** | |
| Administrator Password | `password` |
| Directory Manager DN | `cn=Directory Manager` |
| Directory Manager Password | `password` |
| **Portal Server Secure Remote Access: Gateway Information** | |
| Portal Server Domain | `net.telco.com` |
| Gateway Protocol | `HTTPS` |
| Gateway Domain | `net.telco.com` |
| Gateway Port | `443` |
| Gateway Profile Name | `default` |
| Log User Password | `password` |

2. Restart the Web Server on jesPAM1.

```
# cd /global/jesPAM1/opt/SUNWwbsvr/https-jesPAM1.net.telco.com
# ./stop
# ./start
```

3. Repeat Step 1 and Step 2 on jesPAM2.

4. Install Java ES software on jesSRA1.

   Use the Configure Now option of the Java ES installer. Note that you must run the installer in graphical mode, and not in command line mode (the -nodisplay option) when you install Portal Server Secure Remote Access.

   a. Select the following components:

      - Access Manager
      - Portal Server Secure Remote Access

   b. Select the following sub-components of Access Manager:

      - Access Manager SDK

   c. Select the following sub-components of Portal Server Secure Remote Access:

      - Secure Remote Access Gateway

   d. Enter the configuration parameter values shown in the following table:

**Table 6-23** Access Manager SDK and Portal Server Secure Remote Access Configuration Parameters

| Parameter | Value |
|---|---|
| Access Manager Installation Directory | /global/jesSRA1/opt |
| Portal Server Secure Remote Access Installation Directory | /global/jesSRA1/opt |
| **Common Configuration Settings** | |
| Host Name | jesSRA1 |
| DNS Domain Name | net.telco.com |
| IP Address | 192.168.13.9 |
| Administrator User ID | admin |
| Administrator Password | password |
| System User | root |

**Table 6-23** Access Manager SDK and Portal Server Secure Remote Access Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| System Group | root |
| **Access Manager: Administration** | |
| Administrator User ID | amAdmin |
| Administrator Password | password |
| LDAP User ID | amldapuser |
| LDAP Password | password1 |
| Password Encryption Key | password |
| Install Type | legacy |
| **Access Manager: Directory Server Information** | |
| Directory Server Host | jesDPD.net.telco.com |
| Server Port | 389 |
| Root Suffix | dc=net,dc=telco,dc=com |
| Directory Manager DN | cn=Directory Manager |
| Directory Manager Password | password |
| **Access Manager: Directory Server** | |
| Is Directory Provisioned With User Data | Yes |
| Organization Marker Object Class | sunISManagedOrganization |
| Organization Naming Attribute | o |
| User Marker Object Class | inetorgperson |
| User Naming Attribute | uid |
| **Access Manager: Web Container** | |
| Host Name | jesPAM.net.telco.com |
| Services Deployment URI | amserver |
| Cookie Domain | .net.telco.com |
| Services Port | 80 |
| Server Protocol | HTTP |

**Table 6-23** Access Manager SDK and Portal Server Secure Remote Access Configuration Parameters *(Continued)*

| Parameter | Value |
|---|---|
| **Portal Server Secure Remote Access: Web Container** | |
| Protocol | HTTP |
| Host Name | jesPAM.net.telco.com |
| Port | 80 |
| Deployment URI | /portal |
| **Portal Server Secure Remote Access: Gateway** | |
| Protocol | HTTPS |
| Hostname | jesSRA1 |
| Subdomain | |
| Domain | net.telco.com |
| Host IP Address | 192.168.13.9 |
| Access Port | 443 |
| Gateway Profile Name | default |
| Log User Password | password |
| **Portal Server Secure Remote Access: Certificate** | |
| Organization | telcomail.com |
| Division | mydivision |
| City | mycity |
| State | mystate |
| Country Code | US |
| Certificate Database Password | password |

**5.** Set up the gateway configuration parameters.

**a.** Log in to the Access Manager administration console (amconsole):

http://jesPAM.net.telco.com/amconsole

**b.** In the left pane, under Organizations, click telcomail.com.

**c.** Click Services.

**d.** Click Register SRA Services.

**e.** Select Access List and Net file.

**f.** Click Register.

**g.** Confirm that the following services are selected:

- Access Manager Configuration

  Core

  LDAP

- Portal Server Configuration

  Portal Desktop

  SSO Adapter

- SRA Configuration

  Access List

  Netfile

**h.** Click the Services tab.

**i.** In the left pane locate the Gateway Service. Click the arrow that follows the name.

**j.** In the right pane (Gateway Profile), click Default Profile.

**k.** Locate the Portal Servers field. Confirm that only the following are listed:

- `http://jesPAM.net.telco.com:80`
- `http://jesPAM.net.telco.com`

**l.** Locate the URLs to Which User Session Cookie is Forwarded field. Confirm that only the following are listed:

- `http://jesPAM.net.telco.com:80`
- `http://jesPAM1.net.telco.com:80`
- `http://jesPAM2.net.telco.com:80`
- `http://jesPAM.net.telco.com`
- `http://jesPAM1.net.telco.com`
- `http://jesPAM2.net.telco.com`
- `http://jesMCSb.net.telco.com:80`

- `http://jesMCSb.net.telco.com:82`
- `http://jesMCSb.net.telco.com`

**m.** Select Enable Cookie Management.

**n.** Click Save.

**o.** Select Platform Service.

**p.** Add telcomail.com to the SRA Cookies Domain. The list should include the following:

- `.net.telco.com`
- `.telcomail.com`

**q.** Click Save.

**6.** Edit the gateway configuration file on `jesSRA1`.

The configuration file is `/etc/opt/SUNWps/platform.conf.default`.

**a.** Modify the following line:

```
gateway.virtualhost=jesSRA.net.telco.com 192.168.14.4
www.telcomail.com
```

This enables the load balancer URL `www.telcomail.com` at 192.168.14.4.

**b.** Add the following line:

```
gateway.ignoreServerList=true
```

**c.** Make certain that all entries in `platform.conf.default` for the portal specify the load balancer's URL or IP address. For example:

```
gateway.dsame.agent=http\://jesPAM.net.telco.com\:80/portal/Remo
teConfigServlet

portal.server.host=jesPAM.net.telco.com
```

**7.** Restart the portal server instances on `jesPAM1`.

```
# cd /global/jesPAM1/opt/SUNWwbsvr/https-jesPAM1.net.telco.com
# ./stop
# ./start
```

8. Start the gateway on jesSRA1.

```
# cd /global/jesSRA1/opt/SUNWps/bin
# ./gateway -n default stop
# ./gatway -n default start
```

9. Verify that the gateway is operating correctly.

   a. Configure the jesSRA load balancer. For more information, see "Configuring the Load Balancers" on page 73.

   b. In your web browser, open https://www.telcomail.com.

   c. Log in as buser0001 (the password is password).

      If you succeed, the gateway is operating correctly.

10. Repeat Step 4 throughStep 9 on jesSRA2.

# Module #8 Delegated Administrator Console on Web Server

In this module you install and configure the Delegated Administrator console. The Delegated Administrator console must be installed with a web container. The Delegated Administrator console also has a dependency on the Access Manager SDK.

This procedure requires you to run the Java ES installer twice. First, you install Access Manager SDK and Web Server on jesADM. Next, you install the Delegated Administrator console. To complete the procedure, you run the Delegated Administrator configuration program.

## Installation and Configuration Summary

The installation and configuration procedures are summarized as follows:

1. "Install Java ES software on jesADM." on page 140
2. "Start Web Server on jesADM." on page 142
3. "Install Java ES software on jesADM." on page 142
4. "Configure Delegated Administrator on jesADM." on page 143
5. "Restart Web Server on jesADM." on page 143
6. "Verify that Delegated Administrator is operating properly." on page 143

## Procedure

1. Install Java ES software on `jesADM`.

   Use the Configure Now option of the Java ES installer.

   a. Select the following components:

      - Web Server
      - Access Manager

   b. Select the following sub-components of Access Manager:

      - Access Manager SDK

   c. Enter the configuration parameter values shown in the following table:

**Table 6-24** Web Server and Access Manager Parameters

| Parameter | Value |
|---|---|
| Web Server Root | `/global/jesADM/opt/SUNWwbsvr` |
| Access Manager Installation Directory | `/global/jesADM/opt` |
| **Common Configuration Settings** | |
| Host Name | `jesADM` |
| DNS Domain Name | `net.telco.com` |
| IP Address | `192.168.11.11` |
| Administrator User ID | `admin` |
| Administrator Password | `password` |
| System User | `root` |
| System Group | `root` |
| **Web Server: Administration** | |
| Server Admin User ID | `admin` |
| Admin User's Password | `password` |
| Host Name | `jesADM.net.telco.com` |
| Administration Port | `8888` |
| Administration Server User ID | `root` |
| **Default Web Server Instance** | |
| System User ID | `root` |

**Table 6-24** Web Server and Access Manager Parameters *(Continued)*

| Parameter | Value |
|---|---|
| System Group | root |
| HTTP Port | 80 |
| Content Root | /global/jesADM/opt/SUNWwbsvr/docs |
| Do you want to automatically restart Web Server when system restarts? | Yes |
| **Access Manager: Administration** | |
| Administrator User ID | amAdmin |
| Administrator Password | password |
| LDAP User ID | amldapuser |
| LDAP Password | password1 |
| Password Encryption Key | password |
| Install Type | legacy |
| **Access Manager: Directory Server** | |
| Directory Server Host | jesDPA.net.telco.com |
| Directory Server Port | 389 |
| Directory Root Suffix | dc=net,dc=telco,dc=com |
| Directory Manager DN | cn=Directory Manager |
| Directory Manager Password | password |
| **Access Manager: Directory Server Information** | |
| Directory Server Provisioned With Users | Yes |
| Organization Marker Object Class | sunISManagedOrganization |
| Organization Naming Attribute | o |
| User Marker Object Class | inetorgperson |
| User Naming Attribute | uid |
| **Access Manager: Web Container** | |
| Host Name | jesPAM.net.telco.com |
| Services Deployment URI | amserver |

**Table 6-24** Web Server and Access Manager Parameters *(Continued)*

| Parameter | Value |
|---|---|
| Cookie Domain | .net.telco.com |
| Services Port | 80 |
| Server Protocol | HTTP |

2. Start Web Server on jesADM.

```
# cd /global/jesADM/opt/SUNWwebsvr/https-jesADM.net.telco.com
# ./stop
# ./start
```

3. Install Java ES software on jesADM.

   Use the Configure Later option of the Java ES installer.

   a. Select the following components:

      - Communications Services Delegated Administrator

   b. Select the following sub-components of Delegated Administrator:

      - Delegated Administrator Console and Utility

   c. Enter the configuration parameter values shown in the following table:

**Table 6-25** Delegated Administrator Configuration Parameters

| Parameter | Value |
|---|---|
| Directory Preparation Tool Installation Directory | /global/jesADM/opt/SUNWcomds |
| Access Manager Installation Directory | /global/jesADM/opt |
| Delegated Administrator Server Installation Directory | /global/jesAMD/opt/SUNWcomm |

4. Configure Delegated Administrator on jesADM.

   a. Run the Delegated Administrator configuration program:

   ```
   # cd /global/jesADM/opt/SUNWcomm/sbin
   # ./config-commda -nodisplay
   ```

   b. Enter the configuration parameter values shown in the following table:

**Table 6-26** Delegated Administrator Configuration Parameters

| Parameter | Value |
|---|---|
| Configuration and Data Files Directory | /global/jesADM/var/opt/SUNWcomm |
| Delegated Administrator Components | Delegated Administrator Console |
| Access Manager Host Name | jesPAM.net.telco.com |
| Access Manager Port | 80 |
| Deploy Delegated Administrator Console On | WEB |
| Web Server Root Directory | /global/jesADM/opt/SUNWwbsvr |
| Web Server Instance Identifier | jesADM.net.telco.com |
| Virtual Server Identifier | https-jesADM.net.telco.com |
| Web Server HTTP Port | 80 |
| Domain Separator | @ |

5. Restart Web Server on jesADM.

```
# cd /global/jesADM/opt/SUNWwebsvr/https-jesADM.net.telco.com
# ./stop
# ./start
```

6. Verify that Delegated Administrator is operating properly.

   a. In your web browser, open the following URL:

   http://jesadm.net.telco.com/da/DA/Login

   b. Login with user ID amadmin, password of password.

   Logging in successfully verifies that Delegated Administrator console is operating properly.

# Module #9: Load Balanced Messaging Server MTA (Inbound and Outbound)

In this module you install and configure the Messaging Server MTA instances that function as the inbound message relay and outbound message relay. You do not perform any special configuration for these instances to operate correctly with the load balancer. You simply configure the load balancer. For more information, see "Configuring the Load Balancers" on page 73.

The installation and configuration procedures for the MTA inbound and MTA outbound instances are very similar. The one notable difference is that the MTA inbound is configured to interact with the back-end MTA using LMTP protocols, rather than SMTP protocols, while the MTA outbound does not interact with the back-end MTA, and is therefore not configured to use LMTP.

This module is divided into two separate parts. Part A describes installing and configuring the MTA inbound instances. Part B describes installing and configuring the MTA outbound instances.

## Installation and Configuration Summary

**Part A: Messaging Server MTA Inbound**

1. "Disable the Solaris `sendmail` service on `jesIMR1`." on page 145
2. "Install Java ES software on `jesIMR1`." on page 145
3. "Configure Messaging Server MTA." on page 145
4. "Enable the LMTP protocol." on page 146
5. "Start the Messaging Server MTA on `jesIMR1`." on page 147
6. "Verify the operation of Messaging Server MTA." on page 147
7. "Repeat Step 1 - Step 6 on `jesIMR2`." on page 147
8. "Verify load balancing for Messaging Server MTA inbound." on page 147

**Part B: Messaging Server MTA Outbound**

1. "Install and configure the Messaging Server Message Transfer Agent software on `jesOMR1`." on page 148
2. "Install and configure the Messaging Server Message Transfer Agent software on `jesOMR2`." on page 148
3. "Verify load balancing for Messaging Server MTA outbound." on page 148

## Procedure, Part A: Messaging Server-MTA Inbound

1. Disable the Solaris sendmail service on jesIMR1.

   The Solaris sendmail service is a message transfer agent that listens on port 25, the standard SMTP port. If not disabled, sendmail would conflict with the Messaging Server MTA component.

   Use the following procedure on the Solaris 10 platform.

   a. Look for the sendmail process:

   ```
   # svcs | grep -i sendmail

       online          2:05:09 svc:/network/smtp:sendmail
       svcs -l  svc:/network/smtp:sendmail
       fmri         svc:/network/smtp:sendmail
       name         sendmail SMTP mail transfer agent
       enabled      true
       state        online
   ```

   b. Disable sendmail.

   ```
   # svcadm disable svc:/network/smtp:sendmail
   ```

2. Install Java ES software on jesIMR1.

   Use the Configure Later option of the Java ES installer.

   a. Select the Messaging Server component.

   b. Enter the Messaging Server root parameter value:
   /global/jesIMR1/opt/SUNWmsgsr

3. Configure Messaging Server MTA.

   a. Modify the /etc/hosts file on jesIMR1 to include the following entries:

   ```
   192.168.14.5       smtp.telcomail.com
   192.168.14.9       smtp.telco.net
   192.168.13.3       jesIMR1.net.telco.com jesIMR1 loghost
   192.168.13.4         jesIMR2.net.telco.com jesIMR2
   ```

   b. Run the Messaging Server configuration program.

   ```
   # cd /global/jesIMR1/opt/SUNWmsgsr/sbin
   # ./configure -nodisplay
   ```

**c.** Provide the following parameters requested by the configuration program:

**Table 6-27** Messaging Server Configuration Parameters

| Parameter | Value |
|---|---|
| Fully Qualified Host Name | `jesIMR1.net.telco.com` |
| Directory for configuration and data files | `/global/jesIMR1/var/opt/SUNWmsgsr` |
| Component Selection | `Message Transfer Agent (MTA)` |
| Administrator Username | `mailsrv` |
| Administrator Unix group | `mail` |
| LDAP configuration directory URL:port | `ldap//jesDPD.net.telco.com:389` |
| Bind as | `cn=Directory Manager` |
| Password | `password` |
| LDAP user/group directory URL:port | `ldap//jesDPD.net.telco.com:389` |
| Bind as | `cn=Directory Manager` |
| Password | `password` |
| Postmaster email address | `root@jesMCSb.net.telco.com` |
| Password | `password` |
| Email default domain | `telcomail.com` |
| Organization DN | `o=telcomail.com,dc=net,dc=telco,dc=com` |

**4.** Enable the LMTP protocol.

LMTP is a protocol used by Messaging Server MTA components to interact with each other. In the Telco architecture, LMTP is used for communication between the MTA component on `jesIMR1` and the MTA component on the back-end messaging stores `jesMCSb` and `jesMSc`.

LMPT is lighter and more efficient than the SMTP protocol. Using LMTP eliminates a second user authentication on the backend messaging server where the store is located.

Procedures for enabling LMTP are provided in "Enabling LMTP for Messaging Server MTA Interactions" on page 156.

5. Start the Messaging Server MTA on jesIMR1.

```
# cd /global/jesIMR1/opt/SUNWmsgsr/sbin
# ./start-msg
```

6. Verify the operation of Messaging Server MTA.

   Operation is verified by opening a telnet session to Messaging Server MTA and then using SMTP to conduct an interactive exchange with the MTA.

   a. Open a telnet session.

```
# telnet jesIMR1.net.telco.com 25
Trying 192.168.13.3...
Connected to jesIMR1.
Escape character is '^]'
220 jesIMR1.net.telco.com -- Server ESMTP (Sun Java System Messaging
Server 6.2-3.04 (built Jul 15 2005))
```

   b. Conduct conversation with the MTA.

```
hello jesIMR1
250 jesIMR1.net.telco.com OK, [192.168.13.3].
mail from: <buser0001@telcomail.com>
250 2.5.0 Address Ok.

rcpt to: <buser0002@telcomail.com>
250 2.1.5 buser0002@example.com OK.

data
354 Enter mail, end with a single ".".
subject:test
test smtp from buser0001 to buser0002
.
250 2.5.0 Ok.

quit
221 2.3.0 Bye received. Goodbye.
Connection to jesIMR1 closed by foreign host.
```

7. Repeat Step 1 - Step 6 on jesIMR2.

8. Verify load balancing for Messaging Server MTA inbound.

   Having verified that Messaging Server MTA instances are working on jesIMR1 and jesIMR2, you now verify that you can access these instances through the load balancer.

**a.** Turn off the jesIMR2 instance and access the service through the load balancer:

```
# cd /global/jesIMR2/opt/SUNWmsgsr/sbin
# ./stop-msg
# telnet smtp.telcomail.com 25
```

If this test succeeds then the jesIMR1 instance is working through the load balancer.

**b.** Turn off the jesIMR1 instance and turn on the jesIMR2 instance, and test this condition:

```
# cd /global/jesIMR1/opt/SUNWmsgsr/sbin
# ./stop-msg
# cd /global/jesIMR2/opt/SUNWmsgsr/sbin
# ./start-msg
# telnet smtp.telcomail.com 25
```

If this test works properly then the jesIMR2 instance is also working through the load balancer.

## Procedure, Part B: Messaging Server MTA Outbound

The installation and configuration of Messaging Server MTA outbound is almost identical to that of Messaging Server MTA in bound. The differences are as follows:

**1.** Install and configure the Messaging Server Message Transfer Agent software on jesOMR1.

Repeat Part A, Step 1 - Step 5. Skip Step 4; you do not enable LMTP for the MTA outbound component.

**2.** Install and configure the Messaging Server Message Transfer Agent software on jesOMR2.

Repeat Part A, Step 1 - Step 5. Skip Step 4; you do not enable LMTP for the MTA outbound component.

**3.** Verify load balancing for Messaging Server MTA outbound.

Repeat Part A, Step 6.

# Module #10: Load Balanced Messaging Server MMP and MEM

In this module you install and configure Messaging Server MMP and MEM instances. You do not perform any special configuration for these instances to operate correctly with the load balancer. You simply configure the load balancer. For more information, see “Configuring the Load Balancers” on page 73.

The installation and configuration procedure for Messaging Server MMP and MEM is very similar to the procedure for Messaging Server MTA.

## Installation and Configuration Summary



## Procedure

1. Install Java ES software on `jesMMP1`.

   Use the Configure Later option of the Java ES installer.

   a. Select the Messaging Server component.

   b. Enter the Messaging Server root parameter value:
   `/global/jesMMP1/opt/SUNWmsgsr`

2. Configure Messaging Server on `jesMMP1`.

   a. Modify the `/etc/hosts` file on `jesMMP1` to include the following entries:

```
192.168.13.7       jesMMP1.net.telco.com jesMMP1 loghost
192.168.13.8       jesMMP2.net.telco.com jesMMP2
192.168.14.3       mail.telcomail.com
192.168.14.7       mail.telco.net
192.168.14.8        www.telco.net
```

**b.** Run the Messaging Server configuration program.

```
# cd /global/jesMMP1/opt/SUNWmsgsr/sbin
# ./configure -nodisplay
```

**c.** Provide the following parameters requested by the configuration program:

**Table 6-28** Messaging Server Configuration Parameters

| Parameter | Value |
|---|---|
| Fully Qualified Host Name | jesMMP1.net.telco.com |
| Directory for configuration and data files | /global/jesMMP1/var/opt/SUNWmsgsr |
| Component Selection | Messaging Multiplexor (MMP)<br>Messenger Express (MEM) |
| Administrator Username | mailsrv |
| Administrator Unix group | mail |
| LDAP configuration directory URL:port | ldap//jesDPD.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| LDAP user/group directory URL:port | ldap//jesDPD.net.telco.com:389 |
| Bind as | cn=Directory Manager |
| Password | password |
| Postmaster email address | root@jesMCSb.net.telco.com |
| Password | password |
| Email default domain | telcomail.com |
| Organization DN | o=telcomail.com,dc=net,dc=telco,<br>dc=com |

**d.** Modify the configuration parameters for Messaging Server (MEM) so that it runs `mshttp` in proxy mode:

```
# cd /global/jesMMP1/opt/SUNWmsgsr/sbin
# ./configutil -o local.service.http.proxy -v 1
# ./configutil -o local.service.http.proxy.admin
  -v admin_telco.net
# ./configutil -o local.service.http.proxy.adminpass -v password
```

3. Start the Messaging Server MMP and MEM on jesMMP1.

```
# cd /global/jesMMP1/opt/SUNWmsgsr/sbin
# ./start-msg
```

4. Verify the operation of Messaging Server jesMMP1.

   Operation is verified by opening a telnet session to Messaging Server MMP and then using IMAP to conduct an interactive exchange with the MMP.

   a. Open a telnet session.

```
# telnet jesMMP1.net.telco.com 143
Trying 192.168.13.7...
Connected to jesMMP1.net.telco.com.
Escape character is '^]'
OK [CAPABILITY IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN BINARY LANGUAGE XSENDER X-NETSCAPE XSERVERINFO AUTH=PLAIN]
Messaging Multiplexor (Sun Java(tm) System Messaging Server 6.2-3.04
(built Jul 15 2005))
```

   b. Conduct a conversation with the MMP.

```
a001 login buser0001 password
a001 OK User logged in
a002 noop
a002 OK Completed
a003 Capability
* CAPABILITY IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN BINARY LANGUAGE XSENDER X-NETSCAPE XSERVERINFO
a003 OK Completed
a004 list "" *
* LIST (\NoInferiors) "/" INBOX
* LIST (\HasNoChildren) "/" Drafts
* LIST (\HasNoChildren) "/" Sent
* LIST (\HasNoChildren) "/" Trash
* LIST (\HasNoChildren) "/" new
a004 OK Completed
a005 select inbox
* FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
* OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \  Seen \*)]
* 1 EXISTS
* 0 RECENT
* OK [UNSEEN 1]
* OK [UIDVALIDITY 1103021473]
* OK [UIDNEXT 2]
a005 OK [READ-WRITE] Completed
```

```
a006 fetch 1 (body[1] rfc822.size)
* 1 FETCH (FLAGS (\Seen) RFC822.SIZE 989 BODY[1] {52}
buser0002@telcomail.com to buser0001@telcomail.com
)
a006 OK Completed
a007 logout
* BYE LOGOUT received
a007 OK Completed
Connection to jesMMP1 closed by foreign host.
```

5. Repeat Step 1 - Step 4 on jesMMP2.

6. Verify load balancing for Messaging Server MMP.

   Having verified that Messaging Server MMP is working on jesMMP1 and jesMMP2, you test access to these instances through the load balancer.

   a. Turn off the jesMMP2 instance and access the service through the load balancer:

      ```
      # telnet mail.telcomail.com 143
      ```

      If this test works properly then the jesMMP1 instance is working through the load balancer.

   b. Turn off the jesMMP1 instance and turn on the jesMMP2 instance, and retest:

      ```
      # telnet mail.telconail.com 143
      ```

      If this test works properly then the jesMMP2 instance is also working through the load balancer.

7. Verify load balancing for Messenger Express MEM.

   a. Verify that the Messenger Express HTTP service is running on jesMMP1.

      In your web browser open the following URL:

      `http://jesMMP1.net.telco.com`

      Then log in as user cuser0001@telco.net. The password is password.

   b. Verify that the Messenger Express HTTP service is running on jesMMP2.

      In your web browser open the following URL:

      `http://jesMMP1.net.telco.com`

      Log in as user cuser0001@telco.net. The password is password.

**c.** Verify that load balancing is working for the public consumer class HTTP service.

In your web browser open the following URL:

`http://www.telco.net`

Log in as user `cuser0001@telco.net`. The password is `password`.

Appendix A

# Specialized Implementation Topics

This appendix covers topics and procedures that are used in the Telco deployment, but are too specialized to place in the main body of this document.

# Enabling LMTP for Messaging Server MTA Interactions

LMTP is a protocol used by Messaging Server MTA components to interact with each other. LMTP is used in the Telco architecture for communication between the MTA components on `jesIMR1` and `jesIMR1` and the MTA component on the back-end messaging store (`jesMCSb`, `jesMSc`). LMTP must be enabled on both ends of the communication.

1. Enable LMTP on `jesMCSb` and `jesMSc`.

   a. Edit the `/global/jesMCSb/ms_data/var/opt/SUNWmsgsr/config/dispatcher.cnf` file. First, uncomment and edit the following lines:

```
[SERVICE=LMTPSS]
PORT=225
IMAGE=IMTA_BIN:tcp_lmtp_server
LOGFILE=IMTA_LOG:tcp_lmtpss_server.log
PARAMETER=CHANNEL=tcp_lmtpss
STACKSIZE=2048000
INTERFACE_ADDRESS=192.168.12.5
!
! rfc 2033 LMTP server - native
!
[SERVICE=LMTPSN]
PORT=226
USER=root
IMAGE=IMTA_BIN:tcp_lmtpn_server
LOGFILE=IMTA_LOG:tcp_lmtpsn_server.log
PARAMETER=CHANNEL=tcp_lmtpsn
STACKSIZE=2048000
INTERFACE_ADDRESS=192.168.12.5
```

**b.** Edit the /global/jesMCSb/ms_data/var/opt/SUNWmsgsr/config/imta.cnf file. Uncomment the following text:

```
! tcp_lmtpss (LMTP server - store)
tcp_lmtpss lmtp subdirs 20
tcp_lmtpss-daemon

!
! tcp_lmtpsn (LMTP server - native)
tcp_lmtpsn lmtp subdirs 20
tcp_lmtpsn-daemon
```

**c.** Execute the following commands:

```
# cd /global/jesMCSb/ms_data/var/opt/SUNWmsgsr/sbin
# ./imsimta cnbuild
# ./imsimta restart
```

**2.** Enable LMTP on jesIMR1.

**a.** Activate text databases needed by LMTP.

Edit the /global/jesIMR1/var/opt/SUNWmsgsr/config/option.dat file. Add the following lines:

```
[USE_TEXT_DATABASES=1
DELIVERY_OPTIONS=\
  #*mailbox=@$X:$M$_+$2S%$\$2I@ims-ms-daemon,\
  #&members=*,\
  #*native=@$X:$M,\
  #*unix=@$X:$M,\
  #/hold=$L%$D@hold,\
  #*file=@$X:+$F,\
  #&@members_offline=*,\
  #program=$M%$P@pipe-daemon,\
  #forward=**,\
  #*^!autoreply=$M+$D@bitbucket
```

**b.** Create the general.txt database needed by LMTP.

```
# cd /global/jesIMR1/opt/SUNWmsgsr/config/
# vi general.txt
```

```
LMTP_CS|jesMCSb.net.telco.com   lmtpcs-daemon
```

**c.** Add the text shown in bold to the "rules" section of the imta.cnf file.

```
! tcp_local
! Rules for top level internet domains
<IMTA_TABLE:internet.rules
!
! Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
! Do general.txt lookup for lmtp hosts
.net.telco.com $S$U%$H$D@$(LMTP_CN|$U@$H$D)
.net.telco.com $S$U%$H$D@$(LMTP_CS|$H$D)
!
! tcp_intranet
! Do mapping lookup for internal IP addresses
[] $E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
.telcomail.com $U%$H.telcomail.com@tcp_intranet-daemon
* $U%$&0.example.com
```

**d.** In the "channel" section of the imta.conf file, uncomment the following lines.

```
! tcp_lmtpcs (LMTP client - store)
tcp_lmtpcs defragment lmtp port 225 nomx single_sys subdirs   20
maxjobs 7 pool SMTP_POOL dequeue_removeroute
lmtpcs-daemon

! tcp_lmtpcn (LMTP client - native)
tcp_lmtpcn defragment lmtp port 226 nomx single_sys subdirs   20
maxjobs 7 pool SMTP_POOL dequeue_removeroute
lmtpcn-daemon
```

**e.** Execute the following commands:

```
# cd /global/jesIMR1/opt/SUNWmsgsr/sbin
# ./imsimta cnbuild
# ./imsimta restart
```

**3.** Verify the operation of LMTP.

**a.** Test LMTP on `jesIMR1`.

```
# cd /global/jesIMR1/opt/SUNWmsgsr/sbin

# ./imsimta test -rewrite -debug buser0001@telcomail.com

.....
```

**b.** If you see the following response, LMTP is operating correctly.

```
Expanded address: buser0001@telcomail.com
Submitted address list: tcp_lmtpcs
@jesMCSb.net.telco.com:buser0001@ims-ms-daemon (orig
buser0001@telcomail.com, inter userb0001@telcomail.com
host jesMCSb.net.telco.com) *NOTIFY-FAILURES* *NOTIFY-DELAYS*
```

**c.** If you get the following response (note the string in bold), LMTP is not operating correctly:

```
Expanded address: buser0001@telcomail.com
Submitted address list: tcp_intranet
@jesMCSb.net.telco.com:buser0001@ims-ms-daemon (orig
buser0001@telcomail.com, inter userb0001@telcomail.com,
host jesMCSb.net.telco.com) *NOTIFY-FAILURES* *NOTIFY-DELAYS*
```

**4.** Test LMTP on `jesMCSb`.

Verify end-to-end routing for a test user (`buser0001`) by checking that the email account is located on `jesMCSb`.

**a.** Execute the following commands:

```
# cd /global/jesMCSb/ms_data/opt/ms_data/SUNWmsgsr/sbin

# ./imsimta test -rewrite -debug buser0001@telcomail.com
```

**b.** If you get the following response, LMTP is operating correctly.

.....

```
Expanded address: buser0001@telcomail.com
Submitted address list: ims-ms
buser0001@ims-ms-daemon (orig buser0001@telcomail.com,
inter buser0001@telcomail.com, host ims-ms-daemon)
*NOTIFY-FAILURES* *NOTIFY-DELAYS*
```

The `ims-ms` means that it has found a local queue for `buser0001` and does not have to route the email any further.

# A Sample User Provisioning Script

The following script can be used to provision users for load testing the Telco deployment example. You can enter the number of users you wish to provision, and otherwise modify the script to meet your needs.

**Code Example A-1** Sample User Provisioning Script

```
#! /usr/bin/perl
local $comlocation = "/global/jesPAM1/opt/SUNWcomm/bin/";

sub createuser;
sub moduser;

my $curruser = "";
my $grade = "b";
my $domain = "o=telcomail.com,dc=net,dc=telco,dc=com";

for ($i=0; $i<=$#ARGV; $i++) {
 if ($ARGV[$i] eq "-c") {
 $grade = "c";
 $domain = "o=telco.net,dc=net,dc=telco,dc=com"
 }
}

print "\nTelecommunications Provider user provisioning script \n\n";
print "Enter starting user no: ";
$startuser = <STDIN>;
chomp($startuser);

print "Enter end  user no: ";
$stopuser = <STDIN>;
chomp($stopuser);
print "will attempt to provision users ",$grade,"user" , $startuser , " to ",$grade,"user" ,
$stopuser ,"\n";

for ($usecount=$startuser;$usecount <= $stopuser;$usecount ++) {
    $curruser = sprintf("user%04d",$usecount);
    createuser($curruser,$grade,$domain);
    moduser($curruser,$grade,$domain);
}
```

**Code Example A-1** Sample User Provisioning Script *(Continued)*

```
sub createuser {
    my $curruser = $_[0];
    my $grade  = $_[1];
    my $domain = $_[2];
    my $madmin = "admin";
    if ($grade eq "c") {
     $madmin = "admin_telco.net";
    }
    my $creatstr1 = "commadmin user create -D \"$madmin\" -w password -n \"$domain\" -d
\"$domain\" -l ";
    my $creatstr2 = " -F user -L ";
    my $creatstr3 = " -W password";
    my $commstr = sprintf("%s%s%s%s%s%s%s%s",$comlocation,$creatstr1,
          $grade,$curruser ,$creatstr2,$grade,$curruser,$creatstr3);
    print $commstr,"\n";
    (system($commstr)) && die ("Cmd failed: $! \n");
    sleep (2);
}

sub moduser {
    my $curruser = $_[0];
    my $grade  = $_[1];
    my $domain = $_[2];
    my $mhost = "jesMCSb.net.telco.com";
    my $madmin = "admin";
    if ($grade eq "c") {
     $mhost = "jesMSc.net.telco.com";
     $madmin = "admin_telco.net";
    }

    my $modstr1 = "commadmin user modify -D \"$madmin\" -w password -n \"$domain\" -d
\"$domain\" -l ";
    my $modstr2 = " -S mail,cal";
    my $modstr3 = " -A +objectclass:sunssoadapterperson";
    my $modstr4 = " -A +objectclass:sunportaldesktopperson";
    my $modstr5 = " -A mailhost:$mhost";
    my $modstr6 = " -A +objectclass:sunportalnetfileservice";
```

**Code Example A-1** Sample User Provisioning Script *(Continued)*

```
my $commstr = sprintf("%s%s%s%s%s",$comlocation,$modstr1,$grade,$curruser,$modstr2);
print $commstr,"\n";
(system($commstr)) && die ("Cmd failed: $! \n");
sleep (2);
if ($grade eq "b") {
 $commstr = sprintf("%s%s%s%s%s",$comlocation,$modstr1,$grade,$curruser,$modstr3);
 print $commstr,"\n";
 (system($commstr)) && die ("Cmd failed: $! \n");
 sleep (2);

 $commstr = sprintf("%s%s%s%s%s",$comlocation,$modstr1,$grade,$curruser,$modstr4);
 print $commstr,"\n";
 (system($commstr)) && die ("Cmd failed: $! \n");
 sleep (2);
}
$commstr = sprintf("%s%s%s%s%s",$comlocation,$modstr1,$grade,$curruser,$modstr5);
print $commstr,"\n";
(system($commstr)) && die ("Cmd failed: $! \n");
sleep (2);

if ($grade eq "b"){
 $commstr = sprintf("%s%s%s%s%s",$comlocation,$modstr1,$grade,$curruser,$modstr6);
 print $commstr,"\n";
 (system($commstr)) && die ("Cmd failed: $! \n");
 sleep (2);
}

}
```

# Sun Cluster Software Status Output

This section displays the output from the Sun Cluster Software status check performed at the end of “Module #5: Business-class Messaging Server and Calendar Server on Sun Cluster Nodes” on page 108. It also interprets the output for you.

The first section of the output is displayed in Code Example A-2. This part of the output describes the physical nodes that make up the cluster.

**Code Example A-2** Cluster Node Section

```
- Cluster Nodes --

                    Node name           Status
                    ---------           ------
  Cluster node:       jesMCS1b            Online
  Cluster node:       jesMCS2b            Online
```

The second section of the output is displayed in Code Example A-3. This part of the output describes the private cluster interconnect interfaces and the fact that they are up. They have gigabit cross-over cables connected.

**Code Example A-3** Cluster Transport Paths

```
-- Cluster Transport Paths --

                    Endpoint            Endpoint            Status
                    --------            --------            ------
  Transport path:     jesMCS1b:ce5        jesMCS2b:ce5        Path online
  Transport path:     jesMCS1b:ce1        jesMCS2b:ce1        Path online
```

The third section of the output is displayed in Code Example A-4. This part of the output describes how many votes are required for the cluster to function. It shows that each of the computers is contributing 1 vote to the cluster quorum and that one of the shared disks is being used to provide an additional vote. This means that the cluster will continue to function if at least one computer and the global disk device are alive.

**Code Example A-4** Quorum Summary

```
------------------------------------------------------------------

-- Quorum Summary --

  Quorum votes possible:      3
  Quorum votes needed:        2
  Quorum votes present:       3


-- Quorum Votes by Node --

                    Node Name           Present Possible Status
                    ---------           ------- -------- ------
  Node votes:         jesMCS1b            1        1       Online
  Node votes:         jesMCS2b            1        1       Online


-- Quorum Votes by Device --

                    Device Name         Present Possible Status
                    -----------         ------- -------- ------
  Device votes:     /dev/did/rdsk/d18s2 1        1       Online
```

The fourth section of the output is displayed in Code Example A-5. This section describes the disk device groups set up through Solaris volume manager to support the messaging and calendar stores.

**Code Example A-5** Device Group Status

```
-- Device Group Status -
repository for messaging and calendar
                              Device Group Status
                              ------------ ------
Device group status:              ms_data Online
Device group status:              cs_data Online
```

The fifth section of the output is displayed in Code Example A-6. This part of the output reports that resource group IMS-RG consists of the logical cluster interface name jesMCSb and the messaging and calendar cluster agents.

**Code Example A-6** Resource Groups and Resources

```
Resource Groups and Resources --
                              Group Name Resources
                              ---------- ---------
Resources:                        IMS-RG jesMCSb ims-rs scics-rs

-- Resource Groups --
                              Group Name Node Name State
                              ---------- --------- -----
Group:                            IMS-RG  jesMCS1b Offline
Group:                            IMS-RG  jesMCS2b Online

-- Resources --
jesMCSb the logical hostname
ims-rs the messaging cluster agent
scics-rs the calendar cluster agent.

Resource Name         Node Name   State    StatusMessage
-------------         ---------   -----    -------------
Resource:jesMCSb      jesMCS1b    Offline  LogicalHostname offline. Resource:jesMCSb
jesMCS2b    Online   LogicalHostname online.
Resource: ims-rs       jesMCS1b  Offline   Offline - Stop Succeeded
Resource: ims-rs       jesMCS2b  Online O  Online - Start succeeded.
Resource: scics-rs     jesMCS1b  Offline   Offline
Resource: scics-rs     jesMCS2b  Online    Online
-----------------------------------------------------------------
```

# Index

# D



# F

# H



# I



# J

## L



## M

# O



# P



# Q

# R



# S



# T



# U

## V



## W