IBM

Bynari Insight Server V4 for Linux

on the IBM *e*server iSeries Server

Get to know the Bynari Insight product family of messaging services

Learn how to install and configure the Insight Server and clients

Explore administration and operations tips

Yessong Johng
Fredy Alexander Cruz
Jason Landa
Robin Latham
Marco Manzato
Alex Polash

Redbooks

IBM

International Technical Support Organization

Bynari Insight Server V4 for Linux on the IBM *@server* **iSeries Server**

October 2003

> **Note:** Before using this information and the product it supports, read the information in "Notices" on page vii.

First Edition (October 2003)

This edition applies to Insight Server Version 4.0-4, Insight Connector Version 2.0 Build 35, Insight AddressBook Version 2.0 Build 15, and Insight WebClient Version 2.0 Build 4.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

vii

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server™	iSeries™	OS/2®
@server™	AS/400®	OS/400®
Redbooks(logo) ™	DB2®	PowerPC®
e-business on demand™	IBM®	Redbooks™
ibm.com®	Lotus®	WebSphere®

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

In this world of e-business on demand™ computing, server consolidation in the right fashion becomes critically important. You need reliability, availability, and rich functionality, while maintaining the lowest total cost of ownership (TCO). IBM® @server iSeries™ is proven to be one of the best platforms for server consolidation. Linux on iSeries provides an excellent choice to build the infrastructure of Web-based dynamic mission-critical applications. On top of its well functioning and reliable open source-based solutions, it provides ready-to-use business applications. The Bynari Insight Server, along with its Insight product family, is a fine example of business applications that run on Linux on iSeries.

Bynari Insight Server V4 provides enterprise-level messaging services within and among the various parts of an organization's network of people and resources. It also provides a safe harbor for an organization's messaging needs by using the Internet mail model. Using Insight Server V4 and running on the iSeries server, users can replace the Microsoft® Exchange Server. This allows them to achieve higher reliability, availability, scalability, and even reduce the total cost.

This IBM Redbook is designed to help system administrators and information technology (IT) managers to understand the main benefits of Bynari Insight Server V4 and its product family. It explains how to install, configure, and administer the Insight Server and its products. Plus this redbook offers tips for operating the Bynari Insight Server.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Yessong Johng is an IBM Certified IT Specialist at the IBM International Technical Support Organization, Rochester Center. He started his IT career at IBM as a S/38 Systems Engineer in 1982 and has been working with the S/38, AS/400®, and now iSeries for 20 years. He writes extensively and develops and teaches IBM classes worldwide on the areas of e-business on the iSeries server. His specializes in WebSphere® and Linux implementations on the iSeries server.

Fredy Alexander Cruz is the Independent Software Vendor (ISV) Coordinator at IBM Colombia. He helps developers in infrastructure migrations over software including WebSphere and DB2® on both Linux and OS/400®. He also teaches ISVs about the utilities and technologies related to this task. His most recent project was mounting a demonstration site for the iSeries server that gives support for sales people throughout South America. This site focuses on Linux and Windows® integration, Lotus®, and WebSphere.

Jason Landa is a consultant for Intrcomm Technology in the Basalt, Colorado, office. He has been with Intrcomm Technology since graduating in December 1996 from Minnesota State University, where he earned a degree in mathematics and computer science. He began his career as a programmer in Web-based application development. He has since transitioned into technical sales and consulting.

Robin Latham is the training and technical content developer for Bynari, Inc. Prior to joining the Bynari team, she was the lead mail server trainer for Software Spectrum, Inc. and then served as a training and technical specialist at Microsoft, Inc. Before entering the IT field, Robin was an aviator in the United States Army.

Marco Manzato is a diversified systems specialist with Bynari, Inc. He has 15 years of experience in networking, protocols, and operating systems. He began his career in electrical engineering, later crossing to computers in 1986 in the chemical industry where he worked with VAX, DEC PDP, and IBM OS/2®. He then migrated to working with Windows for a company that converted Systems Network Architecture (SNA) to Transmission Control Protocol/ Internet Protocol (TCP/IP) networking for PCs to access mainframe applications. This lead to work as a systems administrator for the next five years, where he configured and installed networks and operating systems such as Linux, Solaris, Windows NT®.

Alex Polash is a sales specialist at Bynari, Inc. He has been with Bynari since the beginning stages of the Insight Server and Insight Connector, early in 2002. He is currently completing his studies in business management. He is directly involved in presales and sales of Bynari's Insight family of products, working with both end users and Bynari business partners.

Thanks to the following people for their contributions to this project:

Ben Jordan
Alex Khanin
Hyun Kim
Trey Tabner
Shawn Walker
Bynari, Inc.

Gordon Haubenschild
Kay Tate
IBM Rochester

Harlon Trowbridge
IBM Dallas

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

► Use the online **Contact us** review redbook form found at:

> `ibm.com`/redbooks

► Send your comments in an Internet note to:

> redbook@us.ibm.com

► Mail your comments to:

> IBM Corporation, International Technical Support Organization
> Dept. JLU Building 107-2
> 3605 Highway 52N
> Rochester, Minnesota 55901-7829

1

Insight Server for the iSeries server

Insight Server provides enterprise-level messaging services for the various parts of an organization's network of people and resources. It also uses the Internet mail model to provide a safe place for an organization's messaging needs.

You can learn more about Insight Server and its family of products on the Bynari Web site at:

http://www.bynari.net/

1.1 Bynari, Inc.

Bynari, Inc. is a leading-edge software firm, based in Dallas, Texas. Their focus is on providing a full-suite of collaboration products by using open standards and open source software. Bynari develops products for resale through various reseller and distributor channels. Bynari sells their products through third-party mail server vendors, as well as through its own sales and marketing channels.

What sets Bynari apart from other mail messaging companies is its unique technology that provides a complete suite of services to support Microsoft Outlook clients, from Outlook 97 to Outlook XP (2002) without needing a Microsoft Exchange server. The Outlook clients are configured in *corporate workgroup mode*. The users are migrated to the Insight Server using a migration tool that automatically migrates all the data without *any* user intervention. Such popular functions as Outlook calendaring, shared folders, and meeting room scheduling are available.

1.2 Bynari Insight family of products

The Bynari Insight family of messaging service products consist of:

► The Linux-based mail server of the Insight Server
► Middleware components of Insight Connector and Insight AddressBook
► Web Client of Insight WebClient

Bynari uses an open standards model for its mail and messaging server. This model supports Intel® servers, as well as the IBM @server iSeries, pSeries, xSeries, and zSeries servers.

1.3 Insight Server

Insight Server delivers a Linux-based mail services product. It provides the functionality of an enterprise messaging server to users using Outlook clients or Web clients. Insight Server uses open standards and centralized architecture that are superior to other messaging servers and scales from Intel to IBM mainframe servers.

This latest version of Insight Server adds additional ease of management, integrated security, migration and installation tools, and transparent user interface. Insight Server provides fast and easy installation compared to other mail servers. You do not have to be a Linux or Windows professional to install the server. Maintaining the server is easily completed with Insight Server's Web console. Figure 1-1 shows various components of Insight Server and its related modules.

Cyrus IMAP, OpenLDAP, and Postfix each use a series of Berkeley databases to store, index, and retrieve applicable information.
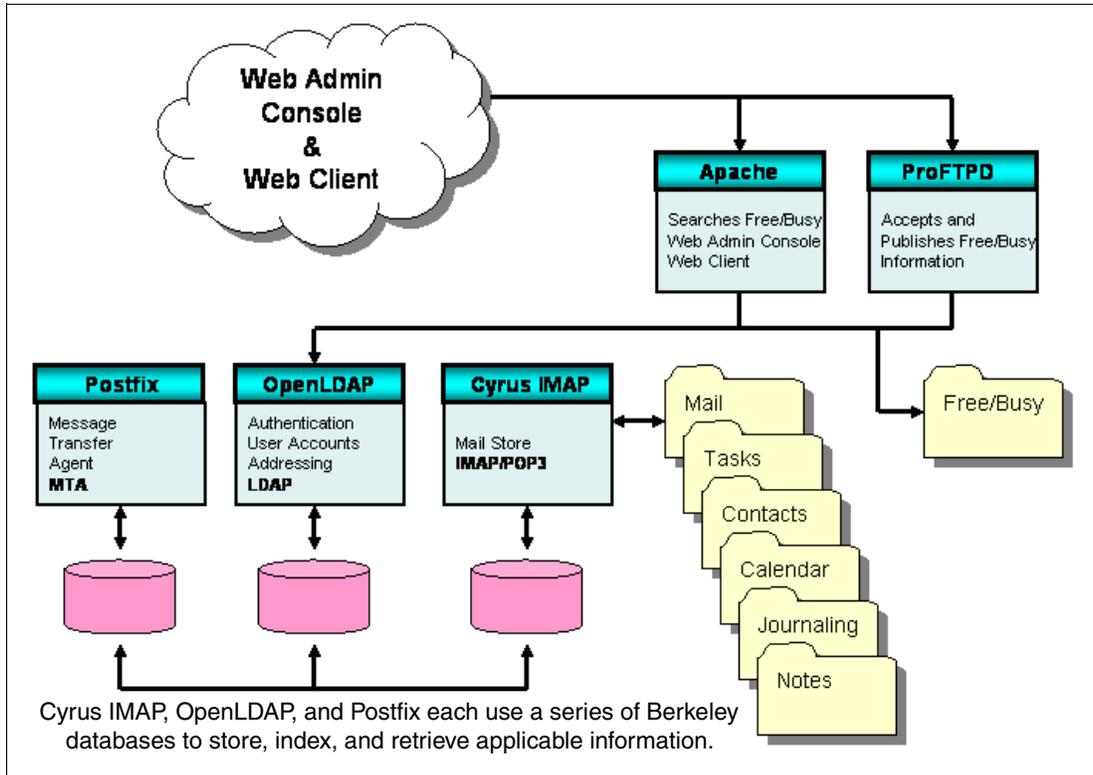
Figure 1-1   Overview of Insight Server components

Table 1-1 provides a description of each component shown on Figure 1-1.

Table 1-1   Insight Server components description

Component	Description
Web Administration Console	Provides an Hypertext Transfer Protocol (HTTP) interface for easy administration of all tasks for Insight Server
Web Client	HTTP interface for the user to retrieve mail, tasks, calendaring, etc.
Apache	Provides the interface for the Web Administration Console and Web Client; makes available any free/busy information that is published.
ProFTPD	Interface that accepts and publishes free/busy information to the Apache component.
OpenLDAP	Contains all user accounts/addresses and is the means for authentication of each user.
Postfix	This is the Message Transfer Agent (MTA) responsible for communicating mail to the proper location.
Cyrus IMAP	Enables each user to connect to the mail store and access their mail by indexing where each user's mailbox is located.

Reliable and cost efficient

Insight Server offers a proven platform for deploying mission-critical messaging solutions at an affordable price. Spiraling costs of proprietary messaging and collaboration products from vendors, such as Microsoft, have caused many organizations to worry about their infrastructures. Insight Server provides significant cost savings for any organization, while allowing for network stability.

Customers looking for an alternative to legacy software will find Bynari, combined with Linux, on IBM @server platforms, to be an attractive option whether it is for a single xSeries server or for large enterprise server consolidation on an iSeries server. Scaling from a single processor on the iSeries server to the largest of the multiprocessor iSeries servers, Bynari offers unparalleled scalability, interoperability, and flexibility. By using Linux, Insight Server, and appropriate hardware systems, the total cost of ownership (TCO) is significantly less than using a Microsoft mail server and other comparably priced messaging products.

Simple migration

Insight Server eliminates downtime and training for Insight Server data migration. The new Bynari Web Administration Console incorporates a migration tool that allows systemic migration from Microsoft Exchange and other third-party Internet Message Access Protocol (IMAP) servers to the Insight Server. This functionality allows for transparent migration for the desktop user and compatibility with Microsoft Exchange and other third-party mail servers to provide phased, mixed, or total migrations. All data, including Lightweight Directory Access Protocol (LDAP) directory information, mailboxes, user configurations, and others, are migrated from the server side.

Security

Insight Server has integrated Secure Sockets Layer (SSL) and Transport Layer Security (TLS) support for all access into the server. This includes the Web administrative interface, Post Office Protocol 3 (POP3)/IMAP for receiving mail, Simple Mail Transfer Protocol (SMTP) for sending mail, and LDAP for directory lookups and manipulation. The Insight Server also has improved Access Control List (ACL) controls for deletion of folders and messages. Reliable Antivirus (RAV), anti-spamming and filtering security software, is integrated with the Web console to provide the best security software on the market. In addition, SpamAssassin, open source anti-spam software, has been integrated into the server. Single user sign-on with other Windows server applications using pGina, open-source software, is also integrated.

Insight Server includes the following security features:

- ► Enhanced e-mail traffic scanning (load balancing/performance)
- ► Information leaks prevention (encryption)
- ► Bulk mail protection (anti-spamming)
- ► Intelligent update (server updates via the Web console)
- ► Warning notifications (log files/admin notifications)

Enhanced management tools

Enhanced console management functions add the ability to configure mail transfers via the Bynari Web-based interface. An Insight Server administrator has more robust configurations options via the Web Administration Console including:

- ► Remote management
- ► System log access
- ► Server-side filtering rules
- ► Account management
- ► Backup and restore tools
- ► Redundancy/high availability
- ► Mailbox management
- ► Scheduled tasks
- ► System-wide aliases
- ► Categorized statistics and reporting
- ► Mail queue management
- ► ACL management

Insight Server features

Insight Server supports the following features:

► Multi-protocol support (including LDAP, POP3, IMAP, SMTP)

► Multi-platform support (supported on all IBM @server platforms under Linux to include the new pSeries)

► Secure operating environment (uses both open source and third-party security measures, including virus protection, anti-spam filtering, stripping of worms, Trojan horses, Visual Basic scripts, etc.)

► Industry leading reliability

► Cost effective (immediate savings compared to the same Microsoft based solution)

► Compatible with multiple versions of Microsoft Outlook, from Outlook 97 to Outlook XP.

► Multiple domains support (Users can have several different domain e-mail addresses stored on a single server, such as john@ibm.com, john@ibm.net, john@ibminc.com, etc.)

► Distributed and consolidated environments

► Microsoft's *corporate group mode* for Outlook compatibility

► Multi-client work environment (supports many different client platforms, including Windows-, Linux-, and UNIX®-based desktops and workstations)

► Extended character sets under the Web console using Unicode Transformation Format (UTF) and Unicode for compatibility with foreign languages

► Localization support for over 130 languages

► Distribution lists (both server-wide mailing lists and personal lists)

► Special folders created outside of the inbox level

► Single user sign-on with other Windows server applications using pGina open source software

► Supports such open source Web clients as Squirrelmail and Internet Messaging Program (IMP)

1.4 Insight Connector

The Bynari Insight Connector enables Microsoft Outlook functionality in IMAP Mailboxes using corporate workgroup mode instead of *Internet only mode*. With the Insight Connector middleware, IMAP mailboxes can now operate as full Outlook information stores containing any kind of Outlook items, not just the messages and posts that IMAP normally handles.

Insight Connector installs as an Exchange client extension, so it's compatible with all versions of Outlook. With our Linux mail server, Insight Server, Insight Connector supports sharing of user's individual IMAP folders, calendaring information, meeting scheduling, and much more. All the functions are natively supported by Outlook. As a result, it becomes possible for users to share data using the Bynari IMAP server, rather than specialized servers.

Insight Connector supports the following features and functions:

► Native Outlook calendar sharing
► Publish free/busy
► Meeting room scheduling
► Contact manager
► Global contact lists
► Task list

- ► Auto archiving
- ► Outlook free-form notes
- ► Activity journal
- ► Voting buttons
- ► Out of office notification
- ► New mail notification enabled
- ► Send/receive group requests
- ► Send/receive meeting request response (accept/decline messages)
- ► POP3 support
- ► Client side rules
- ► Reminder window
- ► Shared folders
- ► LDAP/contact address book
- ► Group scheduling

1.5 Insight AddressBook

The Bynari Insight AddressBook, formerly known as Insight LDAPClient, has the look and feel of the Global Address List with the Show all feature after it is opened. With a 50,000 directory user base, it provides instantaneous lookups when using the Check name feature in a new mail message. After loading AddressBook using Outlook, queries take less than three seconds for the entire directory. When using department lists, lookups are instantaneous.

Insight AddressBook supports the following features:

- ► Enables a global address list from an LDAP server
- ► Allows you to change a schema to work with different servers
- ► Checks (resolve) names on LDAP server
- ► Can enable local caching to support large LDAP servers
- ► Has the same look and feel of Global Address List (GAL)
- ► Performs searches for large directories within seconds

1.6 Insight WebClient

Bynari Insight WebClient provides full-functioning Web access using any Web browser running on Windows, Linux, or MAC. Insight WebClient allows integration and sharing of critical information with any Outlook clients. Other Insight WebClient and Outlook users can share such major functions as calendaring, folder sharing, and meeting scheduling. Access your e-mail, calendar, and contacts from anywhere in the world using an Internet connection. All you need is the Insight Server. You do not need to install any special software on each desktop.

Insight WebClient supports the following features:

- ► Calendaring
- ► Folder sharing
- ► Meeting scheduling
- ► Create events
- ► Free/busy information
- ► Contacts
- ► Journals and tasks
- ► Notes

Outlook functionality

Insight WebClient has a similar look and feel to the Microsoft Outlook interface. It also performs many of the same features. Together with Insight Server, you can now check your mail and calendar, access files from a public folder, and much more all from a Web browser. The uniqueness of this client is its ability to exchange information with any version of Outlook clients. From any remote location, users can access and view critical information about meetings and schedules, and add information into their calendars.

Standardization

The software is the same when accessed through any Web browser, such as Explorer, Netscape, or Opera. Insight WebClient does not require you to install special software on each desktop.

2

Planning and installation

Important: Prior to reading this chapter, you must be familiar with logical partitions (LPARs) and Linux implementation on the iSeries server. To learn more about these topics, see *LPAR Configuration and Management: Working with IBM @server iSeries Server Logical Partitions*, SG24-6251, and *Linux on the IBM @server iSeries Server: An Implementation Guide*, SG24-6232.

This chapter explains how to install Bynari Insight Server V4 on the iSeries server running Linux. It also explains how to set up iSeries Navigator to work with the LPAR configuration.

For more information about Linux, refer to the following Web site:

http://www.linux.org/docs/index.html

9

2.1 Planning the OS/400 environment

The key to a successful installation of Linux on iSeries is in the planning. Bynari Insight Server V4 runs on the iSeries server as a Linux application. Therefore, you should spend a large portion of the planning cycle on planning for LPAR and the Linux partition. As discussed earlier, this redbook focuses on installing Bynari Insight Server.

Before you install Linux, consider the following iSeries server-specific issues:

► **Disk storage requirements**: To install Bynari Insight Server for Linux on the iSeries server, consider the following disk storage requirements:

  – *Basic Linux operating system*: The default Linux system uses approximately 2 GB of disk storage when installed on the iSeries server.

  – *Bynari Insight Server*: We recommend that you have 5 GB of storage to start for 25 users and add 200 MB for each user.

► **Memory requirements**: We recommend that you have 256 MB of memory.

► **Processor requirements**: We recommend that you share half of your processor.

► **Sharing local area network (LAN) adapters**: This is optional. You can use a separate LAN adapter for the Linux partition. This book explains how to use a shared device that uses network address translation (NAT).

► **Internal LAN addresses**: The internal (virtual) LAN is a component of the iSeries server that enables communication between the iSeries server and Linux. You can connect your Linux partition using NAT, proxy Address Resolution Protocol (ARP), or Transmission Control Protocol/Internet Protocol (TCP/IP) routing.

► **OS/400 user privileges**: You must have two kinds of users on OS/400. One kind must have a SECOFR privileges. This allows them to create the disks and the server description in the OS/400 environment. The other kind of use is the service tools user. This user can create the partition, the virtual LAN, reserve memory and processor for that partition, and access the main Linux console.

► **Linux distribution**: IBM is currently working with the following distributors with PowerPC® extensions. Refer to their Web sites for more information:

  – SuSE: http://www.suse.com
  – RedHat: http://www.redhat.com

2.2 Installing Linux

To install Linux, you follow these steps:

1. Create a service tools user.
2. Configure a Linux partition with iSeries Navigator.
3. Create Linux disks, Network Server Storage (NWSSTG), with iSeries Navigator.
4. Create the Network Server Description (NWSD).
5. Link the Linux disks, that is NWSSTG.
6. Configure the virtual LAN.
7. Change the boot parameters of the NWSD.
8. Start the Linux partition.
9. Start the Linux server.

The following sections explain each of these steps.

2.2.1 Creating a service tools user

To work with Linux partitions, you need to do some configurations in System Service Tools (SST). As needed by the Linux LPAR, at least one service tools user ID must have a partition remote panel key with access to the partition number that you need to configure. In addition, you can configure that user to move resources between partitions.

In V5R2, you can create the user by using the SST menu. To configure the service tools user ID, follow these steps:

1. Type the `STRSST` command.

2. Enter a user ID and password for the SST environment (for example, `QSECOFR`).

3. Choose option `8` (Work with service tools user IDs).

4. The Work with Service Tools User IDs display (Figure 2-1) opens. Type option `1` (Create) and enter a user ID, such as `LNXUSR`.

```
               Work with Service Tools User IDs
                                                        System: AS05
 Type option, press Enter.
   1=Create            2=Change password     3=Delete
   4=Display           5=Enable              6=Disable
   7=Change privileges   8=Change description


 Opt  User ID    Description                              Status

      QSECOFR    QSECOFR                                  Enabled
      QSRV       QSRV                                     Enabled
      11111111   11111111                                Enabled
      22222222   22222222                                Enabled



 F3=Exit   F5=Refresh   F12=Cancel
```

Figure 2-1   Work with Service Tools User IDs display

5. The Create Service Tools User ID display (Figure 2-2) appears. Enter the password for this user ID. For the Set password to expire parameter, enter 2 for *No* so that password does not expire. If you leave the default value of 1, then the user must change the password in their next login. Press the F5 key.

```
                    Create Service Tools User ID
                                                      System: AS05
 Service tools user ID name  . . . . . . . :  LNXUSR

 Type choices, press Enter
   Password  . . . . . . . . . . . . . . .


   Allow ID access before
   storage management recovery . . . . . . .    1=Yes, 2=No
   Set password to expire  . . . . . . . . .  2 1=Yes, 2=No
   Description . . . . . . . . . . . . . . .
```

Figure 2-2   Create Service Tools User ID

6. The Change Service Tools User Privileges display (Figure 2-3) appears. All the functions are revoked for this newly created user ID by default. Therefore, you need select option 2 to grant the user access to the partition console. If you want this user to manage the partitions, you must grant the disk units and partitions options.

```
                      Change Service Tools User Privileges
                                                    System: AS05
 Service tools user ID name  . . . . . . . . :   LNXUSR


 Type option, press Enter.
   1=Revoke    2=Grant

 Option    Functions                                          Status
           None                                               Revoked
           Disk units - operations                           Revoked
           Disk units - administration                       Revoked
           System partitions - operations                    Revoked
           System partitions - administration                Revoked
           Partition remote panel key PRIMARY     0          Revoked
           Partition remote panel key XXXXXXXXXX 1           Revoked
           Partition remote panel key XXXXXXXXXX 2           Revoked
           Partition remote panel key XXXXXXXXXX 3           Revoked
           Partition remote panel key XXXXXXXXXX 4           Revoked
           Partition remote panel key XXXXXXXXXX 5           Revoked
           Partition remote panel key XXXXXXXXXX 6           Revoked
           Partition remote panel key XXXXXXXXXX 7           Revoked
                                                                More...
   F3=Exit   F5=Reset   F9=Defaults   F12=Cancel
```

Figure 2-3   Change Service Tools User Privileges (Part 1 of 2)

The display in Figure 2-4 shows the new status.

```
                    Change Service Tools User Privileges
                                                        System: AS05
Service tools user ID name  . . . . . . . . :  LNXUSR


Type option, press Enter.
  1=Revoke   2=Grant


Option   Functions                                        Status
         None                                             Revoked
         Disk units - operations                          Granted
         Disk units - administration                      Granted
         System partitions - operations                   Granted
         System partitions - administration               Granted
         Partition remote panel key PRIMARY     0         Granted
         Partition remote panel key XXXXXXXXXX 1          Granted
         Partition remote panel key XXXXXXXXXX 2          Revoked
         Partition remote panel key XXXXXXXXXX 3          Revoked
         Partition remote panel key XXXXXXXXXX 4          Revoked
         Partition remote panel key XXXXXXXXXX 5          Revoked
         Partition remote panel key XXXXXXXXXX 6          Revoked
         Partition remote panel key XXXXXXXXXX 7          Revoked
                                                             More...
 F3=Exit   F5=Reset   F9=Defaults   F12=Cancel
```

Figure 2-4   Change Service Tools User Privileges (Part 2 of 2)

2.2.2 Configuring a Linux partition with iSeries Navigator

In V5R2, you can configure guest partitions from iSeries Navigator. You must remove resources from another partition and allocate them to the guest partition. This process requires the following steps:

1. Start iSeries Navigator.

2. Enter your login information.

3. Expand **Configuration and Service** and double-click **Logical Partitions** as shown in Figure 2-5.
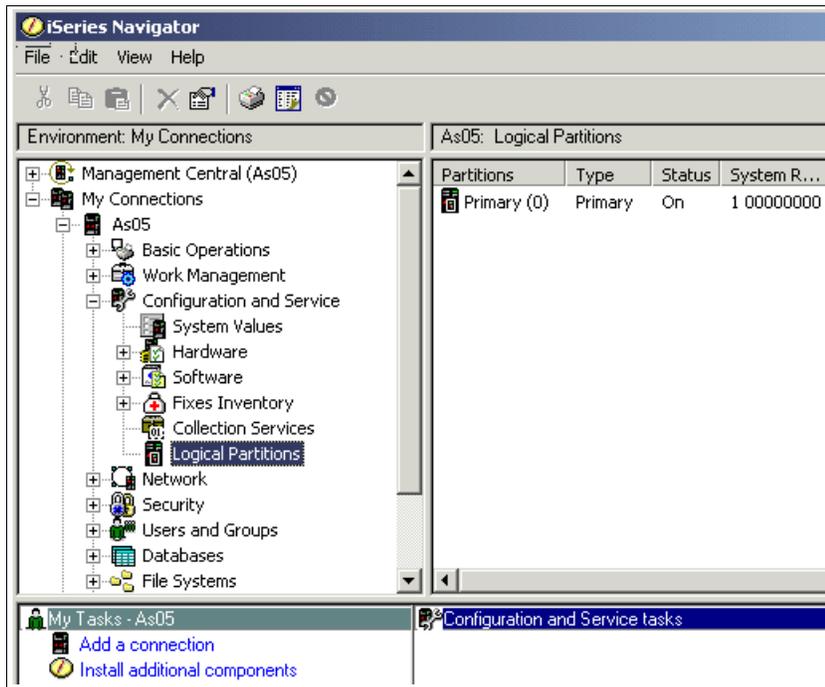

Figure 2-5   Starting LPAR configuration using iSeries Navigator

4. Right-click and select **Configure Partitions**.
5. The Configure Logical Partitions window (Figure 2-6) opens. In the left panel, select the partition that you chose to remove resources. Then in the right panel, select the resource that you want to remove. Right-click the partition and select **Move**.
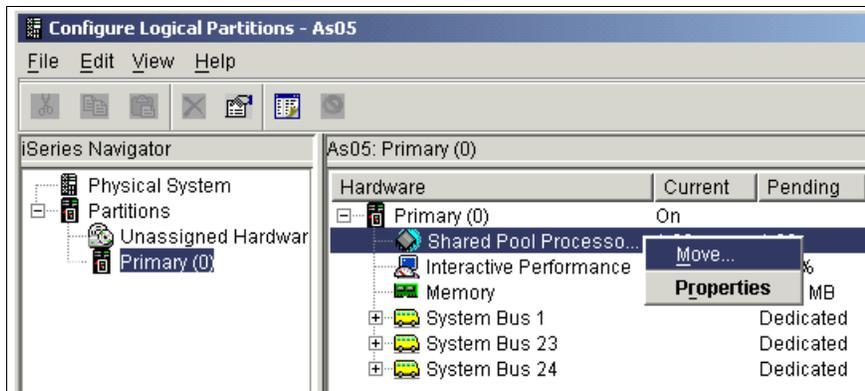

Figure 2-6   LPAR configuration example: Moving a processor (Part 1 of 2)

6. The Move Processing Power window (Figure 2-7) opens. Change the amount of processors that you want to move. In the Move to box, for Logical partition, select **Unassigned Shared** and click **OK**.
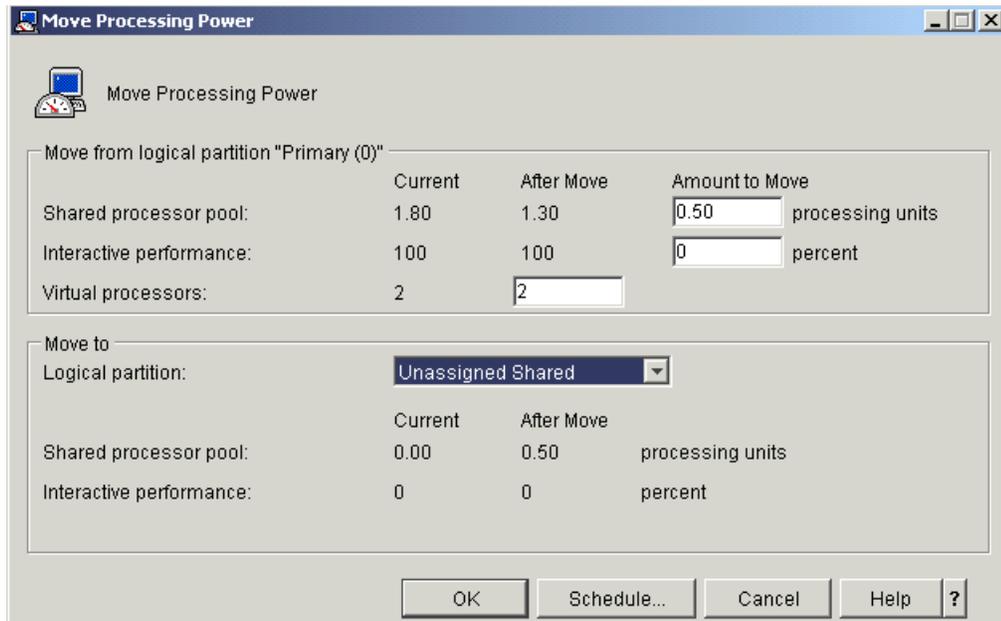

Figure 2-7   LPAR configuration example: Moving a processor (Part 2 of 2)

7. Repeat steps 5 and 6 to move memory.
8. Verify that the amount of processors and memory that you move appear under Unassigned Hardware as shown in Figure 2-8.
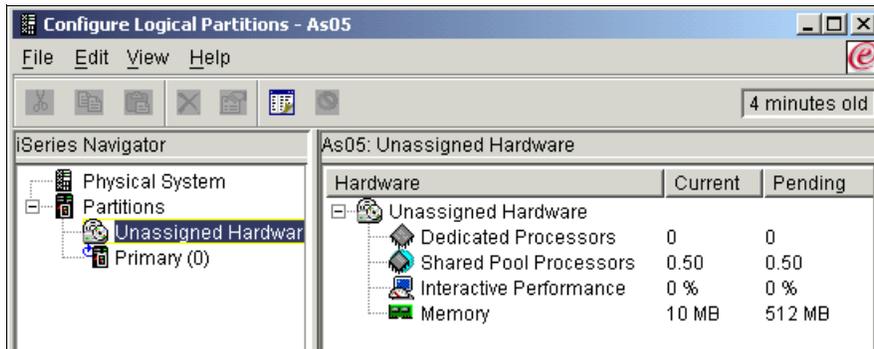

Figure 2-8   LPAR configuration example: Resources verification

Now we are ready to create the Linux partition.

1. On the Configure Logical Partitions window (Figure 2-9), to create a new partition, select **Partitions**. Right-click and select **New Logical Partition**.
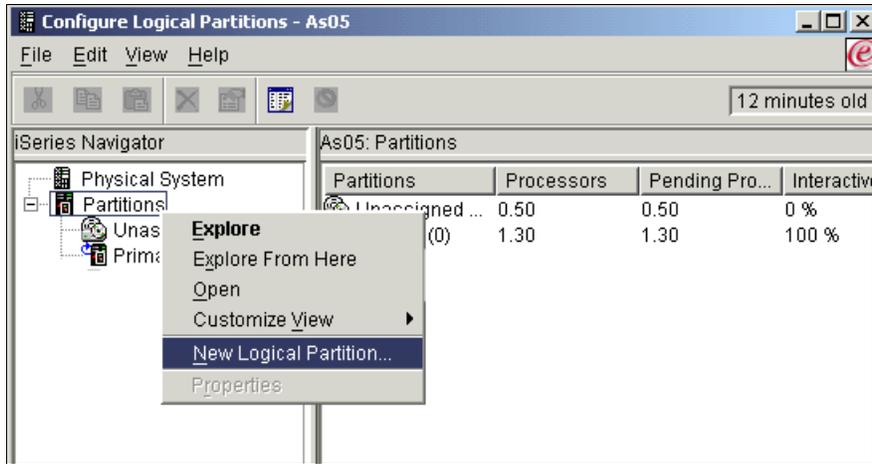

Figure 2-9   Creating a Linux partition: Starting task

2. This starts the New Logical Partition wizard. Click **Next** in the welcome window.

3. On the New Logical Partition - Type of Partition window (Figure 2-10), select the **Create new partition for guest operating system** option. Then click **Next**.
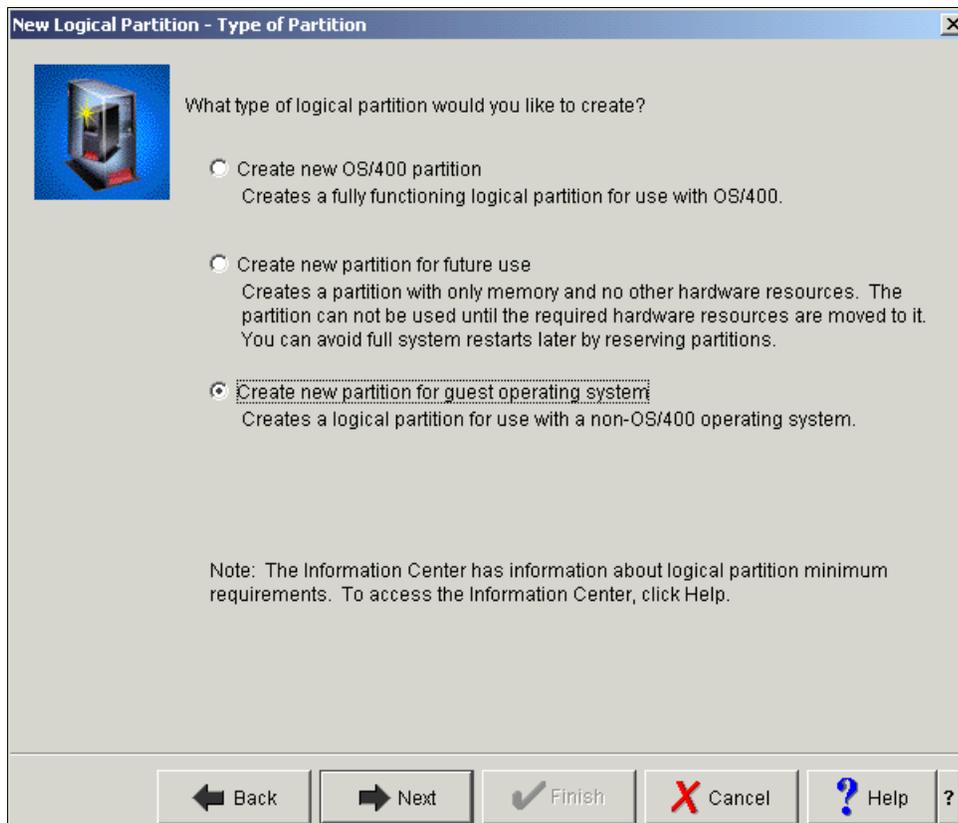

Figure 2-10   Creating a Linux partition: Type of partition

4. On the New Logical Partition - name window (Figure 2-11), specify the name and the number of partition. Then click **Next**.
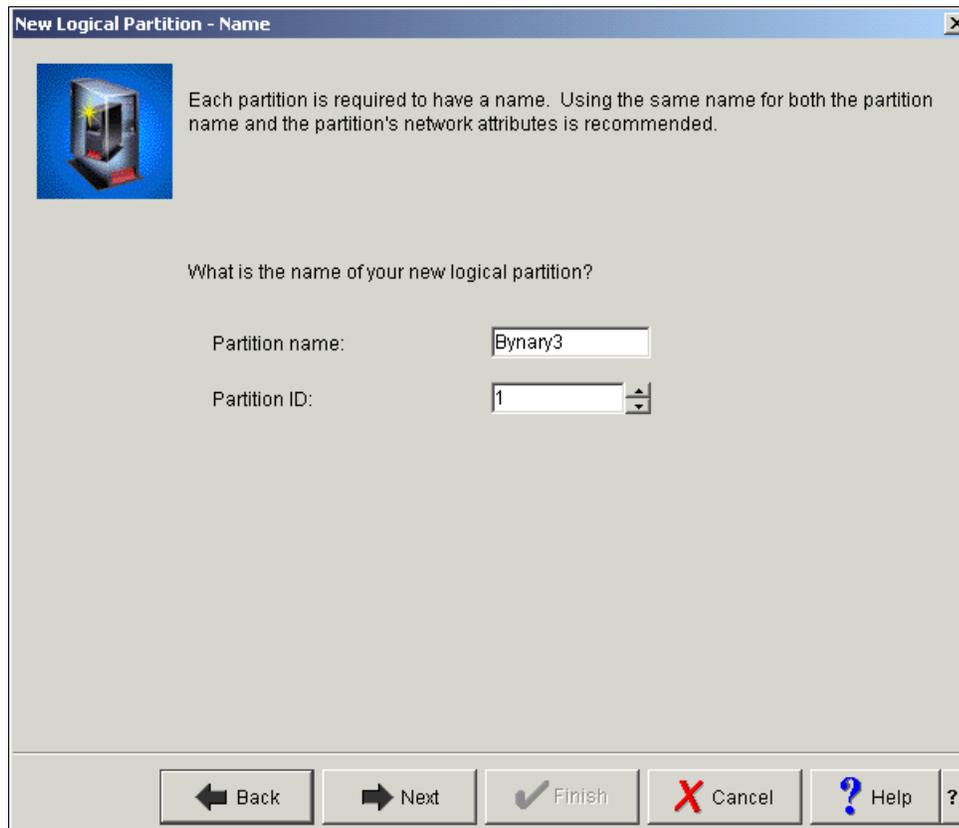

Figure 2-11   Creating a Linux partition: Giving the partition a name

5. On the New Logical Partition Bynary3 - Memory window (Figure 2-12), move the memory that you assign in the Unassigned Hardware space to your new Linux partition. Click **Next** to continue.
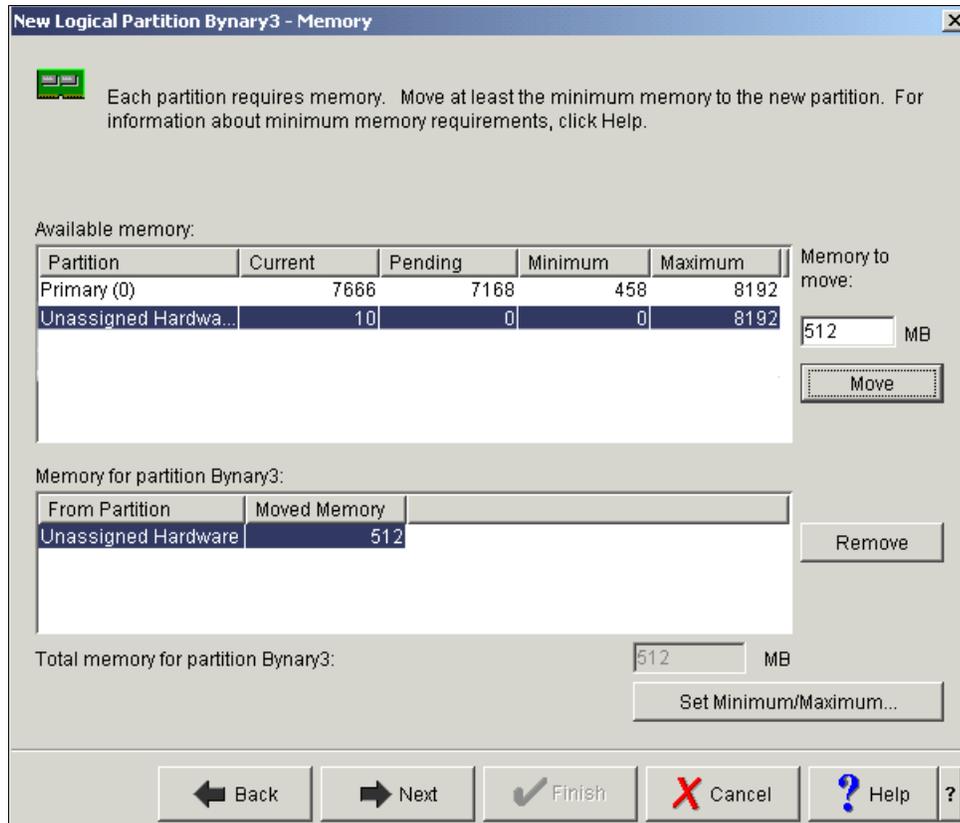

Figure 2-12   Creating a Linux partition: Allocating memory

6. On the New Logical Partition Bynary3 - Processor Type window (Figure 2-13), specify the type of processor for the partition. If you decide to choose a dedicated partition, you must separate one full processor. In our case, we chose the **Shared processor** option. Click **Next** to continue.
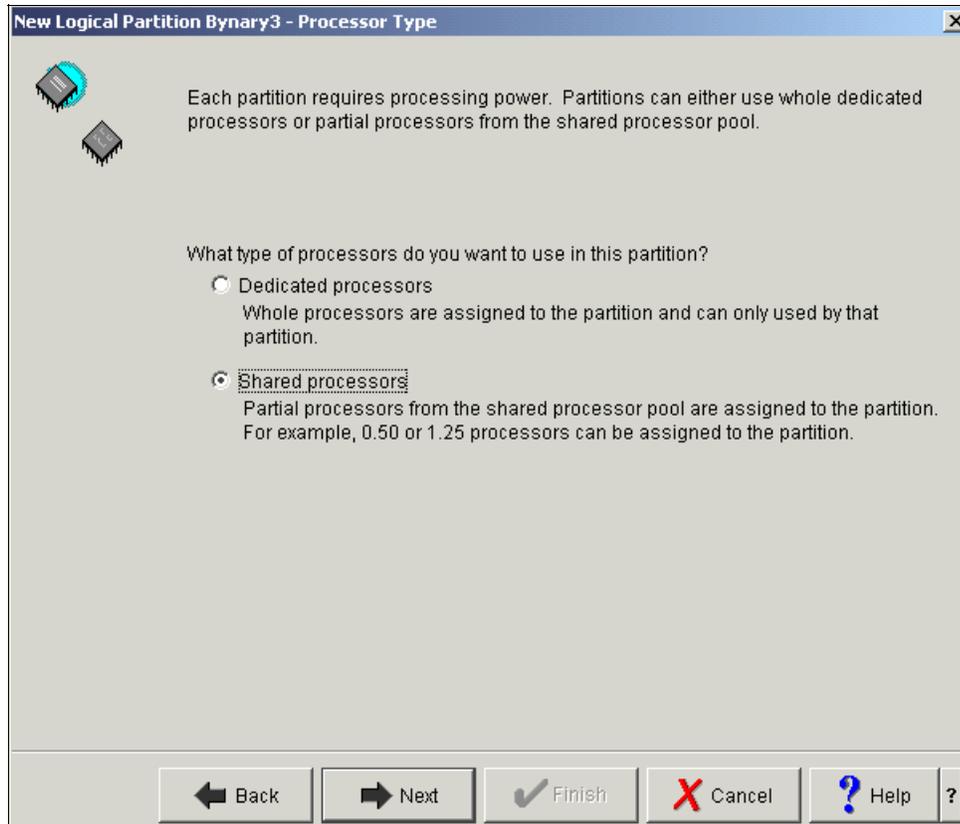

Figure 2-13   Creating a Linux partition: Selecting the processor type

7. As with the memory, move the processing power, from Unassigned Shared, to your Linux partition as shown in Figure 2-14. Click **Next**.
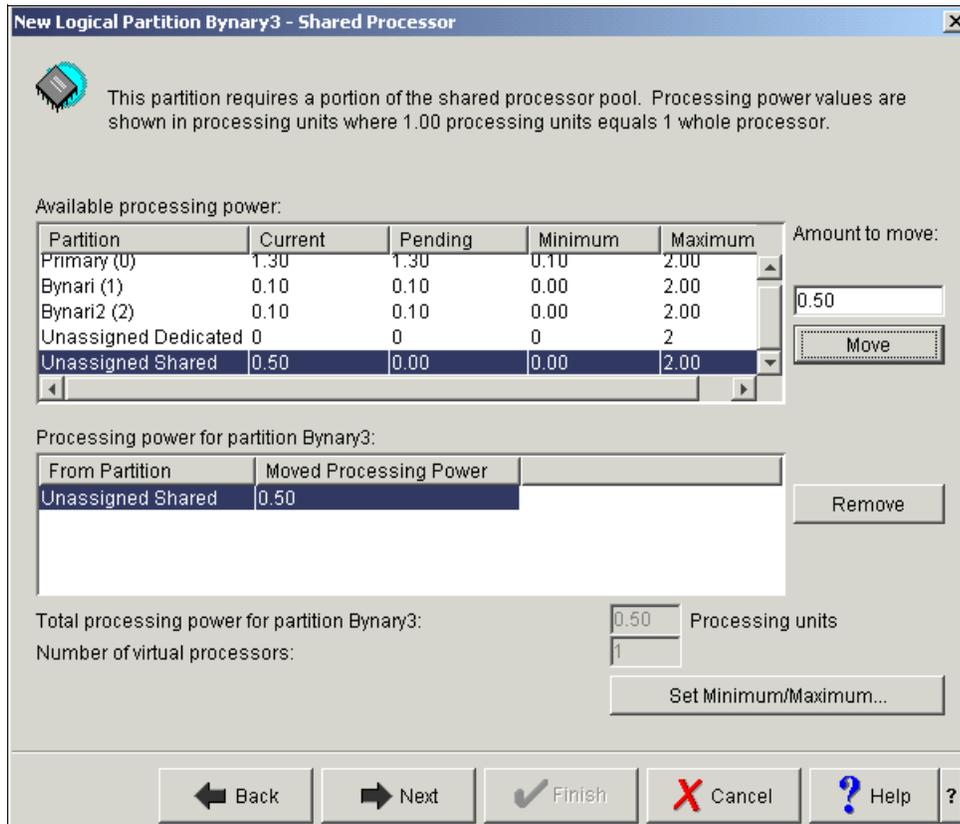

Figure 2-14   Creating a Linux partition: Allocating a processor

8. On the New Logical Partition Bynary3 - Virtual Ethernet window (Figure 2-15), specify the virtual LAN port for the partition. In our example, we chose full communication between partitions but you can select only one communication line. Make sure there is a communication between the host partition and guest partition by having the host partition and guest partition attached to the same virtual LAN.

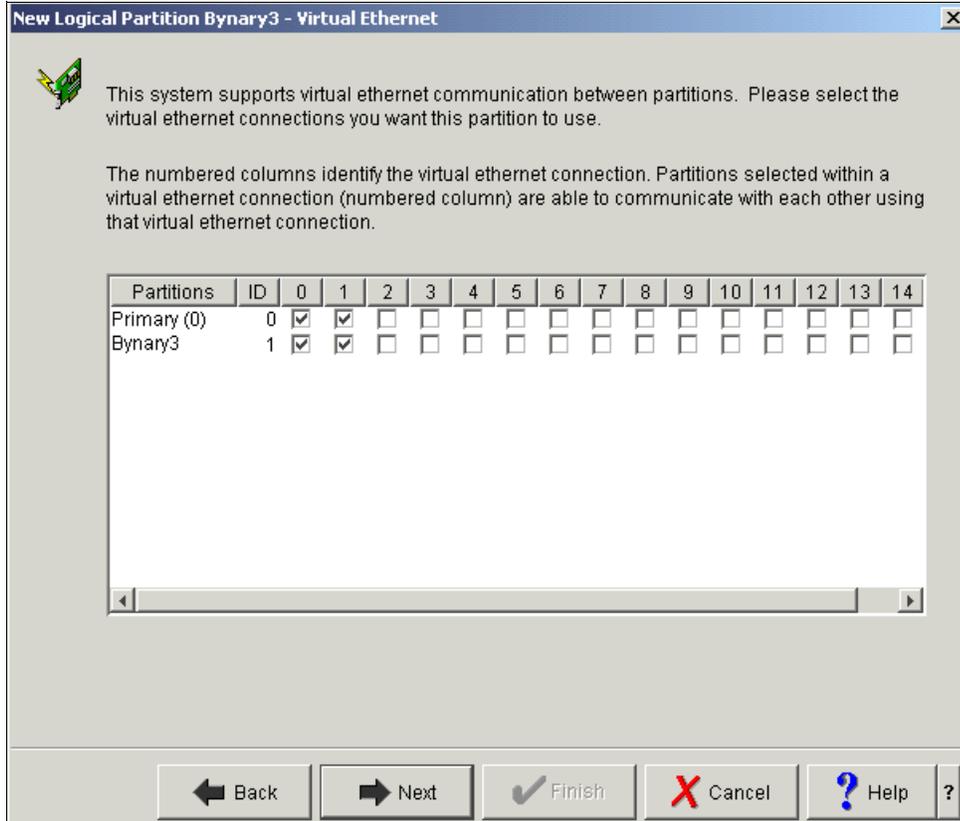*Figure 2-15   Creating a Linux partition: Virtual Ethernet*

9. The New Logical Partition Bynary3 - Select OS/400 Host Partition window (Figure 2-16) displays a list of partitions that are available to host the Linux partition. In this case, only the primary partition is available (which is what we chose). Click **Next**.
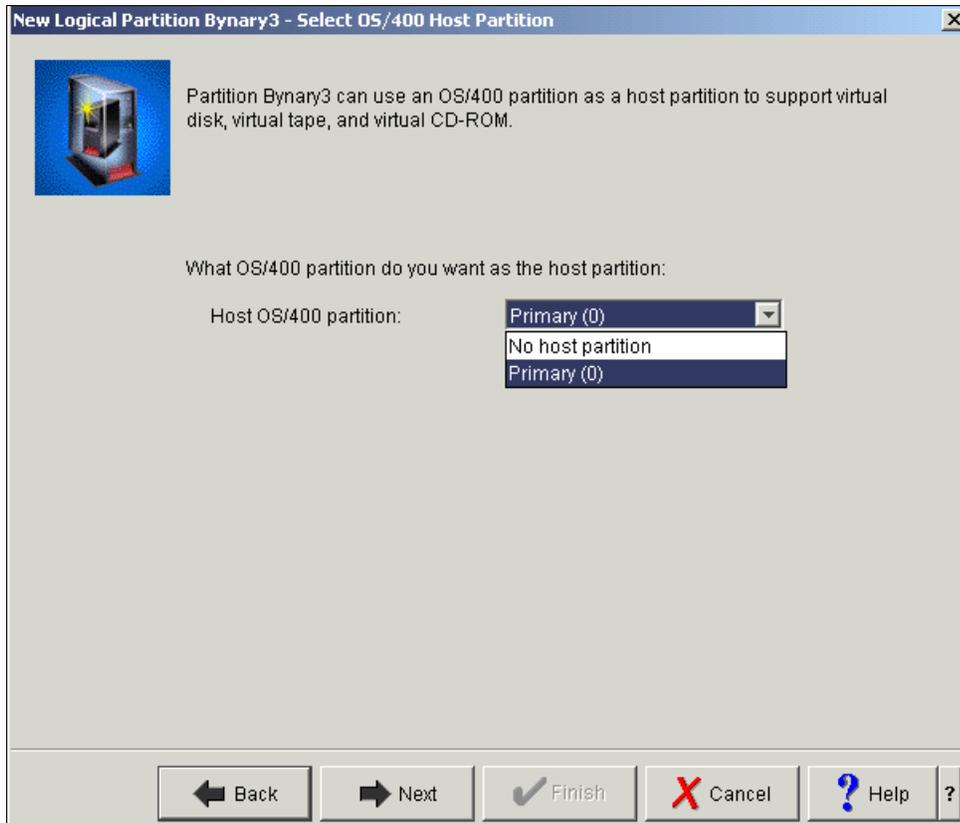

Figure 2-16   Creating a Linux partition: Selecting a host partition

10. You see the New Logical Partition Bynary3 - Summary window (Figure 2-17) that resumes the configuration of your Linux partition. Click the **Finish** button.
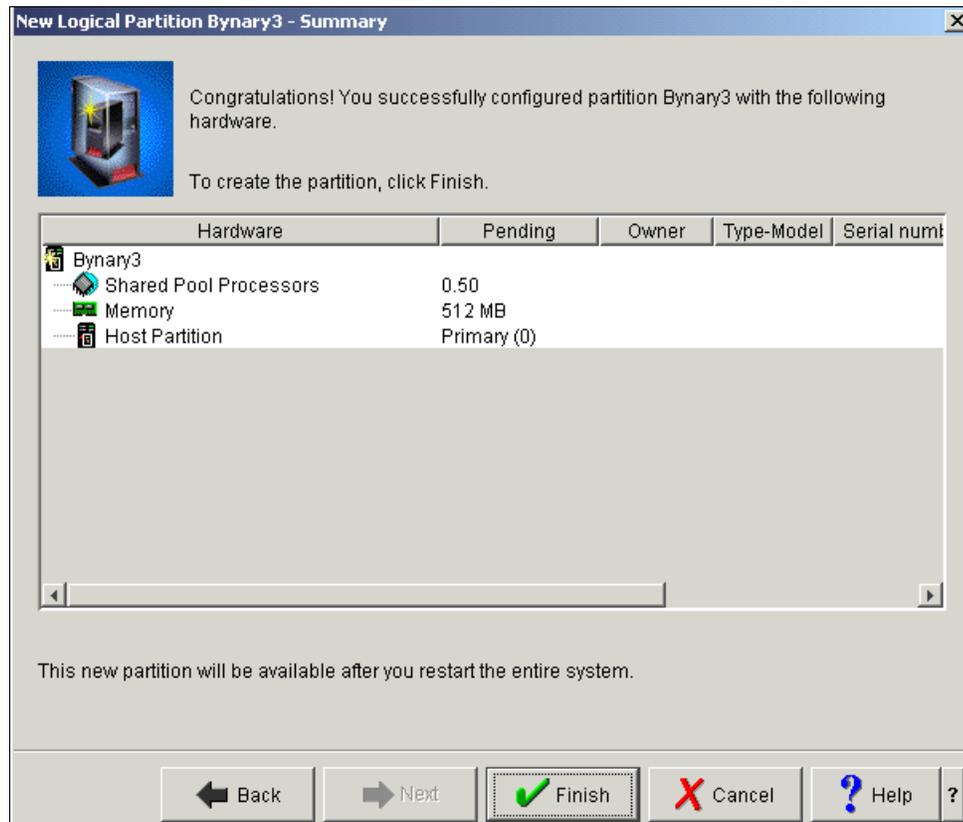
Figure 2-17   Creating a Linux partition: Summary window

11. Activate your new partitions. To do this, you must perform an initial program load (IPL) on the primary partition. Enter the PWRDWNSYS command from active OS/400 primary partition.

2.2.3 Creating Linux disks with iSeries Navigator

To make Linux disks, follow these steps using iSeries Navigator:

1. Open your iSeries server. Expand *your server*-> **Network-> Windows Administration**. Click **Disk Drives**. See Figure 2-18.

2. Click the **Create a new disk drive for windows servers** option in the lower right panel of the iSeries Navigator window.

Figure 2-18   Creating disks

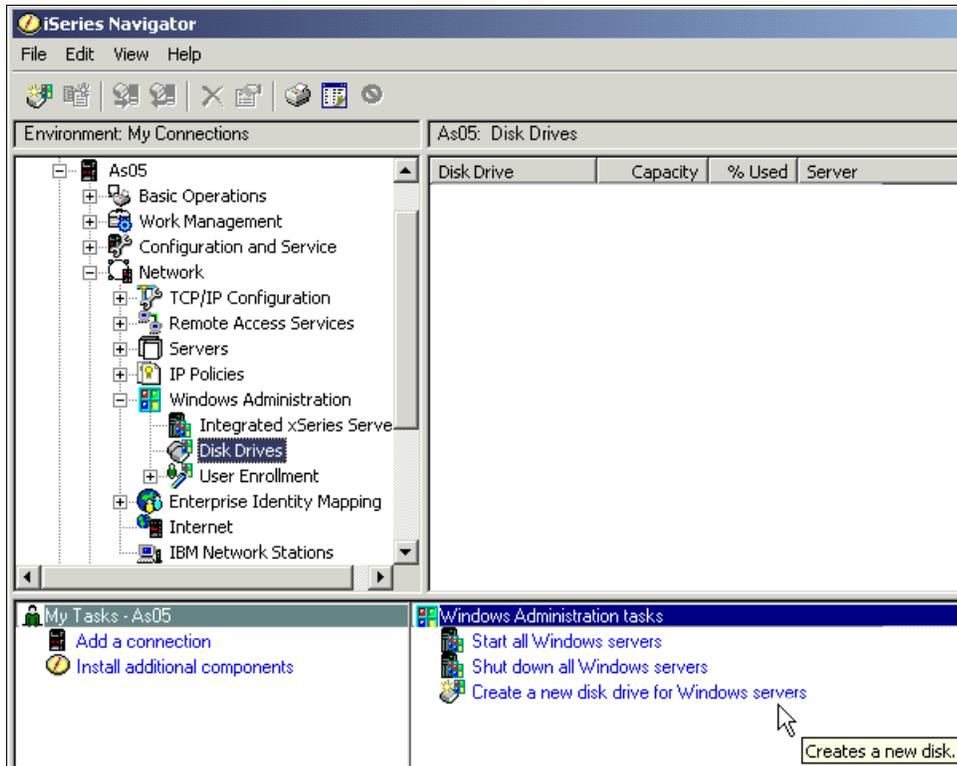3. The New Disk window (Figure 2-19) opens. Enter the information for the disk drive name, description, and capacity. We recommend that you use the same name as the partition. Click the **OK** button.
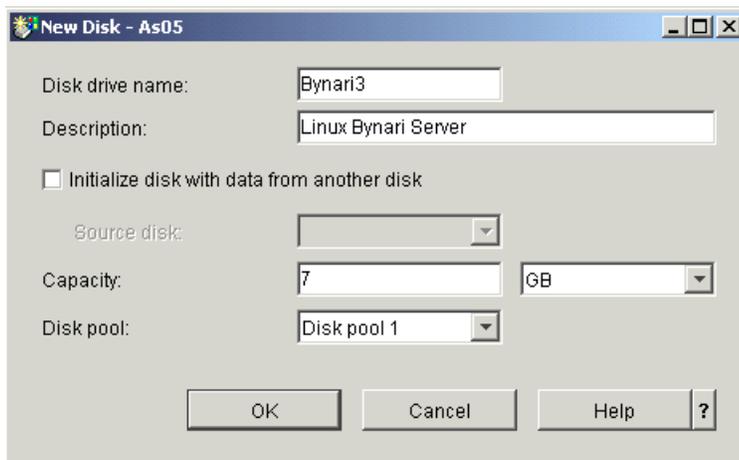

Figure 2-19   Defining a new disk

Now your new disk appears in the iSeries Navigator window, under the Disk Drives panel (Figure 2-18).

2.2.4 Creating the Network Server Description

To create a NWSD, enter the Create Network Server Description (CRTNWSD) command. On the Create Network Server Desc (CRTNWSD) display (Figure 2-20), notice the following parameters:

- ► **Network server description** is the name of the NWSD. We recommend that you use the same name as your partition.

- ► **Resource name** is *NONE.

- ► **Network server type** is *GUEST.

- ► **Online at IPL** is *NO. If you choose *YES, the Linux partition starts with the Partition 0 boot.

- ► **Code page** is 437.

- ► **IPL source** needs to be set as *STMF at installation. Later, you must set this as B when you run Linux after the installation.

- ► **IPL stream file** must be set as the value of the path of the stream file from which the server would boot when *STMF is specified as the IPL source.

- ► **IPL parameters** actual value depends on the Linux distribution that you are installing. Refer to your installation manual for more information.

```
                  Create Network Server Desc (CRTNWSD)

 Type choices, press Enter.

 Network server description . . . > BYNARI3       Name
 Resource name  . . . . . . . . . > *NONE         Name, *NONE
 Network server type  . . . . . . > *GUEST        *WINDOWSNT, *GUEST
 Online at IPL  . . . . . . . . . > *NO           *YES, *NO
 Vary on wait . . . . . . . . .     *NOWAIT       *NOWAIT, 1-15 minutes
 Partition  . . . . . . . . . .                   Name
 Code page  . . . . . . . . . . > 437             *LNGVER, 437, 850, 852, 857...
 Server message queue . . . . .     *JOBLOG       Name, *JOBLOG, *NONE
   Library  . . . . . . . . . .                   Name, *LIBL, *CURLIB
 TCP/IP port configuration:
   Port . . . . . . . . . . . .     *NONE         *NONE, 1, 2, 3, 4...
   Internet address . . . . . . .
   Subnet mask  . . . . . . . . .
   Maximum transmission unit  . .                 Number
   Gateway address  . . . . . . .
               + for more values

                                                             More...

 IPL source . . . . . . . . . . .   *NWSSTG       *NWSSTG, *PANEL, *STMF, A...
 IPL stream file  . . . . . . . .   *NONE

 IPL parameters . . . . . . . . .   *NONE
 Authority  . . . . . . . . . . .   *LIBCRTAUT    Name, *LIBCRTAUT, *CHANGE...
 Text 'description' . . . . . . .   Bynari Insight Server

                                                             Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 2-20   Create Network Server Description

You can view the NWSD and determine its status by entering the following command:

WRKCFGSTS *NWS

On the display that opens, you can select to vary on (option 1) or vary off (option 2) your Linux partition.

2.2.5 Linking Linux disks

To associate the storage space with a server, you must link it to the NWSD. This establishes the pointers in the NWSD.

1. Enter the Work with Network Server Storage Spaces (WRKNWSSTG) command.

2. On the display (Figure 2-21) that appears, select option 10.

```
                    Work with Network Server Storage Spaces
                                                           System: AS05
 Type options, press Enter.
   1=Create   3=Copy   4=Delete   5=Display   6=Print   10=Add link
   11=Remove link


                    %                           Link
 Opt  Name        Used   Size  Server    Drive  Type  Format    Access      ASP


  10 BYNARI3       0    10240                         *NTFS                   1


                                                                        Bottom
 Parameters or command
 ===>
 F3=Exit   F4=Prompt   F5=Refresh   F6=Print list   F9=Retrieve
 F11=Display text      F12=Cancel   F17=Position to
```

Figure 2-21   Work with Network Server Storage Spaces display

3. The Add Server Storage display (Figure 2-22) opens. Enter the information for your NWSD name.

```
                     Add Server Storage Link (ADDNWSSTGL)

 Type choices, press Enter.

 Network server storage space . . > BYNARI3       Name
 Network server description . . . > BYNARI3       Name
 Dynamic storage link . . . . . . > *YES          *NO, *YES
 Drive sequence number  . . . . .   *CALC         1-64, *CALC, *QR

                         Additional Parameters

 Access . . . . . . . . . . . . .   *UPDATE       *UPDATE, *READ, *SHRUPD


                                                                     Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 2-22   Add a Server Storage Link (ADDNWSSTGL) display

Now your server storage is added to the NWSD as shown in Figure 2-23.

```
                    Work with Network Server Storage Spaces
                                                         System:    AS05
 Type options, press Enter.
   1=Create   3=Copy   4=Delete   5=Display   6=Print   10=Add link
   11=Remove link

                    %                           Link
 Opt  Name        Used   Size  Server    Drive Type Format    Access      ASP


      BYNARI3       0   10240  BYNARI3     1    *DYN *NTFS     *UPDATE       1




                                                                    Bottom
 Parameters or command
 ===>
 F3=Exit    F4=Prompt    F5=Refresh    F6=Print list    F9=Retrieve
 F11=Display text        F12=Cancel    F17=Position to
 Network server storage space link added.
```

Figure 2-23   Work with Network Server Storage Space: Linking to NWSD

2.2.6 Configuring the virtual LAN

To configure the network environment, you must configure both the OS/400 partition and the
Linux partition.

On the OS/400 partition

Configuration on OS/400 partition needs to be done to communicate from the network to the
host partition using a LAN adapter over virtual LAN. Follow these steps to create the
communication environment:

1. Create an Ethernet line description. Enter the Create Ethernet Line (CRTLINETH)
   command.
2. Create an interface for the OS/400 side of the virtual LAN.
3. Create the NAT from virtual LAN interface to the OS/400 network.

Creating an Ethernet line description

The following example shows the command to create an Ethernet line description for virtual
LAN:

CRTLINETH LIND(VETH) RSCNAME(CMN05) LINESPEED(1G) DUPLEX(*FULL)

In this command, note the following explanation:

▶ LIND is the name of the new line.

▶ RSCNAME is the name of the resource that you want to use. You can use the
   WRKHDWRSC *CMN command to see the virtual resource that you define when you
   create the new partition as shown in Figure 2-24.

The virtual resource is actually defined to the OS/400 as type 268C. In the example in Figure 2-24, two virtual LAN ports are available with type 268C. They are resource CMN05 and CMN06.

► LINESPEED and DUPLEX are options of the Ethernet communication environment.

```
                    Work with Communication Resources
                                                      System:    AS05
 Type options, press Enter.
   5=Work with configuration descriptions   7=Display resource detail


 Opt   Resource        Type  Status             Text
       CMB01           284E  Operational        Combined function IOP
         LIN02         2838  Operational        LAN Adapter
           CMN02       2838  Operational        Ethernet Port
         LIN01         2838  Operational        LAN Adapter
           CMN01       2838  Operational        Ethernet Port
       CMB03           268C  Operational        Combined function IOP
         LIN05         268C  Operational        LAN Adapter
           CMN05       268C  Operational        Ethernet Port
           CMN06       268C  Operational        Ethernet Port




                                                                 Bottom
 F3=Exit    F5=Refresh    F6=Print    F12=Cancel
```

Figure 2-24   Displaying the virtual LAN resource

Creating an interface for the OS/400 side of the virtual LAN

You must create the interface with an IP address that is a subnet of the OS/400 network. Use the Add TCP/IP Interface (ADDTCPIFC) command as shown in the following example:

```
ADDTCPIFC INTNETADR('192.168.1.1') LIND('VETH') SUBNETMASK('255.255.255.0')
```

Note the following explanation:

► INTNETADR is IP address that the virtual LAN uses to communicate between the iSeries and Linux servers.

► LIND is the name of the line that you create in "Creating an Ethernet line description" on page 27.

This interface works like a gateway for your Linux partition. Now you have to create another interface for your local area network with any real device for the NAT utility. In this example, we use the IP address 10.1.1.5 on a line description called ETHLINE.

Start this device by entering the following command:

```
STRTCPIFC INTNETADR('10.1.1.5')
```

You can enable IP datagram forwarding with the following command:

```
CHGTCPA IPDTGFWD(*YES)
```

Creating the NAT from the virtual LAN interface to the OS/400 network

To create NAT using the virtual LAN interface to the OS/400 network, follow these steps using iSeries Navigator:

1. Open iSeries Navigator. Expand **your server-> Network-> IP Policies**. Select **Packet Rules**. See Figure 2-25.

2. In the bottom right panel, select the **Edit IP Packet Rules** option under IP Policies tasks or click the Rules Editor button (beneath the menu bar).
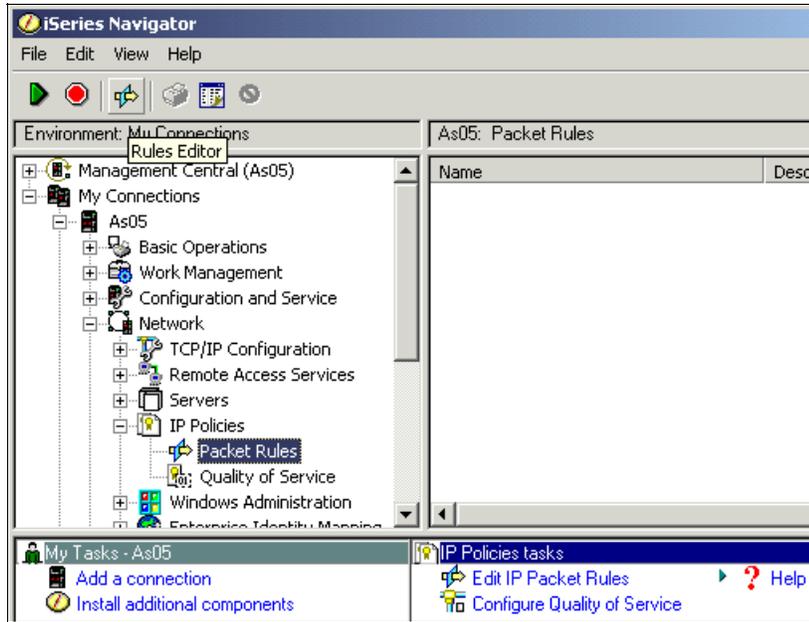

Figure 2-25   iSeries Navigator: Package Rules

3. The Packet Rules Editor window (Figure 2-26) opens. On the Welcome window, select the **Create a new packet rules file** option and click **OK**.
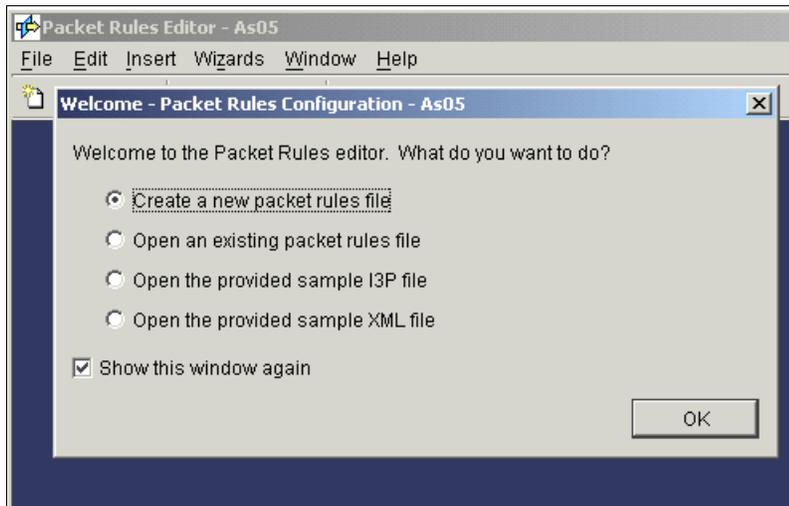

Figure 2-26   Packet Rules Editor

4. A text mode panel of the Packet Rules Editor window (Figure 2-27) opens. Type the following contents of the new packet rules:

```
ADDRESS LINUXPART    IP = 192.168.1.5 TYPE = TRUSTED
###Internal interface - Real address for Linux partition
ADDRESS SHELL    IP = 10.1.1.5 TYPE = BORDER
###Valid external address
```

```
MAP LINUXPART TO SHELL    LINE = ETHLINE    JRN = OFF
###Mapping Address
```
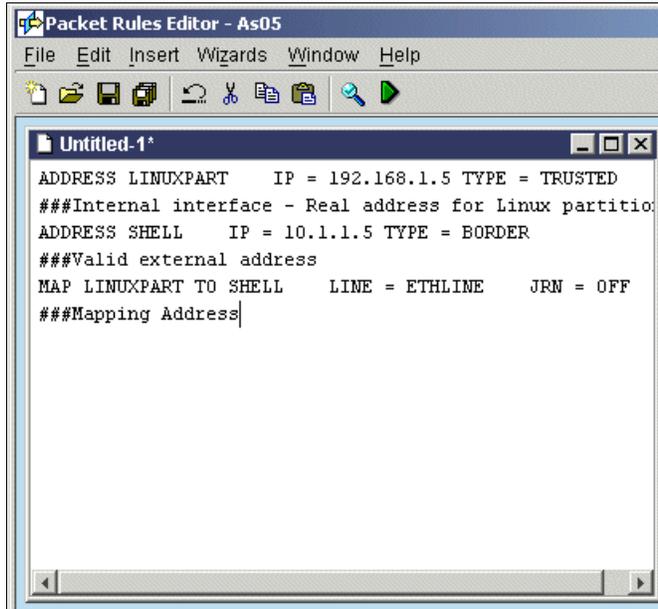

Figure 2-27   Contents of the new packet rules

5. When you are done editing the file, save it as shown in Figure 2-28. In our example, we name the file `bynari1.I3P`.
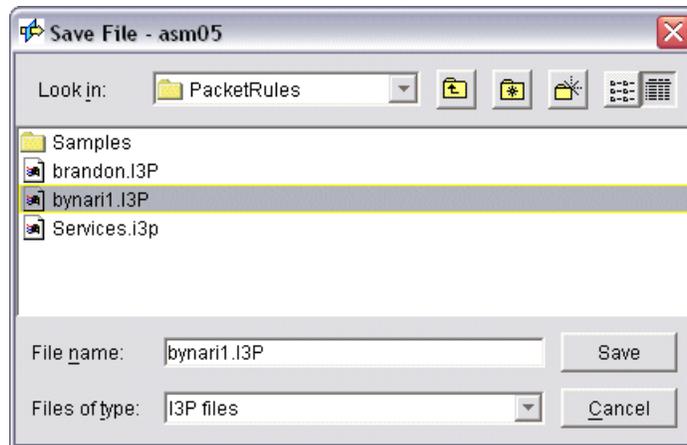

Figure 2-28   Saving the contents

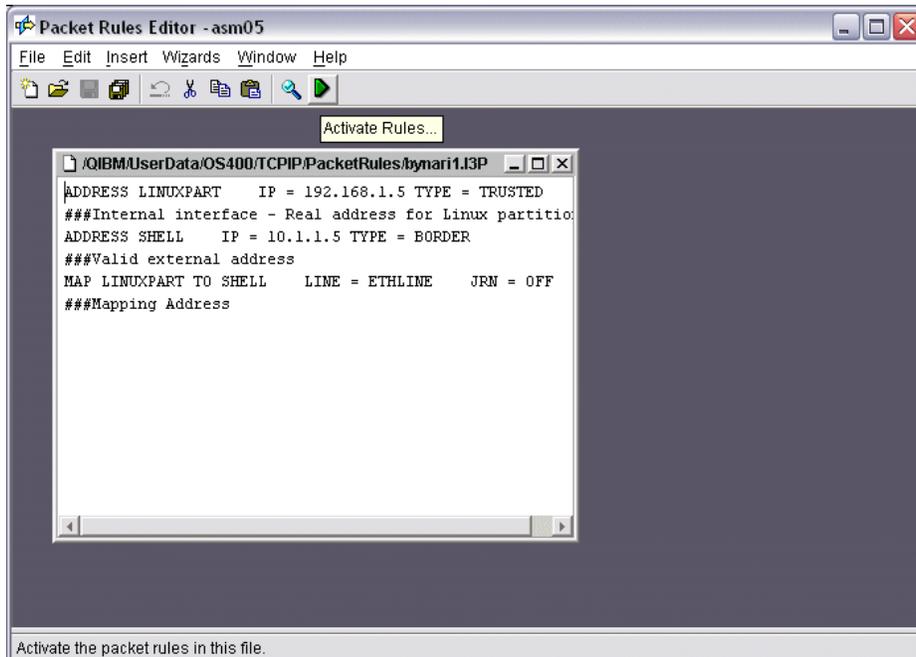6. Activate the newly created rules by clicking the green arrow as shown in Figure 2-29.

Figure 2-29   Activating the newly created rules

7. The Activate Packet Rules window (Figure 2-30) opens. Under Packet rules files, select
   Activate only selected file. Under Interface, select **Activate these rules on all
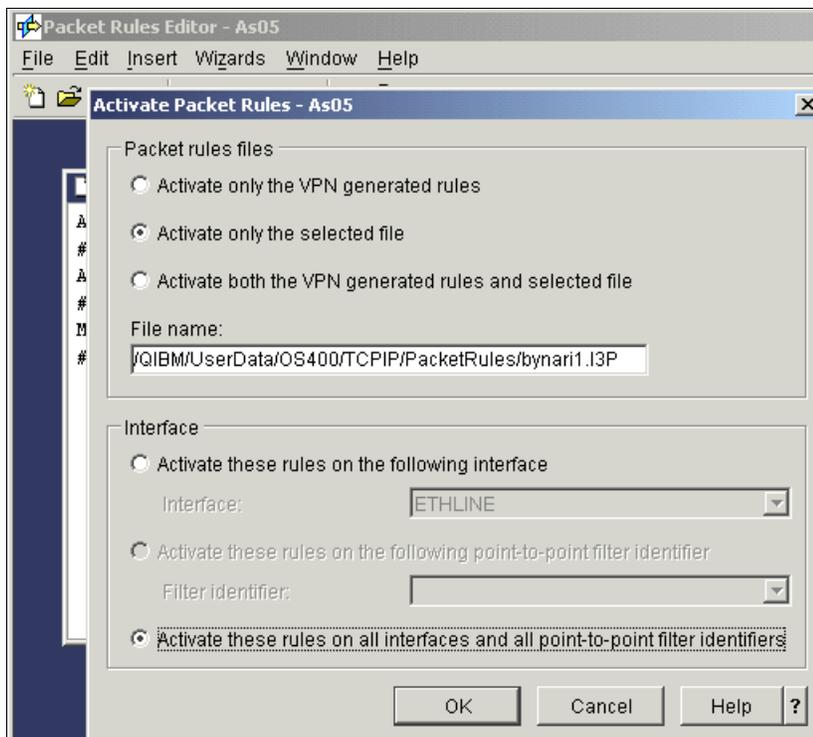   interfaces**. Click **OK**.

Figure 2-30   Activate Packet Rules

8. A confirmation message is displayed on the message window that opens automatically beneath the Rules Editor window. Close the window to end the configuration of NAT.

On the Linux partition

On your Linux partition, you need to set up the TCP/IP environment correctly. Be sure to use the correct IP address, subnet mask, port number (as explained in "Creating an Ethernet line description" on page 27), and gateway IP address.

During the TCP/IP setup in Linux, you need to know your network device. The network device is always ETH or VETH, plus the port number.

This example provides the following values for the Linux server:

► Interface IP address: 192.168.1.5
► Subnet Mask: 255.255.255.0
► Gateway IP address: 192.168.1.1
► Network Device: ETH0

Now your network environment is correctly configured.

2.2.7 Changing the boot parameters of the NWSD

Before you start the Linux server, change the IPL parameter of the NWSD. This parameter differs among Linux distributions. To do this, follow these steps:

1. Run the WRKNWSD command.

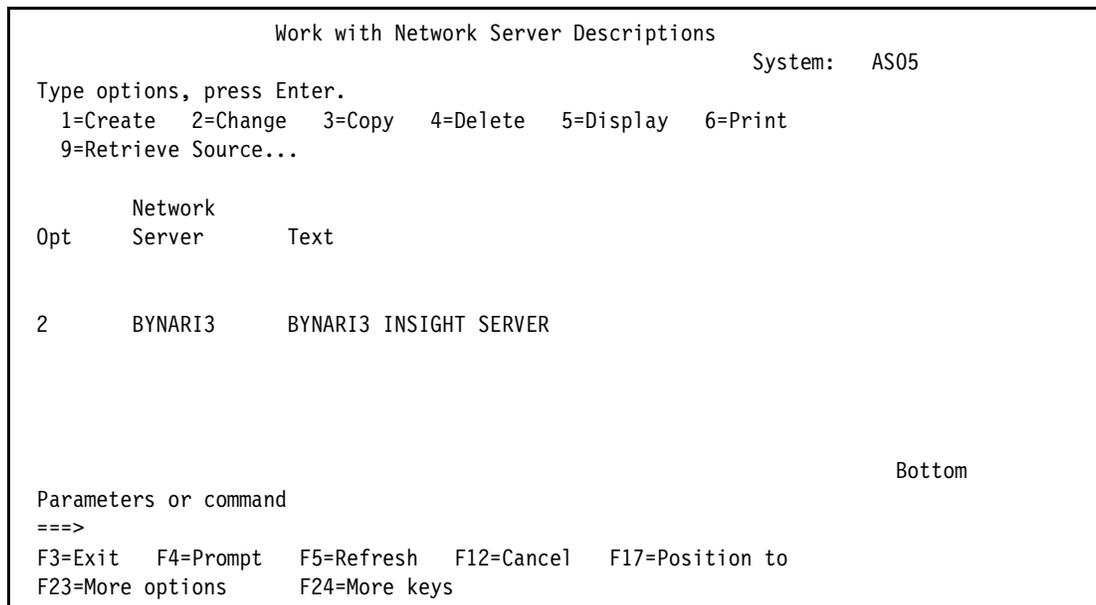2. On the Work with Network Server Descriptions display, select option 2 as shown in Figure 2-31.

```
                   Work with Network Server Descriptions
                                                          System:    AS05
 Type options, press Enter.
   1=Create    2=Change   3=Copy    4=Delete    5=Display    6=Print
   9=Retrieve Source...


        Network
 Opt    Server        Text


 2      BYNARI3       BYNARI3 INSIGHT SERVER




                                                                  Bottom
 Parameters or command
 ===>
 F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F17=Position to
 F23=More options        F24=More keys
```

Figure 2-31   Work with Network Server Description

3. This takes you to the Change Network Server Desc (CHGNWSD) display shown in Figure 2-32. This example shows the IPL parameter for the SLES 8 Linux distribution.

   You need to change three keywords on this display: IPL source, IPL stream file, and IPL parameters. The actual values may vary depending on your Linux distribution or installation method. Refer to your distribution installation manual for more information.

```
                         Change Network Server Desc (CHGNWSD)

 Type choices, press Enter.

 IPL source . . . . . . . . . . .   *STMF         *SAME, *NWSSTG, *PANEL...
 IPL stream file  . . . . . . . .   /QOPT/SU810.001/ISERIES64

 IPL parameters . . . . . . . . .   vnc=1 vnc_password=yourpwd




 Text 'description' . . . . . . .   'BYNARI2 INSIGHT SERVER'




                                                                        Bottom
 F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
 F24=More keys
```

Figure 2-32   Changing NWSD: SLES8 example

2.2.8 Starting the Linux server

Now you can start your server for the first time:

1. Enter the following command:

   WRKCFGSTS *NWS

2. Select option 1.

3. While your server starts, you can connect to the virtual Linux Console using the following command on a DOS command line:

   telnet *sofia* 2301

   In this example, *sofia* is the name of your iSeries server.

4. Enter the user ID and password of the service tools user that you create in 2.2.1, "Creating a service tools user" on page 11. This is illustrated in Figure 2-33.

```
OS/400 Guest Partition Console
 1: BYNARI3
Enter the console partition number:
1
BYNARI3 : Enter OS/400 service tools userid:
YESSONG
BYNARI3 : Enter OS/400 service tools password:
BYNARI3 : Console connecting...
```

Figure 2-33   Connecting to the Linux virtual console

Here begins the real installation of Linux. The following steps vary between Linux distributions. See your Linux documentation to complete the installation.

2.2.9 Starting the Linux partition

After you install and configure your Linux server, change the IPL source when they are booted for the first time. Figure 2-34 shows the keywords that you must change. Again, you must change the keywords IPL source, IPL stream file, and IPL parameters.
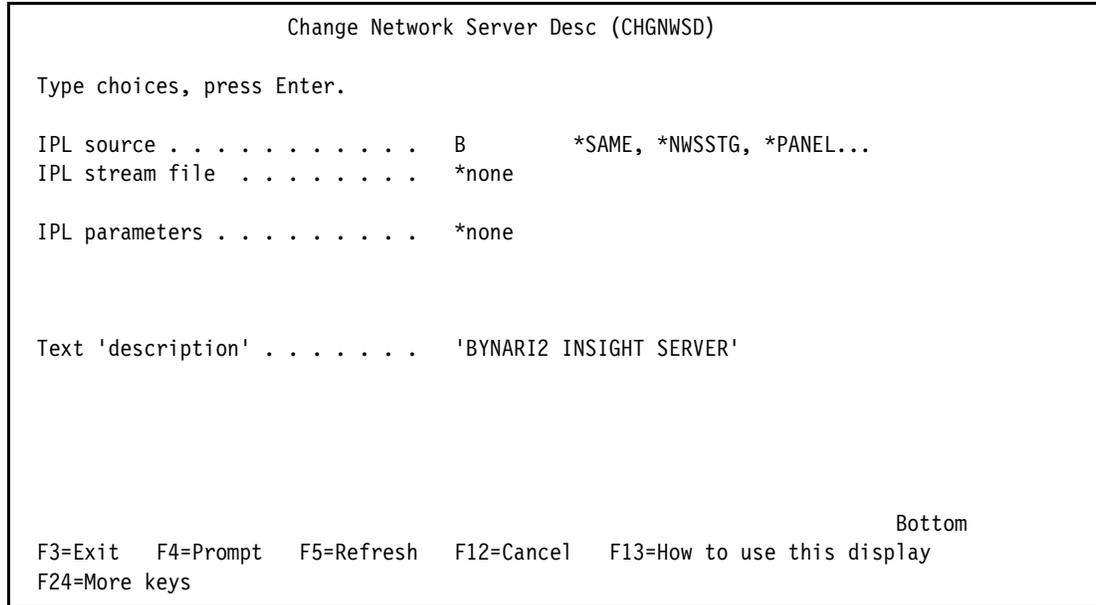
```
                    Change Network Server Desc (CHGNWSD)

 Type choices, press Enter.

 IPL source . . . . . . . . . . .   B          *SAME, *NWSSTG, *PANEL...
 IPL stream file  . . . . . . . .   *none

 IPL parameters . . . . . . . . .   *none




 Text 'description' . . . . . . .   'BYNARI2 INSIGHT SERVER'




                                                                    Bottom
 F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
 F24=More keys
```

Figure 2-34   Changing the IPL source

2.3 Preparing the Linux environment for Bynari Insight Server

Before you begin the installation, you need to disable some services that can cause conflicts, especially with active port numbers, during the installation.

As mentioned in Chapter 1, "Insight Server for the iSeries server" on page 1, Bynari Insight Server is composed of open source packages to provide full functionality. Some of these programs use listening ports for communications between the client and server. Because of this, before you install the Bynari Insight Server, you must verify that these services are not active nor running.

Table 2-1 shows which services can be in conflict.

Table 2-1   List of services and ports that must be disabled

Service	Port
Simple Mail Transfer Protocol (SMTP)	25
Post Office Protocol (POP)	110
File Transfer Protocol (FTP)	20 or 21
Lightweight Directory Access Protocol (LDAP)	389
Internet Message Access Protocol (IMAP)	143

To see if any port is active, run the **netstat** command in a window shell of Linux. The shell is shown in Figure 2-35.

```
bynari:~ # netstat -paln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5801            0.0.0.0:*               LISTEN      715/Xvnc
tcp        0      0 0.0.0.0:5901            0.0.0.0:*               LISTEN      715/Xvnc
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      543/portmap
tcp        0      0 0.0.0.0:6001            0.0.0.0:*               LISTEN      715/Xvnc
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1733/master
tcp        0      0 10.1.1.5:5901           9.10.132.91:3889        ESTABLISHED 715/Xvnc
tcp        0      0 :::22                   :::*                    LISTEN      574/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           459/dhcpcd
udp        0      0 0.0.0.0:111             0.0.0.0:*                           543/portmap
```

Figure 2-35   Running the netstat command in a Linux shell

The Runlevel editor and `ntsysv` are utilities in which we can configure the servers that start automatically at boot time. If any services shown in Table 2-1 are active, use the Runlevel editor in the SuSE Linux server, or use the `ntsysv` program in the RedHat Linux server, to disable the service. Or you can edit the inted.conf file of your Linux server.

2.3.1 Running the Runlevel editor to disable required ports

This section explains how to use the Runlevel editor to disable required ports for SuSE users:

1. Open KDE Control Center. In the left panel, select **YaST2 Modules-> System-> Runlevel editor** (Figure 2-36).
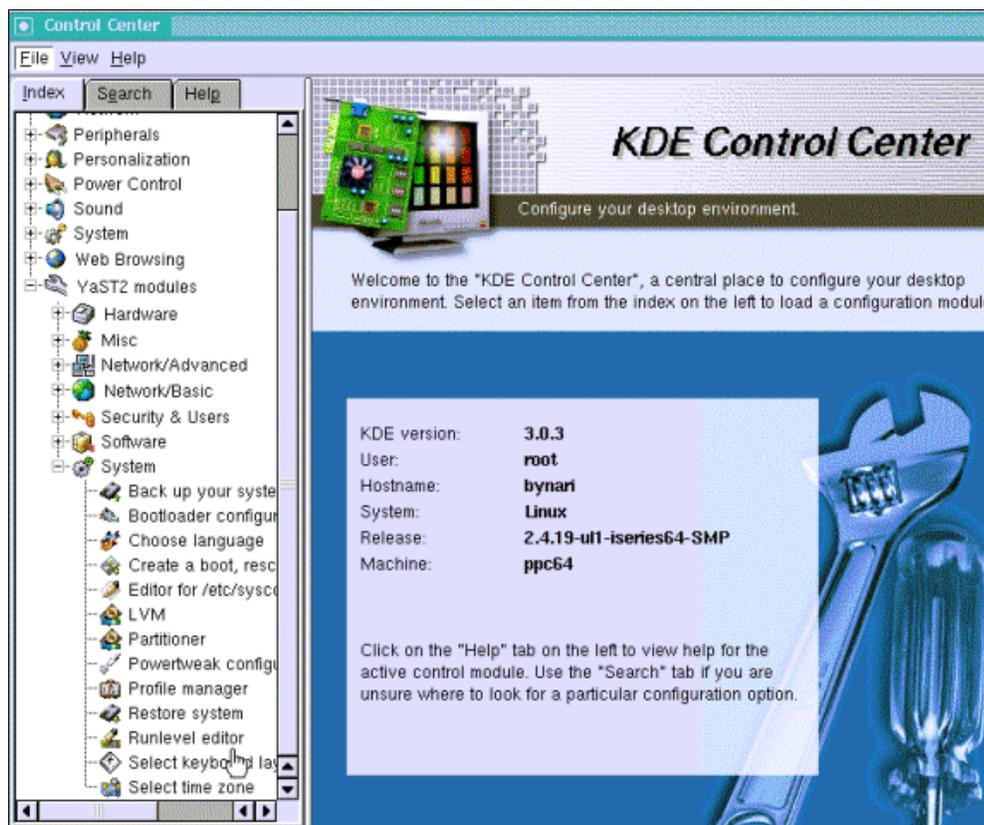
Figure 2-36   SuSE Control Center

2. On the Runlevel editor: default runlevel window (Figure 2-37), click **Runlevel properties**.
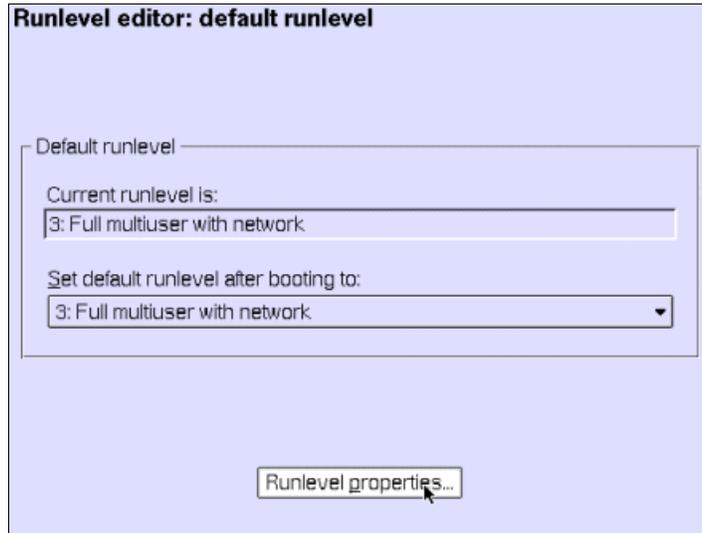
Figure 2-37   Runlevel editor: default runlevel

3. A new window opens to disable a service. Complete these tasks:

   a. Click to select the server.

   b. Verify whether the server is running by looking under the Running column. Yes indicates that you have to stop them.

   c. Click the **Start/Stop/Refresh** button to stop the server.

   d. Deselect the run levels at which the service runs. In this example (see Figure 2-38), the service *postfix* is running. It starts in runlevels 3 and 5.

   e. Click the **Finish** button to exit.
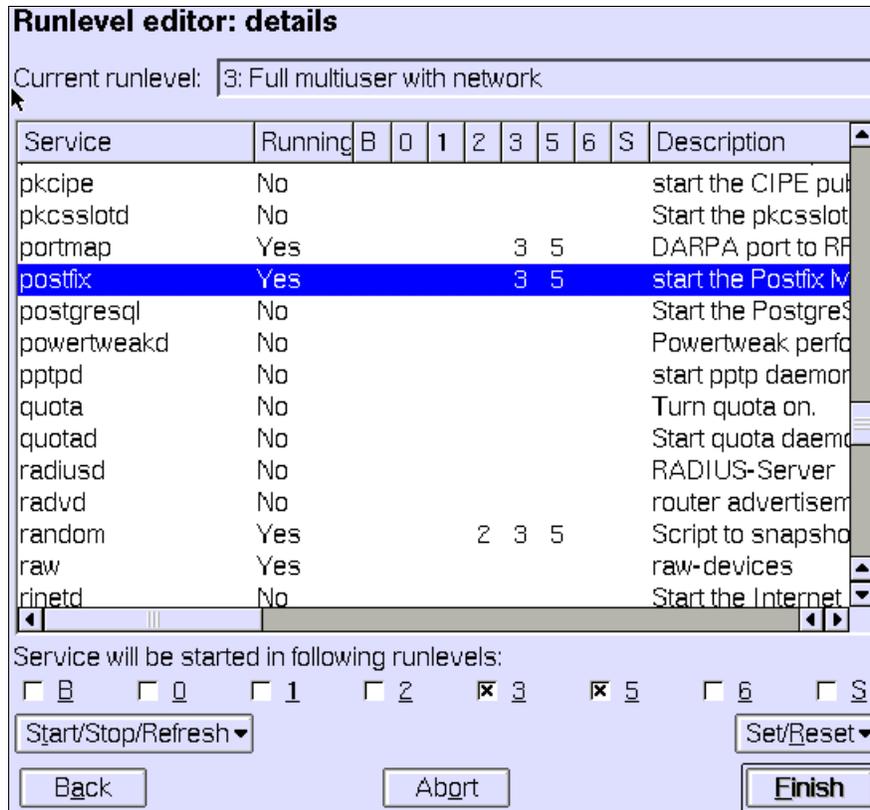
Figure 2-38   Runlevel editor: details

Editing the inetd.conf file to disable required ports

In some cases with SuSE, you may not find the services you need on the Runlevel editor. If that's the case, you need to edit the inetd.conf file.

The inetd.conf file contains the configuration of the network services that starts when you start Linux. You simply comment or uncomment the services that you want to enable or disable when starting up Linux. Figure 2-39 illustrates the contents of a inetd.conf file. If you have services to be disabled, simply insert the comment tag (#) and restart the server.

```
# If you make changes to this file, either reboot your machine or send the
# inetd a HUP signal with "/etc/init.d/inetd reload" or by hand:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that signal.
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# echo stream tcp nowait root internal
# echo dgram udp wait root internal
# discard stream tcp nowait root internal
# discard dgram udp wait root internal
# daytime stream tcp nowait root internal
# daytime dgram udp wait root internal
# chargen stream tcp nowait root internal
# chargen dgram udp wait root internal
# time stream tcp nowait root internal
# time dgram udp wait root internal
#
# These are standard services.
#
# ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd
# ftp stream tcp nowait root /usr/sbin/tcpd vsftpd
#
# If you want telnetd not to "keep-alives" (e.g. if it runs over a ISDN
# uplink), add "-n". See 'man telnetd' for more details.
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
# nntp stream tcp nowait news /usr/sbin/tcpd /usr/sbin/leafnode
# smtp stream tcp nowait root /usr/sbin/sendmail sendmail -L sendmail -Am -bs
....
# Pop et al
#
# pop2 stream tcp nowait root /usr/sbin/tcpd ipop2d
# pop3 stream tcp nowait root /usr/sbin/tcpd ipop3d
# pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/popper -s
#
# Imapd - Interactive Mail Access Protocol server
# Attention: This service is very insecure
# imap stream tcp nowait root /usr/sbin/tcpd imapd
The Internet UUCP service.
#
# uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting. Most sites
# run this only on machines acting as "boot servers."
#
# tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
# bootps dgram udp wait root /usr/sbin/bootpd bootpd -c /tftpboot
# swat is the Samba Web Administration Tool
swat stream tcp nowait.400 root /usr/sbin/swat swat
....
#
# End.
```

Figure 2-39   The inetd.conf example file

2.3.2 Running the ntsysv utility to disable required ports

You can use the `ntsysv` utility to disable the required port number for RedHat users:

1. Open a Linux shell and enter the following command:

   `#root> ntsysv`

2. On the window (Figure 2-40) that appears, complete these tasks:

   a. Use the arrows key and press the Spacebar to select or deselect the services.
   b. When you are done, press the Tab key to highlight the OK button.
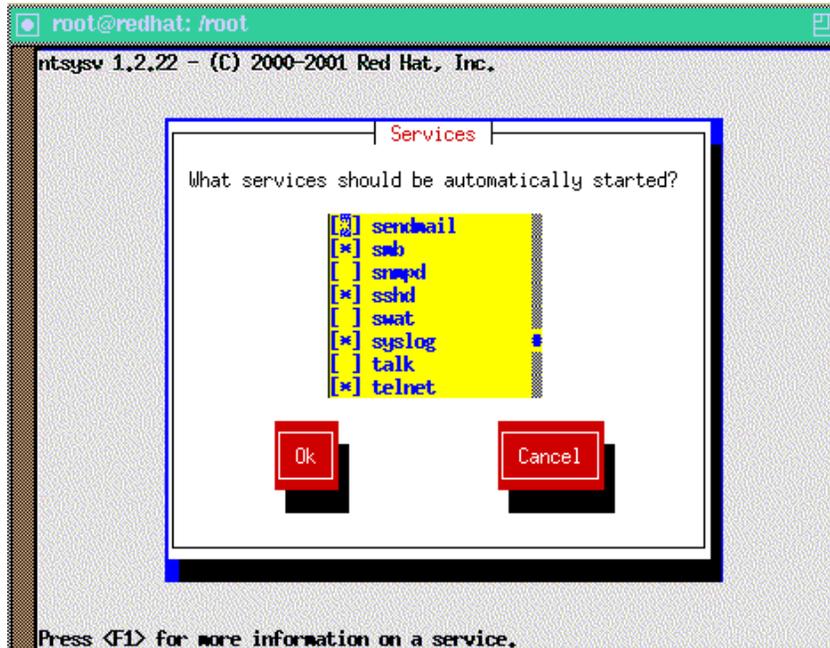   c. Press the Spacebar again to finish the service configuration.

Figure 2-40   The ntsysv command

2.4 Bynari Insight Server installation process

Red Hat Package Manager (RPM) is a powerful, command line-driven package management system. It is capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files along with information about the package like its version and description. RPM is also used to install and uninstall the Bynari Insight Server Program.

Installing Bynari Insight Server

The first step when installing Bynari Insight Server is to obtain the RPM package. This case expects that you already have the package. Follow these steps:

1. You need Linux root privileges to install the software. We recommend that you install the software as *root*.

2. The minimum disk space required for Bynari Insight Server installation is 500 MB. This space should exist under the /opt folder. If you do not have enough space, create new disk space.

   Figure 2-41 illustrates the configuration of disk space on a particular Linux installation using the disk utility of the Linux KDE control manager. As shown in this example, the

original disk drive of /dev/hda3 (the second entry on the right panel) has only 35.8 MB of free space. Therefore, you must create a new disk drive (in other words, a new NWSSTG) with enough space. In this example, we created a new drive, /dev/hdb1, with a size of 2.9 GB. It has 1.7 GB in free space, which should be large enough. Notice that its mount point is /opt.
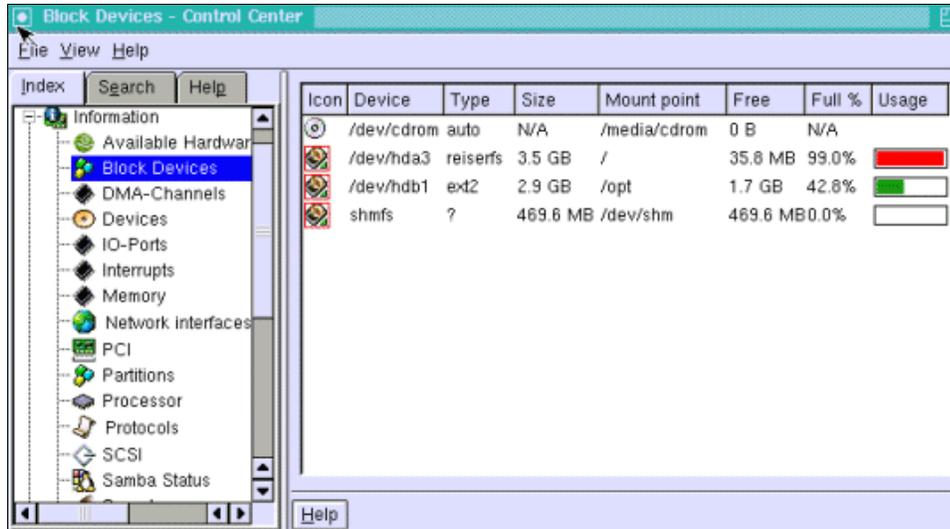
Figure 2-41   Block Devices - Control Center

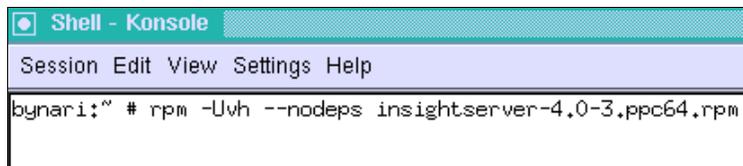3. Start a terminal shell and run the command shown in Figure 2-42.

Figure 2-42   The rpm command

4. Copy the user ID and password that the installation scripts provide you as shown in Figure 2-43. You need the user ID and password for the configuration phase (see 2.4, "Bynari Insight Server installation process" on page 39). If you see the message "`To start Insight Server 4.0 now, run...`" as shown on the eighth line in Figure 2-43, that means the installation is done.
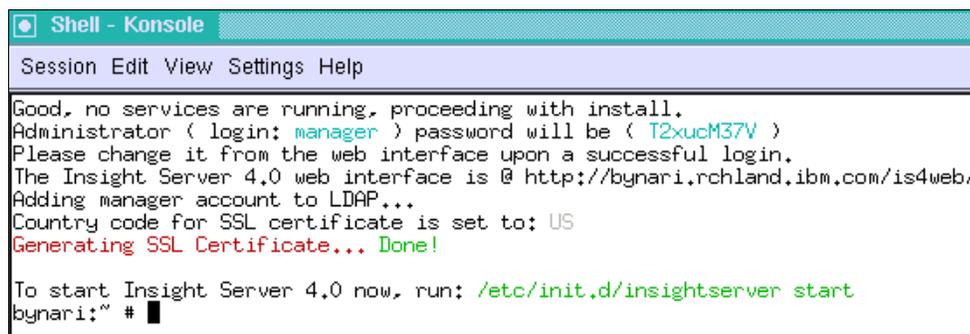
Figure 2-43   Insight installation script

5. To start Insight Server, run the following command under the /etc/init.d folder as shown in Figure 2-44:

`./Insight Server start`

```
bynari:/etc/init.d # ./insightserver start
 * Caching service dependencies...                              [ ok ]
 * Starting syslogd, klogd...                                   [ ok ]
 * Starting apache...                                           [ ok ]
 * Starting saslauthd...                                        [ ok ]
 * Starting Cyrus imapd...                                      [ ok ]
 * Starting postfix...                                          [ ok ]
 * Starting proftpd...                                          [ ok ]
 * Starting ldap-server...                                      [ ok ]
 * Starting vcron...                                            [ ok ]
bynari:/etc/init.d # []
```

Figure 2-44   Starting Insight Server

Uninstalling the Bynari Insight Server

To uninstall the product, run the following command as root:

`#root> rpm -e Insight Server-4.03`

3

Setting up and configuring Bynari Insight Server

This chapter explains step-by-step how to set up and configure the Bynari Insight Server. To complete these operations, you essentially perform two primary tasks. One task is to configure the server. The other task is to configure the clients, either a Microsoft Outlook client or a Web client.

43

3.1 Web Administration Console login

The Insight Server provides a Web interface for configuration. This is the Web Administration Console. The manager user carries out most Insight Server configuration tasks using this Web console. To login to the Web console, you must provide the following information:

► Uniform Resource Locator (URL) of the Insight Server site
► Password for manager user

You can find this information on the installation scripts window shown in Figure 2-43 on page 40. Login to the Web console as shown in Figure 3-1.
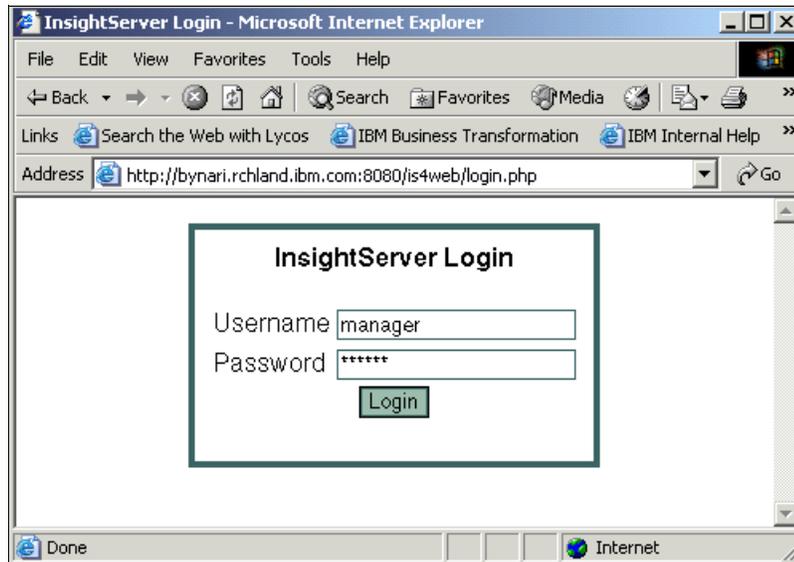
Figure 3-1   Web console login

With the Web Administration Console, you can:

► Manage the server license
► Work with the manager user
► Work with the Account Browser
► Work with the Mailbox Browser
► Configure Bynari Server Services
► Work with mail management
► Check logging files
► Check statistics
► Run schedule tasks
► Perform and restore a backup
► Work with redundancy
► Use the migration wizard
► Use the help browser

3.2 Activating Insight Server with the license key

To activate Insight Server with a license key, follow these steps:

1. Activate the Bynari Insight Server. Click the **About** link in the Web console (Figure 3-2).
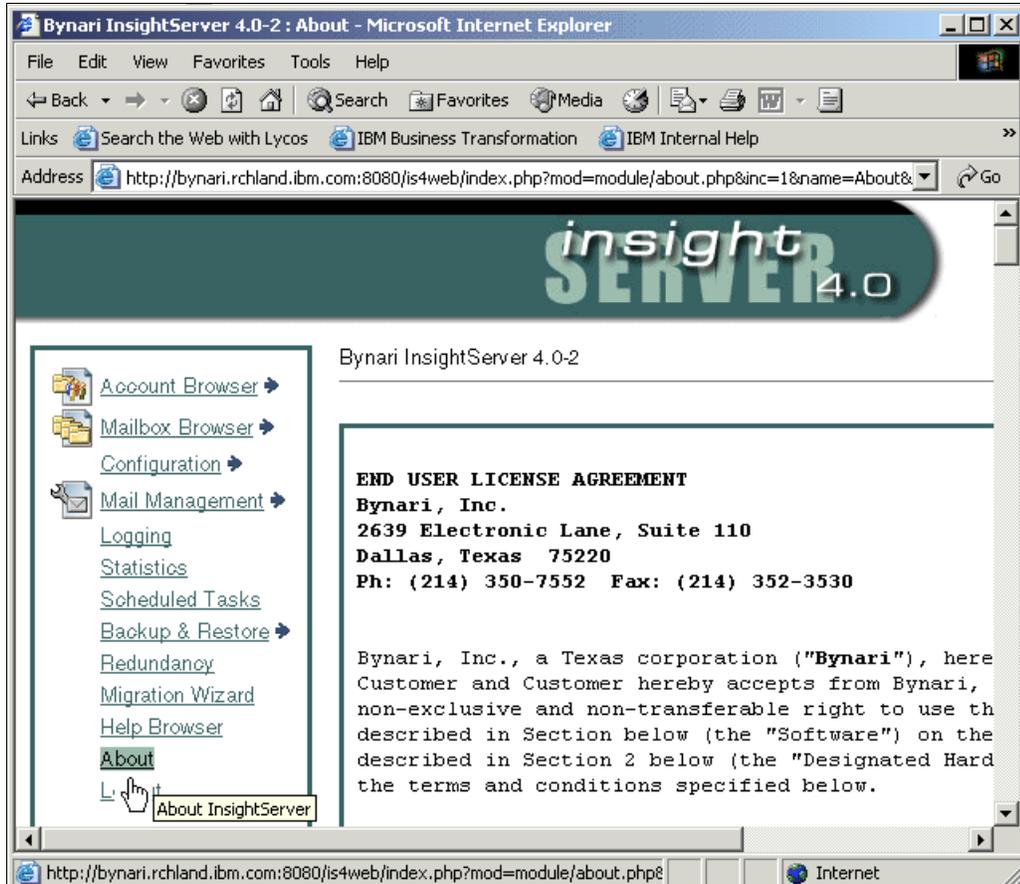
Figure 3-2   Activating Insight Server (Part 1 of 3)

2. Scroll down the page until you see License Key. Type your key in the field as shown in Figure 3-3. This key is sent by e-mail from Bynari. Click the **Submit** button to continue.

Figure 3-3   Activating Insight Server (Part 2 of 3)

3. Scroll to the bottom of the page and check whether your key is activated (see Figure 3-4).

Figure 3-4   Activating Insight Server (Part 3 of 3)

3.3 Working with the manager user

The *manager user* has all the configuration privileges in the Bynari Insight Server environment. For that reason, you must change the default settings before you place the server into production. To change the default settings, follow these steps:

1. Select **Account Browser** in the left menu.

2. On the Create New panel (Figure 3-5), click the **manager user** link.

Figure 3-5   Configuring the manager user

3. Another window opens as shown in Figure 3-6. Here you can modify the manager password. You can assign any person of the organization for the manager role. Enter any information that you think is necessary. Then click the **Update** button.
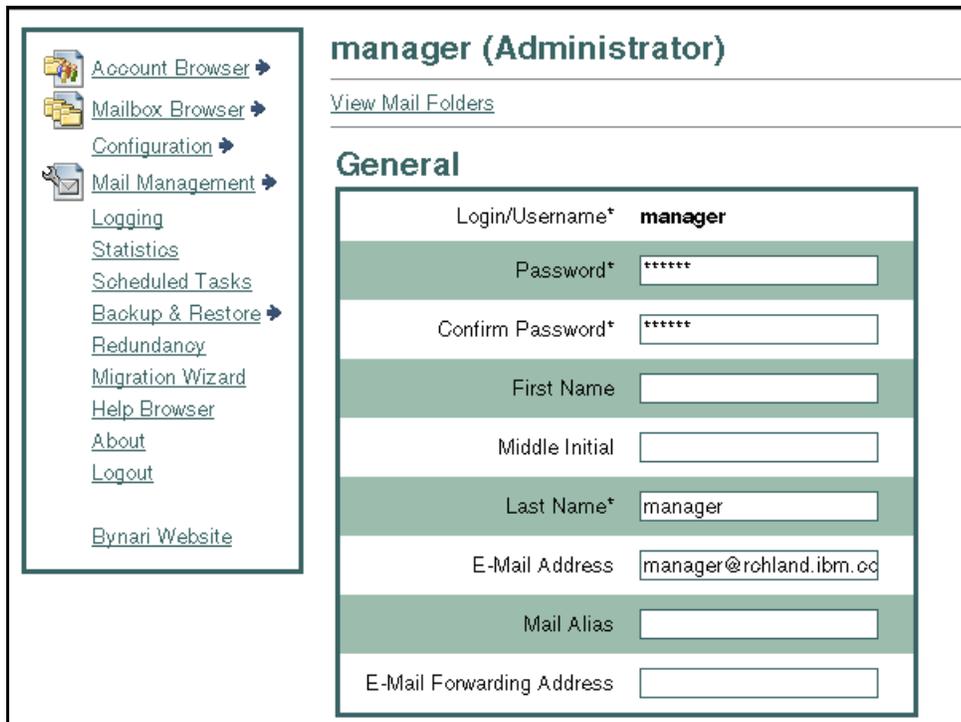
Figure 3-6   Updating the manager profile

3.4 Working with the Account Browser

The *Account Browser* is the administration tool. This utility allows you to create an organization with objects for the domain, organizations, groups inside the organization, users, and resources. These objects reside in the Lightweight Directory Access Protocol (LDAP) server.

The following sections explain how to create these objects.

3.4.1 Creating a domain

If you have only one domain to work with, you don't need to create a new domain. The same domain where Insight Server is installed, rchland.ibm.com in this case, is used for all the resources you create as manager user. If this is the case, you may skip to 3.4.2, "Creating an organization" on page 49.

One of the main characteristics of Binary Insight Server is that the mail server supports multiple domains. The following steps show you how to create a new domain, rchland.bynari.com, where the new organization, Bynari, resides.

1. To create a new Domain organization, click **Account Browser-> Create New-> Domain** as shown in Figure 3-7. Or you can click **Domain** from the navigator bar.
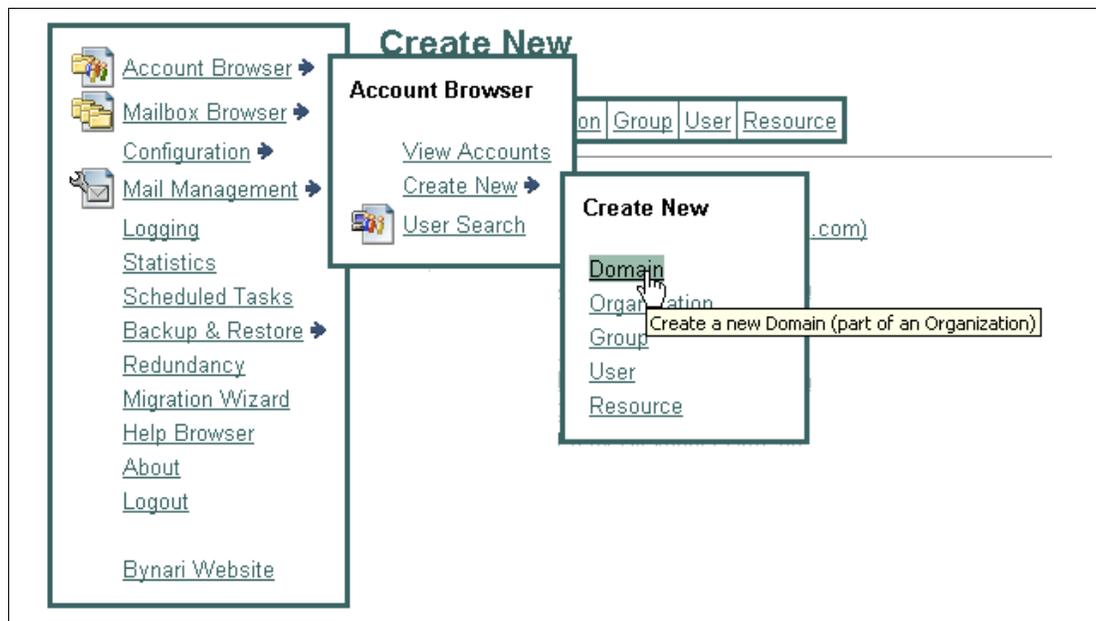
Figure 3-7   Main menu: Creating a new domain

2. The Creating new Domain page (Figure 3-8) opens. Enter the appropriate and necessary information for the Domain. The fields marked with an asterisk (*) indicated *required* information. Then click the **Create** button at the bottom of the page.

Figure 3-8   Creating new Domain: Parameters

3. The new domain and organization now appear in the LDAP tree. The system gives you a message about the status of the insert (see Figure 3-9). The letter "o" means organization.

Figure 3-9   Creating new Domain: LDAP tree

3.4.2 Creating an organization

The *organization* is the root unit in the LDAP tree. For that reason, you must create it before you create users and resources. This example explains how to create a new organization, IBM, in the same domain as Insight Server, rchland.ibm.com.

To create a new organization, follow these steps:

1. Select **Account Browser-> Create New-> Organization** (Figure 3-10). Or you can click **Organization** from the navigator bar.
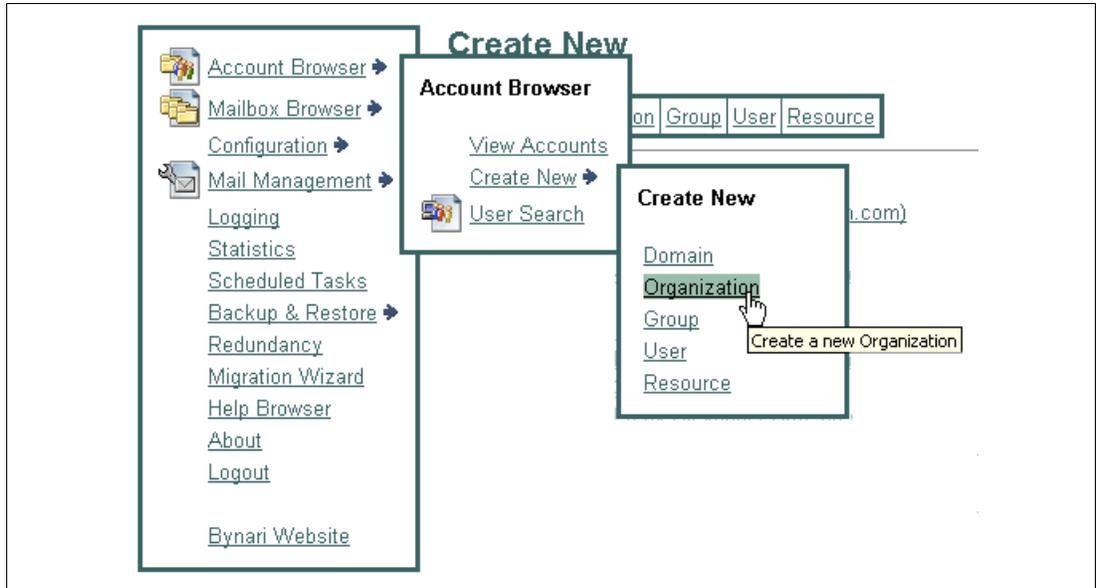
Figure 3-10   Main menu: Creating an organization

2. On the Creating new Organization page (Figure 3-11), complete the fields with your organization's information, such as post office box, address, phone number, and etc. Click the **Create** button toward the bottom of the page to submit the changes.

Figure 3-11   Creating new Organization: Parameters

3. Check the status of your new entry in the LDAP tree. A status message (see Figure 3-12) appears at the top of the page. The new organizations are now displayed as a folder.
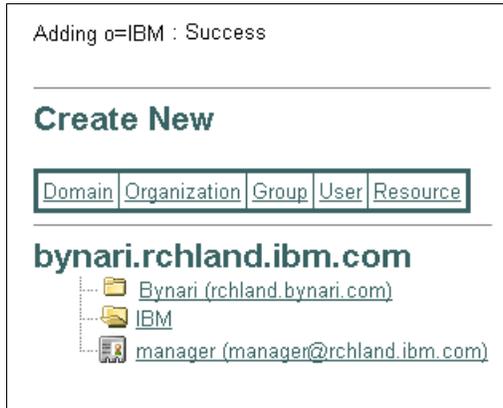
Figure 3-12   Creating new Organization: LDAP tree

3.4.3 Creating a group

A *group* is a subdivision of an organization. A group is useful if you want to identify such business areas as marketing, production, and so on.
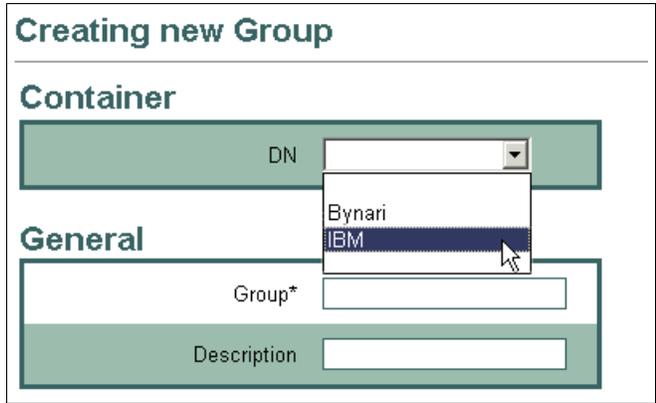
To create a group, follow these steps:

1. From the main menu of the Web Administration Console, select **Account Browser-> Create New-> Group**. Or you can click the **Group** option on the navigator bar as shown in Figure 3-13.


Figure 3-13   Main menu: Creating a new group

2. On the Creating new Group page (Figure 3-14), select the distinguished name (DN). The DN is used for the LDAP to keep an entry unique. In this example, there are two entries in the LDAP server as reflected in the DN option.

Figure 3-14   Creating new Group: LDAP search

3. Enter the information for your group as shown in Figure 3-15. Click the **Create** button.
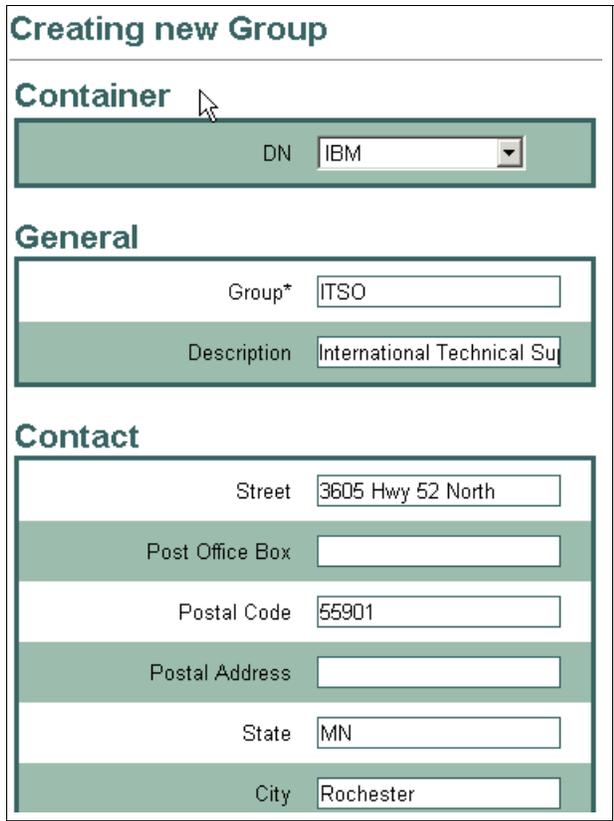
Figure 3-15   Creating new Group: Parameters

As shown in Figure 3-16, the new entry is reflected in the LDAP tree as a subfolder of the organization selected for DN. The letters "ou" mean organizational unit.
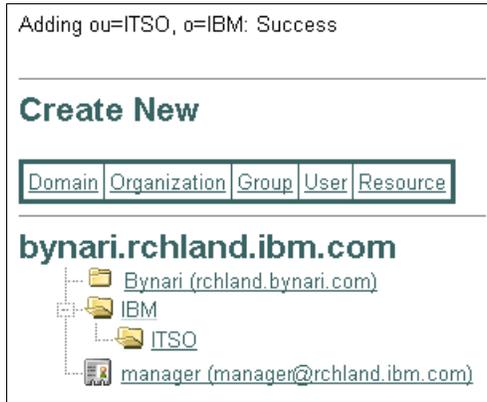

Figure 3-16   Creating new Group: LDAP

3.4.4 Creating a user

To create a new user, follow these steps:

1. From the main menu, select **Account Browser-> Create New-> User** as shown in Figure 3-17. Or you can click the **User** option on the navigator bar.
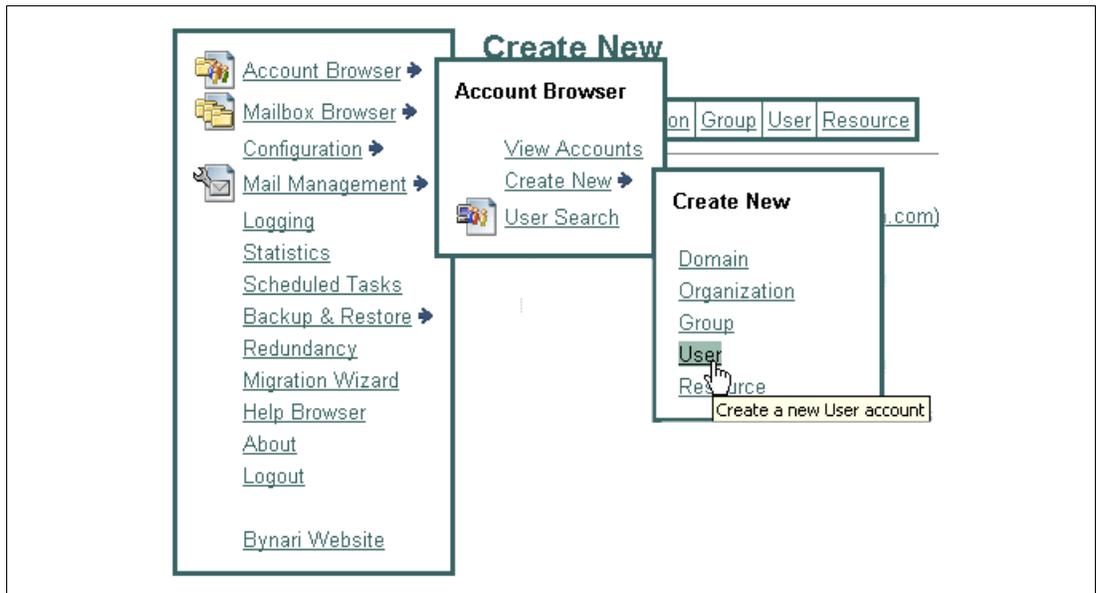

Figure 3-17   Main menu: Selecting to create a new user account

2. An organization can have three types of entries: users, groups, or resources. A *group* is a collection of multiple users. As such, an organization is a collection of groups. This concept is implemented in the LDAP server as illustrated in Figure 3-18 for DN. When you create a user, you can either make that user directly belong to an organization (for example, "IBM") or into a group (for example, "ITSO" group in "IBM" organization).

Select the DN. Then enter all the information about your worker. Under the General section, type the user ID, password, and any personal identification information. At this time, you can define the user ID to use the mail server.

Figure 3-18   Creating new User: LDAP search

3. Enter the personal information of your user. This includes the phone number, address, Post Office Box, and so on. You can also enter information about the user's status in the company, such as the type of employee, title, office location, etc. and so on as shown in Figure 3-19.

Figure 3-19   Creating new User: Parameters

4. Decide on the quota of the user's mail box. If you don't set the quota, the system wide quota is used. Also determine whether you want to create the mailbox folder to this user. If you want to create a mailbox, select the **Create mailbox?** option as shown in Figure 3-20.

Click the **Create** button.

Figure 3-20   Creating new User: Mail folder and quota

The changes are reflected in the LDAP tree as shown in Figure 3-21. Now you see an additional entry of "cn", which stands for common name. LDAP server uses this to distinguish the users. Bynari uses "cn" also to distinguish resources.

*Figure 3-21   Creating new User: LDAP tree*

3.4.5 Creating a resource

You can create resource accounts to represent a *resource*, such as a conference room or video projector. Insight Server manages this account automatically to accept or to decline a meeting request. To create a new resource, follow these steps:

1. From the main menu, select **Account Browser-> Create New-> Resource**. Or you can click the **Resource** option on the navigator bar as shown in Figure 3-22.

Figure 3-22   Main menu: Selecting to create a new resource

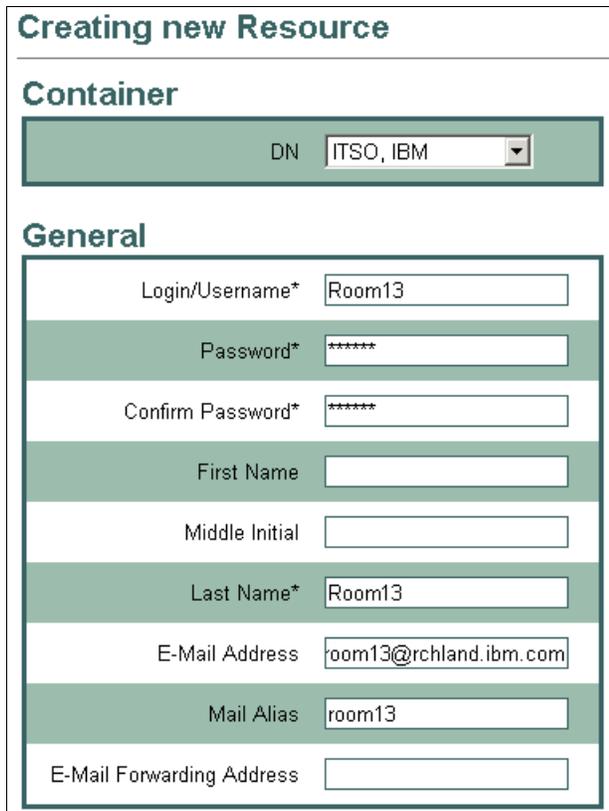2. Any resource that belongs to an organization or group is reflected under the DN options. This is the same as for users. Select a DN option as shown in Figure 3-23.
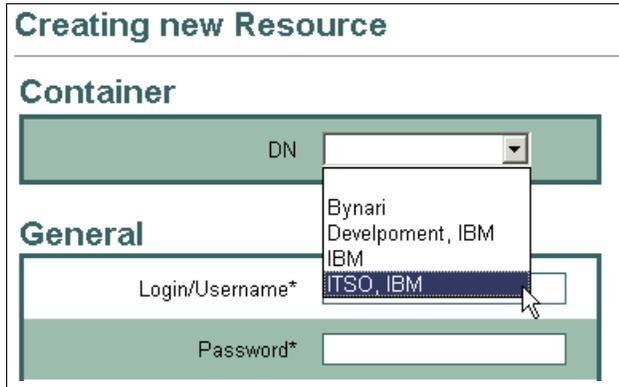
Figure 3-23   Creating new Resource: LDAP search

3. Resources also have a user ID, password, etc. for using the mail service of Insight Server. Enter the information for the resource as shown in Figure 3-24.

Figure 3-24   Creating new Resource: Parameters

4. Set the quota and the creation of the mailbox folder as shown in Figure 3-25. Click the **Create** button.
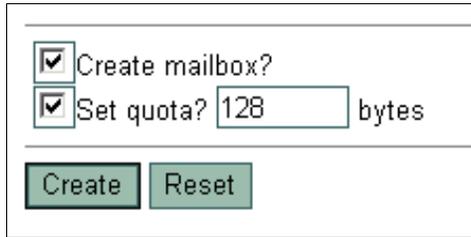
Figure 3-25 Creating new Resource: Mail folder and quota

The changes appear in the LDAP tree. Figure 3-26 shows a typical server configuration.
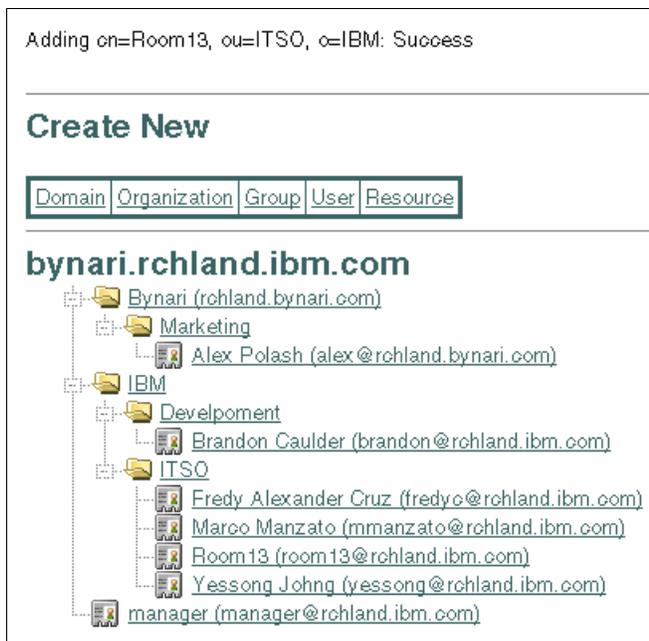
Figure 3-26 Creating new Resource: LDAP tree

3.5 Creating distribution lists

Distribution lists are system aliases that represent a group of e-mail addresses. A system alias can be setup for a distribution list. This alias name is not displayed in the LDAP client listing in Outlook.

To create a distribution list, follow these steps:

1. Select **Mail Management-> System Aliases** as shown in Figure 3-27.
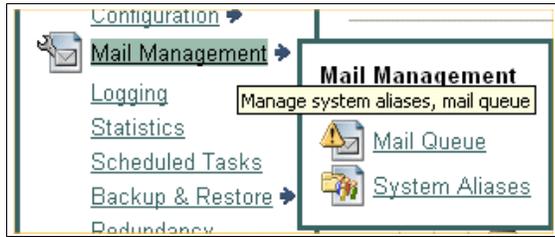
Figure 3-27   Creating an alias for a distribution list

2. Assign an alias name for a distribution list, for example, `building1`. Enter mail addresses to belong to that distribution list. Then, click **Add**. See Figure 3-28.

Figure 3-28   Adding distribution list entries

3.6 Working with the Mailbox Browser

The Mailbox Browser is a utility to work with folders. As the manager user, you can work with the systems folder. You can also create system-wide shared folders at this point. With Mailbox Browser, you can view or create folders as shown in Figure 3-29.
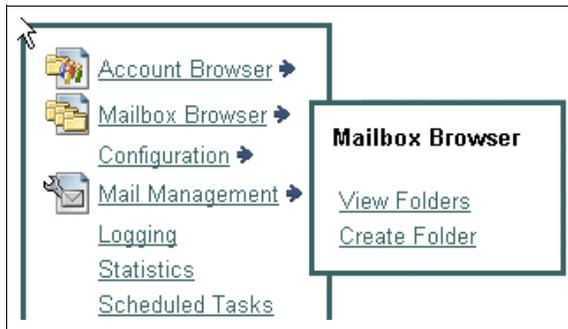
Figure 3-29   Mailbox Browser utilities

If you want to share information, you can make these folders sharable. The example in Figure 3-30 shows how to create a folder for tasks. In this scenario, the project leader assigns the tasks to each developer. A developer can follow these tasks every time they open Microsoft Outlook or Web Client.

Figure 3-30   Creating a folder

As shown in Figure 3-30, the types of folders match the types of folders that Microsoft Outlook has. From here, you can create all the utility folders that Microsoft Outlook provides.

When you click the Create button, a new page appears (Figure 3-31). This page manages the quota and privileges of the folder. This example leaves open access for all users and defines the manager user as the owner of the folder.

Figure 3-31   Editing a folder

Reselect the Mailbox Browser link to see the page as shown in Figure 3-32. If you select the new folder, Bynari Project, the editing folder window displays the Editing folder page (Figure 3-31) again.

Figure 3-32   Viewing folders

4

Configuring Insight Connector and Insight AddressBook

The Bynari Insight Connector is a plug-in for Microsoft Outlook that installs as an Exchange client extension. The Insight Connector uses the Internet Message Access Protocol (IMAP) to create, download, synchronize, and set permissions on all mail folders. The configuration that follows allows you to use Outlook as the client interface to the IMAP server.

Notes:

► You must install Outlook in Corporate Workgroup mode for all features to perform correctly.

► Before installing Insight Connector, back up any existing PST files. We recommend that you set up Insight Connector using a brand new PST file.

► The Bynari Insight Connector installs only on systems where the user has administrative rights. You can change the user rights to install the Bynari Insight Connector and then reset them to the original rights.

4.1 Installing Insight Connector

These steps explain how to manually install and configure the Insight Connector for Outlook. If you want to use an unattended installation, contact Bynari Technical Support for assistance.

1. Verify that Outlook is installed with all of the latest service packs and critical updates. If it is not installed, install it at this time.

> **Note:** If Outlook *was not* installed previously, we recommend that you do *not* create any user profiles at this time. If Outlook *was* installed previously and a user profile was created, we recommend that you create a completely new profile (importing mail from previous profiles is covered in the chapter for migration).

2. Ensure that Outlook and any other unnecessary programs are closed before you install Insight Connector.

3. Locate and launch the executable file for the Insight Connector installer package as shown in Figure 4-1.
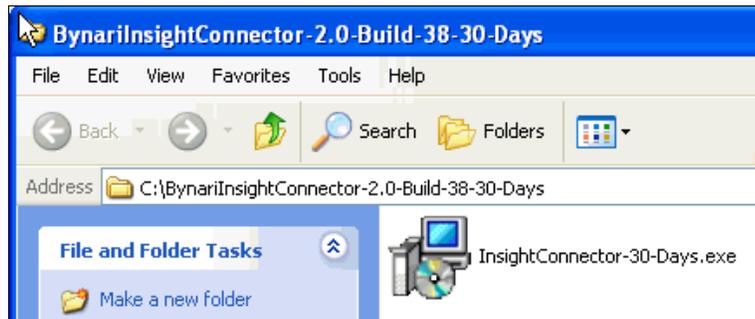
Figure 4-1   Insight Connector installer package

4. InstallShield initializes and prepares for setup. Then the Welcome window opens. Click **Next**.

5. The next window displays the license agreement. Read the license agreement and click **Yes** if you agree to it. Then click **Next**.

6. The next window asks you for the location of where you want the program files to reside. If you desire a specific location, change it. If you want to change the location and you are not sure of where to place the program, contact your Network Administrator. If not, click **Next**.

7. The Folder Synchronization Options panel (Figure 4-2) opens. Select the type of synchronization you want (details for each option are explained in 4.3, "Insight Connector synchronization settings" on page 71). We recommend that you choose **Every time I select the folder**. Then click **Next**.
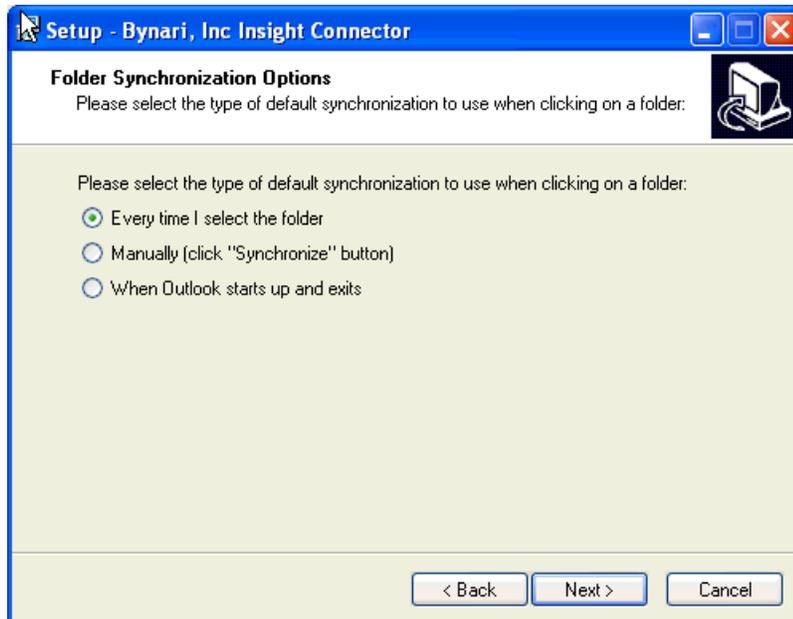
Figure 4-2   Selecting the synchronization type

8. The next window allows you to choose whether you want the Insight Connector toolbar visible or hidden. We recommend that you keep the toolbar *visible*. If you keep the toolbar visible, you can always hide it again. For normal operations and how to change more settings, see 4.2.3, "Setting Insight Connector advanced options and preferences" on page 69. Click **Next**.

9. On the last window, click **Finish**.

The installation portion of the connector is now complete. Now you need to configure Outlook to take advantage of the Insight Connector.

4.2 Configuring Outlook and Insight Connector

This section explains how to configure Outlook to best use Insight Connector. To create a profile, Outlook uses a wizard for most of the steps. Only one window at a time is active. Microsoft developed the creation of profiles this way so that users won't lose their place in the process.

Complete the steps in the following sections for your specific version of Outlook.

For Outlook 98 and 2000

Follow these steps:

1. Right-click the **Outlook** icon on the desktop and select **Properties**. The Microsoft Mail Properties window opens.

2. From the Properties window, select **Show profiles**.

3. On the Mail Profiles window, click **Add**. The Microsoft Outlook Setup wizard opens.

4. On the Setup wizard (Figure 4-3), select **Manually configure information service** and click **Next**.
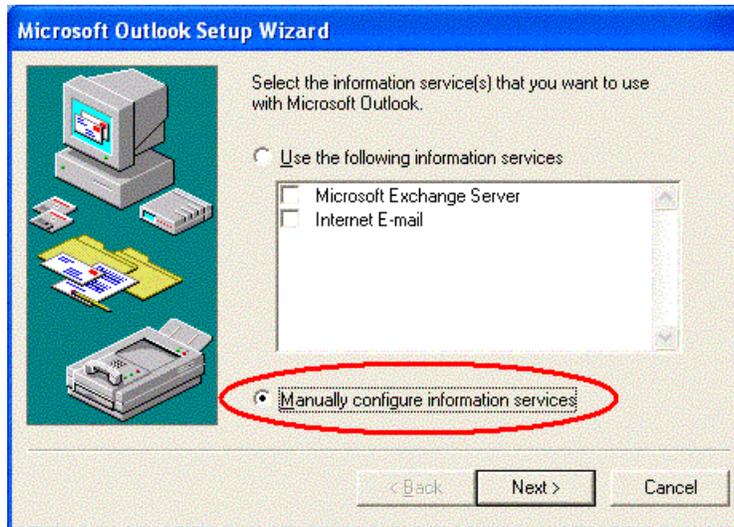
Figure 4-3   Adding a mail profile

5. On the next window, name the profile. This name is displayed later in the Profile window. If the computer is to be used by more than one user, the name is displayed in the Log in As User window when Outlook opens. Click **Next**.

6. The Properties window opens indicating the profile name. For example, if you set the profile name in the previous step to "David", this window specify "David Properties". Click **Add** to add a service.

7. On the Add Service to Profile (Figure 4-4) window, select **Internet E-Mail** and click **OK**.

Figure 4-4   Adding the mail service

8. The Mail Account Properties window (Figure 4-5) opens. Follow these steps:

    a. Click the **General** tab.

        i.   Enter the name for the mail account. The description of what can go there is provided at the top of the page. This is a guideline. Anything will work that can be used to tell the user the purpose of this profile.

        ii. In the User information section, enter the user's name, organization, e-mail address, and reply address. The e-mail address and reply addresses are required.

    b. Click the **Servers** tab. Enter the appropriate information for your e-mail server as shown in Figure 4-5. The items that are circled are required.
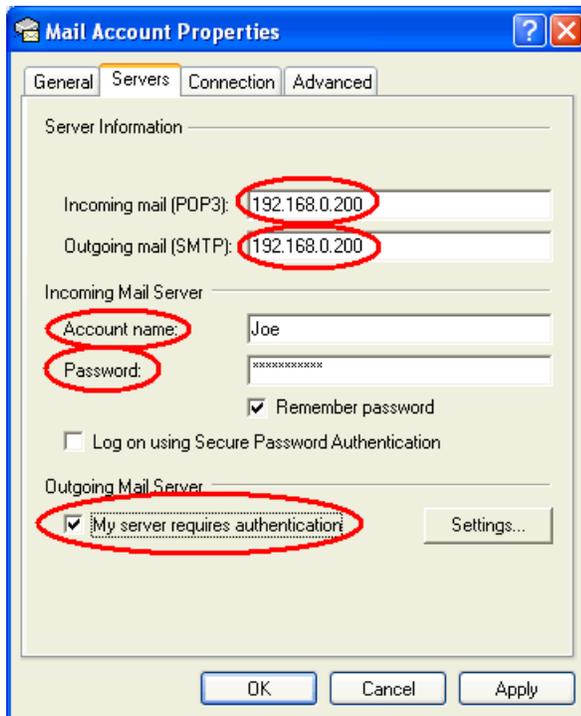
Figure 4-5   Specifying the server settings

> **Note:** We recommend that you set Incoming mail to *None*. You can switch it back after configuration if you still want to use the Post Office Protocol 3 (POP3) features. If POP3 is used for retrieval, duplicate mail may be created if the PST file becomes corrupt or if the option to leave mail on the server is not selected. The account name is the user ID on the server with the password. Select **My server requires Authentication** to allow the user to relay and select settings.

   c. On the Account Properties window, click the **Advanced** tab.

   d. On the Advanced page (Figure 4-6), if POP3 is enabled (using an address in the incoming servers for POP3), select the **Leave a copy of messages on server** option. We recommend that you select this option even if POP3 is disabled. Click **OK**.
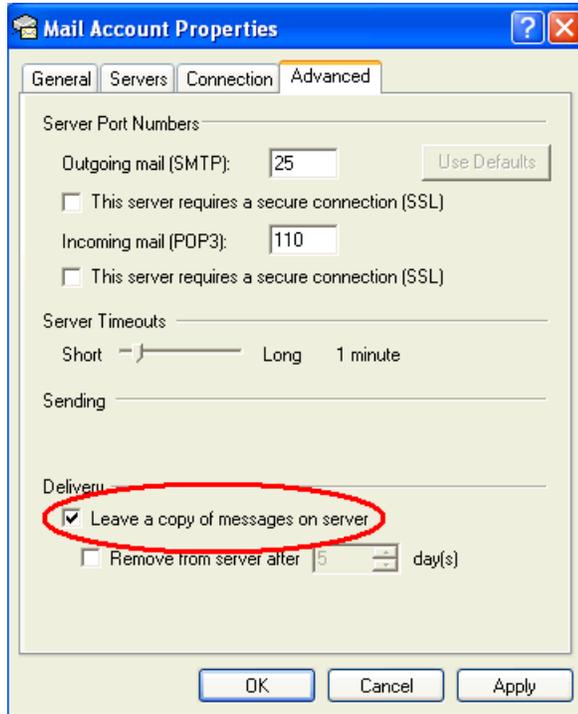
Figure 4-6   Selecting the option to leave a copy on the server

> **Note:** Do not close the Profile Properties window since you now need to add a delivery point for incoming mail.

9. On the Profile's Properties window, click **Add**.

10. On the Add Service to Profile window (Figure 4-7), select **Personal Folders** and click **OK**.

Figure 4-7   Adding a service to profile

11. The Create/Open Personal Folders file box opens. Name the file as appropriate. We recommend that you name the PST file the same as the user name. Click **Open**.

12. The Create Microsoft Personal Folders window opens. Assign it an appropriate name. This is the name of the folder as it appears inside Outlook. Naming the folder the same as the PST file helps in troubleshooting and diagnostics.

Click **OK**. The PST file is automatically assigned to the mail profile created in the previous steps.

13. On the Profile Properties window, click **OK**.

14. On the Mail Setup wizard window, click **Finish**.

15. On the Profiles window, click **Close**.

Next you configure the Insight Connector when you open Outlook for the first time. Now go to 4.2.1, "Configuring Insight Connector" on page 68, skipping the following section "For Outlook XP".

For Outlook XP

Follow these steps:

1. Open the Microsoft Mail Properties window. Right-click the **Outlook icon** on the desktop and select **Properties**.

2. On the Mail Setup window, select **Show profiles**.

3. On the Mail Profiles window, click **Add**.

4. On the next window, type a name to describe the profile you want to add. Click **OK**.

5. The E-mail Accounts window opens (Figure 4-8). Select **Add a new e-mail account**, and click **Next**.

Figure 4-8   Settings for the accounts Internet e-mail server

> **Note:** We recommend that you set Incoming mail (POP3) to *none*. You can switch it back after the configuration if you still want to use the POP3 features. However, there is the possibility of duplicate mail using POP3 with the connector. The account name is the user ID on the server with the password. Select **My server requires authentication** to allow the user to relay and select settings.

6. On the next window, select **POP3** from the list of choices. Click **Next**.

7. On the Internet E-mail Settings window, enter the appropriate information. You must include a name, e-mail address, incoming mail address (POP3), outgoing mail address (SMTP), user name, and password.

8. Click **Next** on the next window.

9. On the last window, click **Finish**. The data file (PST) is automatically created for the user in Outlook XP.

10. The Mail Profiles window now shows the name of the profile that is created. Click **OK** to close the window.

Next you configure Insight Connector when you open Outlook for the first time. This is explained in the following section.

4.2.1 Configuring Insight Connector

If Bynari Insight Connector was installed for the first time, a wizard starts when you open Outlook. Follow these steps to configure Insight Connector:

1. On the first window, click **Next**.

2. On the next window, follow these steps:

   a. Enter the required information:

      • **Host Name**: Enter the IP address of the server.
      • **Port**: Use the default 143 or 993 if Secure Sockets Layer (SSL) is selected.
      • **Login**: Enter the login name or user name on the server.
      • **Password**: Type the user password for the specific user.

   b. To determine if your information was correct, select **Ping Server**.

   c. If the message is correct, you receive the `Successfully connected` ... message (Figure 4-9). Click **OK**.

Figure 4-9 Successful ping

   d. Click **Next**.

3. On the next window, select **Use an existing .PST file**. Choose the newly created PST file. Click **Next**.

4. A list of instructions appears. It explains how to modify the Outlook settings. Click **Next**. This is discussed in following section.

5. On the last window, click **Finish**. This completes the configuration of the Insight Connector.

4.2.2 Configuring Insight Connector after upgrading from a previous version

To configure Insight Connector after you upgrade from a previous version and to use an existing installation of Outlook with a PST file, follow these steps:

1. Open Outlook and continue the configuration of the Bynari Insight Connector.

2. With V2.0 and later, the wizard automatically starts. Click **Cancel** on this first window.

3. On the next window, you are asked if you want to run the wizard the next time you open Outlook. Select the **Yes** or **No** answer.

If you are upgrading from an earlier version of the Connector, at this point, you are finished. Outlook opens normally. However, if this is an existing installation of Outlook and this is the first time that Insight Connector is installed, follow these steps:

1. From the Insight Connector toolbar, select **IMAP Mailboxes** (Figure 4-10).

Figure 4-10   Selecting the IMAP Mailboxes button

2. The Insight Connector Options window opens. Click **Add**.

   a. Select the **Use existing PST file** option. Highlight the desired PST file displayed. It should have the name that was given when the PST file was created. Click **OK**.

   b. Select **Options**. Enter the server IP address or name of the server, the user ID, and password.

   c. Select **Ping Server** to check for connectivity. It returns the `Connected Successfully` message.

   d. On the Insight Connector Options window, click **OK**.

After you enter the information, you can synchronize the Outlook folders to the server.

4.2.3 Setting Insight Connector advanced options and preferences

Connector V2.0 is not synchronized in the INBOX folder by default if you are using POP3. You must select this option in the Insight Connector configuration. All incoming message are left in the inbox and remain on the server if, on the Internet E-mail Service page, select the Leave messages on server option.

IMAP implementation (recommended)

The following steps explain how you can use the inbox as a standard IMAP folder.

From within Outlook

Follow these steps:

1. Ensure that the POP3 address for the Insight Connector is set to **None**. You set this option when you set up the mail profile. See 4.2, "Configuring Outlook and Insight Connector" on page 63.

2. Select the **Inbox** folder and, on the Insight Connector toolbar, click the **Folder** button.

3. The Insight Connector Folder Option window opens. Select **Synchronize INBOX folder**. Click **OK**.

For Outlook XP

Follow these steps:

1. From Outlook XP, select **Tools-> Options**.

2. Click the **Mail Setup** tab. Click the **Send/Receive** button.

3. In the Send/Receive Groups window, click **Edit**.

4. On the Send/Receive Settings - All Accounts window (Figure 4-11), deselect the **Receive mail items** option. Insight Connector automatically synchronizes your mailbox for you. Click **OK**.
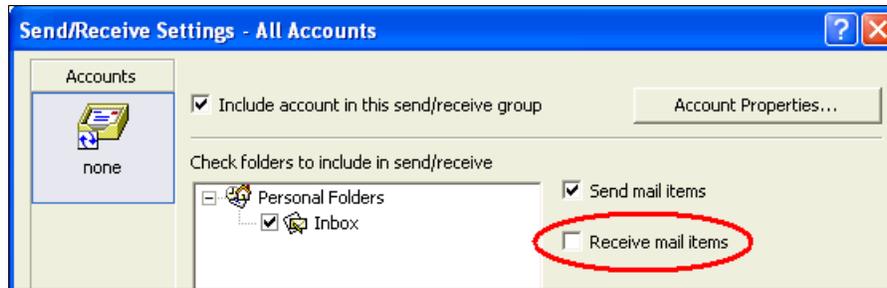
Figure 4-11   Deselecting the Receive mail items option

5. On the Send/Receive Groups window, click **Close**.

6. On the Options window, click **OK**.

For Outlook 98/2000

Follow these steps:

1. From Outlook 98/2000, select **Tools-> Options-> Internet e-mail**.

2. On the Internet e-mail page, deselect the **Check my local network connection(s) for new mail every "X" minutes** option.

3. On the Options window, click **OK**.

POP3 implementation (optional)

All inbox e-mail is managed by POP3. The remaining folders are IMAP folders. For example, synchronization occurs on the server.

You can select the inbox to send/receive automatically, based on a set schedule, as explained in the following sections.

For Outlook XP

Follow these steps:

1. From Outlook XP, select **Tools-> Options**.

2. On the Options window, follow these steps:

3. Click the **Mail Setup** tab.

4. On the Mail Setup page, click the **Send/Receive** button.

5. On the Send/Receive Groups window, the settings are completely determined by the user. Set the options as desired. For more help on what each option does, see the Outlook Help files.

6. In the Mail Account Properties window, click the **Server** tab.

7. On the Server page, replace NONE with the actual POP3 server (usually the same as the SMTP server).

8. On the Options window, click **OK**.

In Outlook 98/2000

In Outlook 98/2000, follow these steps:

1. Select **Tools-> Options-> Internet e-mail**.

2. On the Internet e-mail page, select the **Check my local network connection(s) for new mail every "X" minutes** option.

3. On the Options window, click **OK**.

4.3 Insight Connector synchronization settings

Insight Connector has several options for synchronizing folders. As explained earlier in this chapter, the inbox, by default, is not synchronized. All other mail folders are regular IMAP folders and are synchronized normally.

When synchronization occurs between Outlook and the IMAP server, a comparison is made between the Unique Identifier (UID) of each object. The IMAP server uses a Unique Identifier (UID) on all messages that it stores. Conversely, Outlook uses a Global Unique Identifier (GUID) for messages. Both are stored internally in the message. The Insight Connector keeps a table of all the GUIDs and IMAP UIDs to compare Outlook and IMAP.

The Outlook object GUID never changes, even when the message is modified. However, the IMAP server always assigns a new UID when you modify a message. This is because the IMAP server doesn't allow you to overwrite the original message. In turn, the connector has to upload the modified object and delete the old message from the IMAP server.

Here is a scenario:

1. User1 has a task in a folder, as does User2 (same original task).

2. User2 modifies the task, but User1 does not.

3. User2's folder is synchronized. User2's Outlook uploads the modified message, gets a new IMAP UID (10), and deletes the previous IMAP UID (5).

4. User1 synchronizes their folder. The connector detects that IMAP UID 5 does not exist anymore and deletes the local task. The Connector detects a new IMAP UID (10) and downloads the new message. This creates a new task in Outlook (respectively a new GUID is created).

The entire synchronization depends on which user synchronizes first, thus updating the UID. The GUID is never modified. It is a unique number that is generated by Outlook.

Understanding that an IMAP UID only progresses to a higher number, you can see that if User1 modifies a task one second after User2 but User1 never synchronized the folder, User1 can lose their changes.

In addition, Insight Connector also looks at the time stamp of when that message was modified. The time is stored in the same table that was mentioned earlier. If the connector detects that a message's last modification time was changed (meaning the time is greater than the time that was stored in the table), the connector uploads the message to the server and removes the old message from the IMAP folder. This works the same way that the UID does.

To synchronize a folder, follow these steps:

1. Select the folder you want to synchronize. On the Insight Connector toolbar (Figure 4-12), click the **Folder** button.

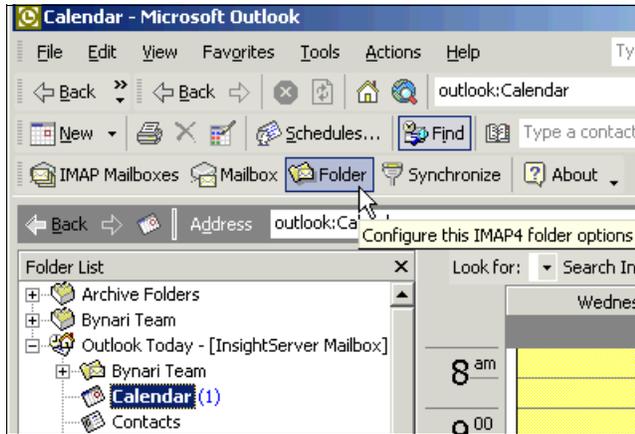*Figure 4-12   Folder button on the Connector toolbar*

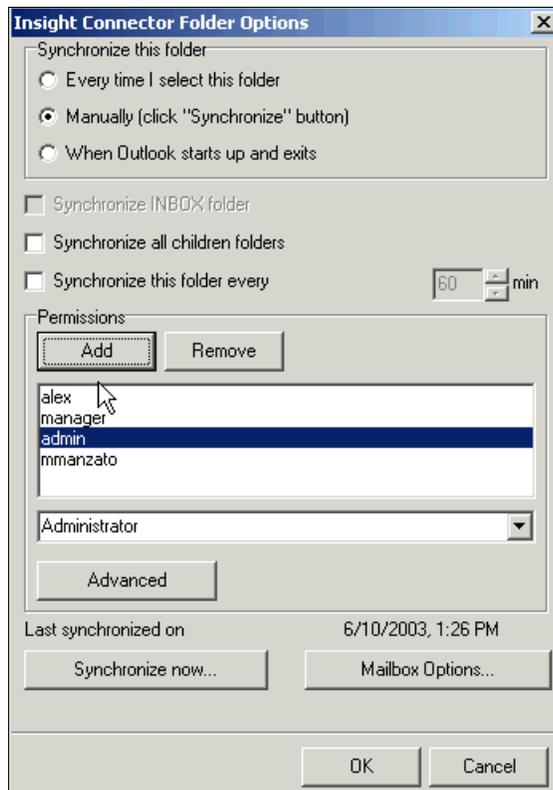2. The Insight Connector Folder Options window (Figure 4-13) opens.

Figure 4-13   Insight Connector Folder Options

The options at the top specify *when* you want synchronization to occur for that folder. Choose from the following options:

– **Every time I select this folder**: This means that the folder synchronizes every time you click the folder.

– **Manually** (the recommended option): The folder synchronizes only when you click the Synchronize button on the Connector toolbar.

– **When Outlook starts up and exits**: The folder synchronizes only when you open and close Outlook.

We recommend that you synchronize folders manually to restrict heavy network traffic due to constant folder synchronization.

The next set of options specify *what* or *how* you want to synchronize. You can choose to:

Note: You can select the Synchronize INBOX folder only if you highlight the INBOX folder *before* you click the Folder button. Otherwise, this option is not available.

– **Synchronize all children folders**: This is a root folder with subfolders, as shown in Figure 4-14. This option synchronizes *all* the folders underneath the root folder automatically when the root folder is synched.
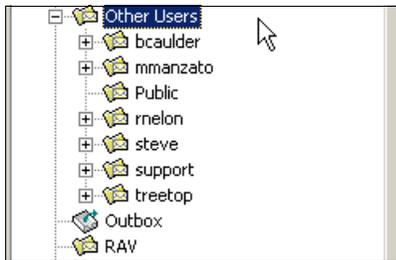
Figure 4-14   Root folder with subfolders

– **Synchronize this folder every X minutes**: This option sets the interval for how often this folder synchronizes (Figure 4-15). The minimum is one minute. We recommend that you set the most important folders to synchronize every 1 to 5 minutes, such as the INBOX (if you are using IMAP retrieval for INBOX).
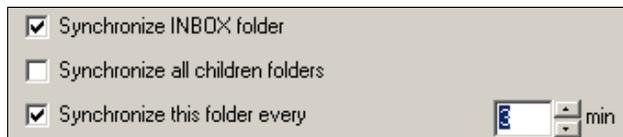
Figure 4-15   Sync options

3. Click **OK** to apply your settings. At any time, you can manually click the **Synchronize** button on the Insight Connector toolbar to perform a manual synchronization for a folder (Figure 4-16).

Figure 4-16   Synchronize button on Connector toolbar

4.4 Insight Connector folder sharing

Insight Connector allows Outlook users to share personal or public folders with other users that reside on the same mail server. Folders can include, calendars, inbox, tasks, contacts, etc. To share folders with users on the same mail server, follow these steps:

1. With Outlook open, select **View-> Folder List** as shown in Figure 4-17.
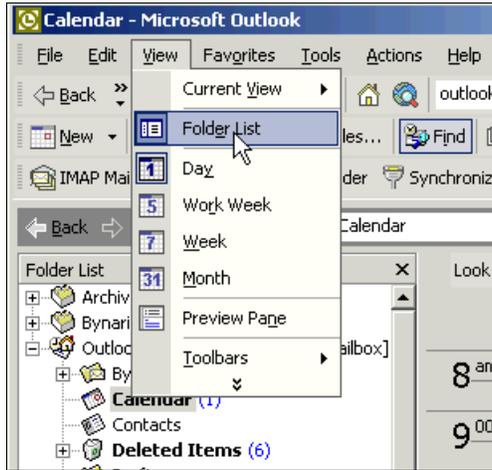
Figure 4-17   Selecting Folder List

2. Highlight the folder you want to share. Then on the Insight Connector toolbar, click the **Folder** button. See Figure 4-18.
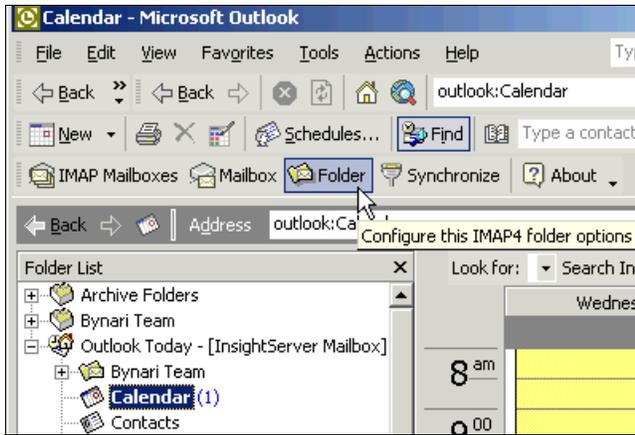
Figure 4-18   Selecting Folder for the folder properties

3. The Insight Connector Folder Options window (Figure 4-19) opens. Click **Add** to add users.
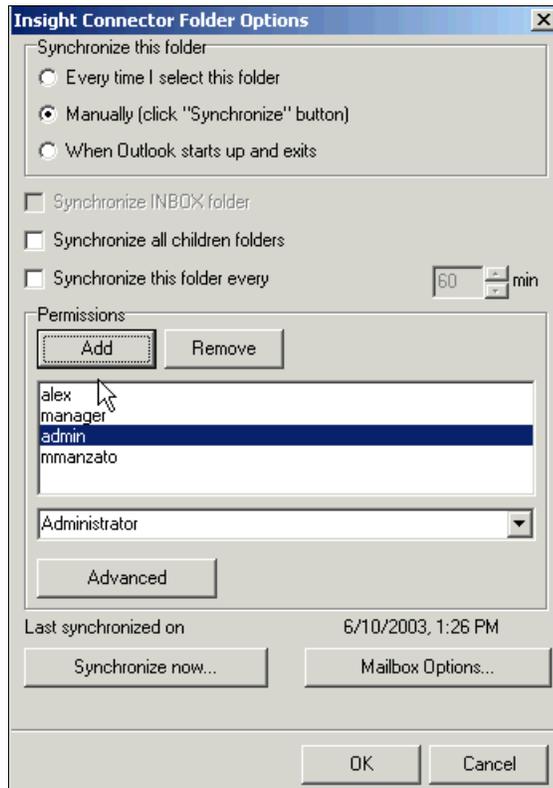
Figure 4-19   Insight Connector Folder Options window

4. Enter the user name, using the e-mail ID on the Bynari server. You can find the user ID on the user Administration window of the Bynari server (Figure 4-20).

5. Select the permissions for the person that will view this folder as shown in Figure 4-20. There are four standard predefined folder option permissions that you can set up:

   – **Administrator**: Full rights
   – **Guest**: Lookup, Read, Set Seen Flag rights
   – **Power User**: All rights, except for Administrator
   – **User**: All rights, except for Create, Delete, and Administrator
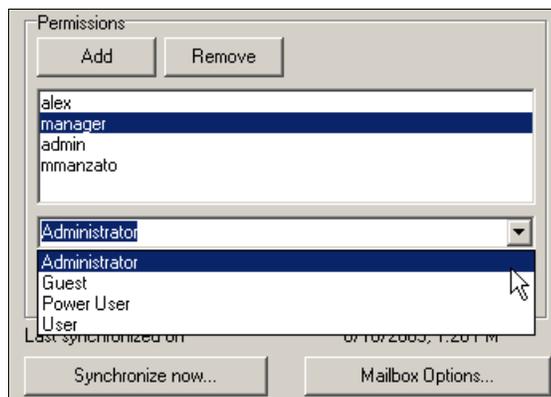
Figure 4-20   Predefined folder permissions

6. You can also set up customized folder permissions. In the Insight Connector Folder Options window (Figure 4-19), click the **Advanced** button.

7. On the Permissions window (Figure 4-21), you find all the access control list (ACL) permissions. Select each permission you want to assign to a user. Click **OK**.

Figure 4-21   Advanced Permission options

Table 4-1 lists all the permissions that are available.

> **Note:** If a user does not have "delete" rights, and tries to edit a shared file or contact, that user receives an error message upon synchronization. The message indicates that they do not have delete rights to that folder. This is because, when you edit a document or contact, you must delete the old file before uploading the new one. This is an Request for Comments (RFC) ACL standard.

Table 4-1   Access control list permissions

Permissions	Description
Lookup	The user may see that the mailbox exists.
Read	The user may read the mailbox. The user may select the mailbox, fetch data, perform searches, and copy messages from the mailbox.
Insert	The user may insert new messages into the mailbox.
Set Seen Flag	Keep per-user seen state. The Seen and Recent flags are preserved for the user.
Write	The user may modify flags and keywords other than Seen and Deleted (which are controlled by other sets of rights).
Post	The user may send mail to the submission address for the mailbox. This right differs from the Insert right. The delivery system inserts trace information into submitted messages.
Create	The user may create new submailboxes of the mailbox, or delete or rename the current mailbox.
Delete	The user may store the Deleted flag and perform expunges.
Administrator	The user may change the ACL on the mailbox.

8. Repeat steps one through seven as necessary for other users that you to want to share a folder.

9. On the Insight Connector Folder Options window, click **OK** to accept the newly defined permissions.

10. Synchronize the folder to the server to ensure the permissions are applied on the server. Highlight the root folder. On the Insight Connector toolbar, click **Synchronize**.

Viewing shared folders

After a root synchronization is done, all the folders appear as shown in Figure 4-22. The folders that are shared by another user are listed under the root folder, which is Other Users in this case.
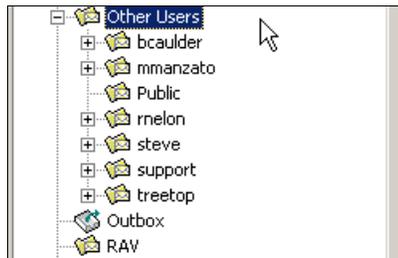
Figure 4-22   Other Users shared folder list

In Outlook, public folders that are created on the Insight Server appear under Shared Folders as shown in Figure 4-23. You can learn about the options and configuration settings for public folders in Chapter 7, "Administration and operations of Insight Server" on page 105.

Figure 4-23   Shared Folders public folder list

4.5 Insight Connector free/busy configuration

Outlook allows users to share free/busy information from their calendars with other users on their mail server. With the Microsoft Office Internet Free/Busy Service, users can publish their free/busy times to a shared Internet location. Members of the service can view each other's free/busy information. They can also help control which members have access to their information.

To configure free/busy, follow these steps:

1. From Insight Connector, select **Tools-> Options-> Calendar Options**.

2. Under Advanced options (Figure 4-24), deselect the **When sending meeting requests over the Internet, use iCalendar format** option. Click the **Free/Busy Options** button.
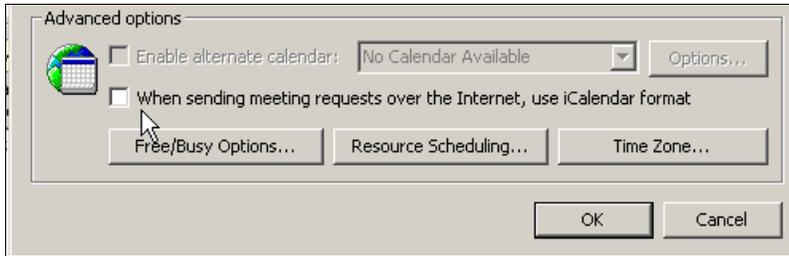
Figure 4-24   Deselecting the When sending meeting requests... option

3. On the Free/Busy Options window (Figure 4-25), specify the following information:

   – **Options**: Here you can choose how often and for how long free/busy information is valid. We recommend that you specify two months of free/busy information and one to five minute automatic updates.

   – **Publish at my location**: Enter the File Transfer Protocol (FTP) address and the user name and password.

   – **Search location**: Enter the Uniform Resource Locator (URL) for the free/busy times of the shared Internet location.

   Click **OK** to apply the settings.
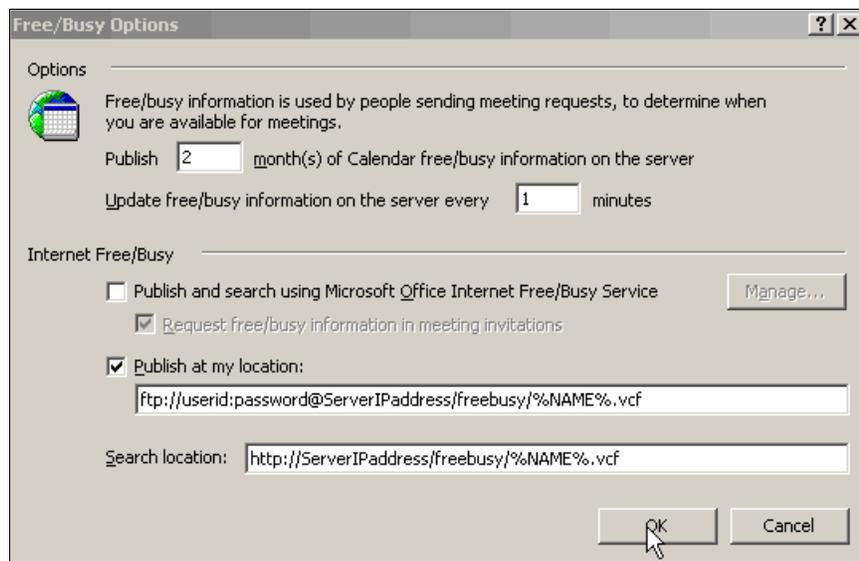
Figure 4-25   Free/Busy Options window

4.6 Registering Insight Connector

Insight Connector should automatically register when entering the license key as described in 4.1, "Installing Insight Connector" on page 62. If the product fails to register, manual validation may be required.

Normally the license key is passed via the Internet, through port 80, to the Bynari Key Validation Servers. The key is then checked. If it is valid, the product is registered. To check for connectivity, you can ping:

http://register.bynari.net

Note: If the workstation resides behind a firewall and port 80 is blocked, you can configure port 3080 for automatic registration and validation of the license key.

To manually validate a license key, follow these steps:

1. Open the License Key window. This window opens during installation. Or you can click **About->Register**.

2. On the License Key window (Figure 4-26), ensure that your license key is entered in the Enter your Insight Connector license key field.

3. Click the **Key Support** button.
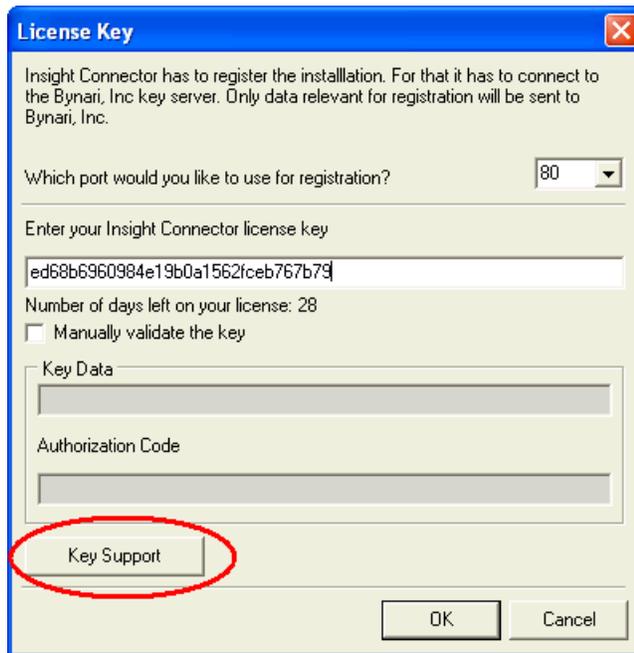
Figure 4-26   Key Support button

4. Copy and paste the contents of the window that opens into an e-mail and send it to Bynari, Inc. Support at `mailto:support@bynari.net`.

5. A Bynari representative will contact you as soon as possible. They provide validation information for you to enter into the Key Data and Authorization Code fields on the License Key window (Figure 4-27).

6. Click **OK** to finish the registration process.
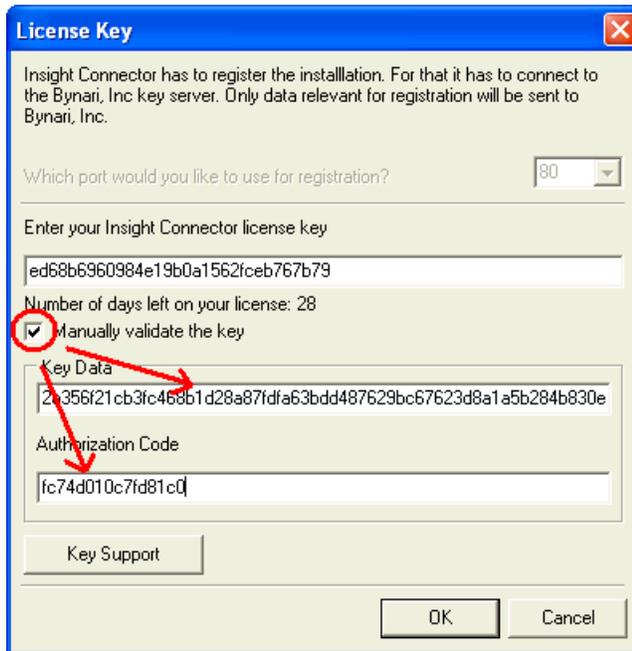
Figure 4-27   Manually entering the information

4.7 Insight Connector toolbar and buttons

This section describes the functionality of the Insight Connector buttons on the toolbar. We recommend that you keep the toolbar visible at all times. During installation of the Insight Connector, the user is asked whether they want the toolbar hidden or visible. If the toolbar is hidden, you can make it visible again by right clicking anywhere on the Outlook toolbar and choosing **Insight Connector**. To hide the toolbar, reverse the process.

The Insight Connector toolbar and buttons include:

► **IMAP Mailboxes button**: This button allows the user to add or change settings to connect to an IMAP server and a corresponding mailbox. Clicking this button takes the user to a window that provides the instructions for Outlook on how to communicate with a server and where to store mail, after it is retrieved.

  – The main window shows the number of mailboxes for which Insight Connector is set up.

  – The Options button sets the address, port, and account information for authentication to the IMAP server. It also has a button to test connectivity labeled "Ping Server".

  – The Add button allows the user to set up a local destination delivery point, known as a PST file.

  – The Delete button removes any mailboxes setup for Insight Connector.

  – The PST file field below these buttons shows the location and name of the PST file for the selected mailbox in the window above them.

► **Mailbox button**: This button performs the same function as the Options button under IMAP mailboxes.

► **Folder button**: This button allows the user to change settings on a folder when it is highlighted. Clicking this button takes the user to the Insight Connector Folder Options page in the Inbox Properties window (Figure 4-28) that offers the following options:

– The Synchronize this folder section allows the following choices:

• *Every time I select this folder*: Whenever the folder is chosen, it performs synchronization with the server.

• *Manually click*: This option only synchronizes the folder when you click the synchronization button.

• *When Outlook starts and exits*: This forces synchronization upon startup and shutdown of Outlook.

– The next section has three check boxes:

• *Synchronize INBOX folder*: The first check box is only available when the INBOX folder is selected. This allows the inbox to be synchronized when POP3 settings are used.

• *Synchronize all children folders*: If the folder has subfolders, they are synchronized at the same time.

• *Synchronize this folder every*: This option lets you set an interval in minutes of how often the folder is synchronized automatically.

– The next section covers permissions. Refer to the Insight Connector documentation for settings and a description of the ACL.

– The Last synchronized on section shows when the folder was last synchronized. It also has a Synchronize now button and an Options button.
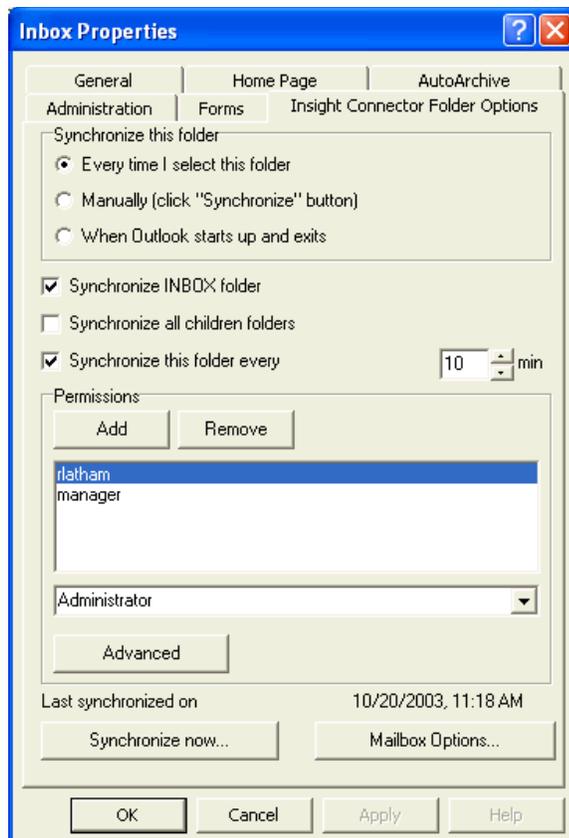

Figure 4-28   Insight Connector Folder Options page in the Inbox Properties window

▶ **The Synchronize button**: When you click this button, it synchronizes the chosen folder immediately.

4.8 Unattended installation

To install the Insight Connector with minimal user intervention, the administrator (or manager) can modify a setup.ini file that answers most configuration settings. To perform an unattended installation, follow these steps:

1. Download the Insight Connector zip file and setup.ini file from the Bynari, Inc. Web site at:

   http://www.bynari.net

2. Unzip the files. Place the Install package and setup.ini file into a new folder.

3. Modify the setup.ini file for a user as explained in the following section.

4. The manager must copy the Insight Connector package and the setup.ini file to the root directory.

5. After the files are in place, install Insight Connector:

   a. From your desktop, click **Start-> Run**.

   b. Type the following line:

      ```
      InsightConnectorRetail.exe /y c:\setup.ini /silent
      ```

   c. Allow the installation process to run.

   The installation is now complete.

After the Insight Connector package finishes, you can open Outlook.

4.8.1 Modifying the setup.ini file

A sample of the setup.ini file follows. You *must* modify those items that are highlighted in bold. Each user must have a setup.ini file specifically created for their instance of Outlook. An unattended installation only works for a fresh installation of the Insight Connector. You must set up manually subsequent profiles or users through Outlook. See 4.8.2, "Description of changes for the setup.ini file" on page 83, for an explanation of the modifications in the setup.ini file.

```
[General]
CompanyName=Company Name.
InstallRootPath=c:\Program Files\Bynari, Inc

[Misc]
Verbose=No
LogFile=

[Profile]
NewProfile=Yes
DefaultProfile=Yes
ProfileName=John
ProfilePassword=password
PSTDisplayName= Personal Folders
PSTFile=c:\connector\john.pst

[Insight Connector]
Key= eb30878cacb97a5b84ce4e367f9fdd8f
InstallPath=c:\Program Files\Bynari, Inc\InsightConnector
```

```
ServerName=192.168.3.195
ServerPort=143
UseSSL=No
UserName=john
Password=password
StorePassword=Yes
SyncInbox=Yes
HideToolbar=No
;Valid options: WhenFolderSelected, Manually, StartStop
;         WhenFolderSelected = Every time I select this folder (DEFAULT)
;         Manually = Click "Synchronize" button
;         StartStop = When Outlook starts up and exists
DefaultFolderSyncFlag=WhenFolderSelected

[FreeBusy]
ReadURL=http://mail.bynari.net/freebusy/%NAME%.vcf
WriteURL=ftp://mail.bynari.net/freebusy/%NAME%.vcf

[POP3]
DisplayName=John's Acct
AccountName=John's POP Account
EmailAddress=john@brds2.com
Server=none
Port=110
UseSSL=No
UserName=john
UserPassword=password
StorePassword=Yes

[SMTP]
AccountName=John's Acct
EmailAddress=john@brds2.com
Server=192.168.3.195
Port=25
UseSSL=No
Organization=Company Name
ReplyToAddress=john@brds2.com
UserName=john
Password=password
```

4.8.2 Description of changes for the setup.ini file

The following sections explain the changes for the setup.ini file.

[General]

► `CompanyName=Company Name`

This can be any word value. We recommend that you use the company name.

► `InstallRootPath=c:\Program Files\Bynari, Inc`

This is the location that the automatic installer uses for installs. Bynari recommends that you use the default location, but you may change it for administrator purposes.

► `[Misc]`

`Verbose=No`

If set to Yes, the user is prompted for all changes.

- ► `LogFile=`

  If set to Yes, a log file is generated for the installation and stored in the install root path location specified above.

- ► `[Profile]`

  `NewProfile=Yes`

  If this is set to "No", a new profile is not created. However, you must still designate a profile (see the following item).

- ► `DefaultProfile=Yes`

  If this is set to "No", this profile is not the default profile used when opening Outlook.

- ► `ProfileName=John`

  This is the name of the profile to be used or created.

- ► `ProfilePassword=password`

  This is the password for the profile to be used.

- ► `PSTDisplayName=Personal Folders`

  This is the display name for the PST file under the profile and within Outlook.

- ► `PSTFile=c:\connector\john.pst`

  This is the name and location that the unattended installation creates the PST file. Bynari recommends that you use the default location, although you may change it for administrator purposes. You must modify the name of the PST file for each user.

[Insight Connector]

- ► `Key= eb30878cacb97a5b84ce4e367f9fdd8f`

  This is the valid license key obtained from Bynari, Inc.

- ► `InstallPath=c:\Program Files\Bynari, Inc\InsightConnector`

  This is the location in which Insight Connector installs. Bynari recommends that you use the default location, but you may change it for administrator purposes.

- ► `ServerName=192.168.3.195`

  You can use either an IP address or the fully qualified name of the computer, such as *mail.company.com*.

- ► `ServerPort=143`

  This is the port for connecting to the mail server. If you are going to use SSL, then set this to 993.

- ► `UseSSL=No`

  If you are using port 993 in the preceding line, then this value should be `Yes`.

- ► `UserName=john`

  This is the account name used for authentication.

- ► `Password=password`

  This is the password of the account name used for authentication.

- ► `StorePassword=Yes`

  If this value is set to No, then every time the mailbox synchronizes, the user is prompted for a password.

- ► `SyncInbox=Yes`

  If set to No, the Inbox is not set to synchronize.

- ► `HideToolbar=No`

  If set to Yes, the toolbar for the Insight Connector within Outlook is hidden.

- ► `DefaultFolderSyncFlag=WhenFolderSelected`

  This items sets the default to *on* when folders should be synchronized. The valid options are:

  - **WhenFolderSelected**: Every time I select this folder (default)
  - **Manually**: Click the **Synchronize** button
  - **StartStop**: When Outlook starts and exits

  The options are better under "DefaultFolderSyncFlag" than on top.

[FreeBusy]

`ReadURL=http://mail.company.com/freebusy/%NAME%.vcf`
`WriteURL=ftp://mail. company.com/freebusy/%NAME%.vcf`

Set the server name of where free/busy information will be published.

[POP3]

- ► `DisplayName=John's Acct`

  This sets the value for the display name of the protocol used in the profile.

- ► `AccountName=John's POP Account`

  This sets the value for the display name for the account settings under the protocol properties for the profile.

- ► `EmailAddress=john@brds2.com`

  This item sets the value for what e-mail address to use.

- ► `Server=none`

  You can use either an IP address or the fully qualified name of the computer, such as *mail.company.com.* We recommend that you set this to NONE to prevent the user from being prompted for a user name/password each time the server is checked. It also prevents the likelihood of duplicate e-mails.

- ► `Port=110`

  This item sets the port for checking mail.

- ► `UseSSL=No`

  If you are using SSL, set this item to `Yes` and modify the preceding line with the appropriate port.

- ► `UserName=john`

  This is the account name used for authentication.

- ► `UserPassword=password`

  This is the password of the account name used for authentication.

- ► `StorePassword=Yes`

  If this value is set to No, then every time the mailbox synchronizes, the user is prompted for a password.

[SMTP]

► `AccountName=John's Acct`

This sets the value for the display name of the protocol used in the profile.

► `EmailAddress=john@brds2.com`

This sets what e-mail address to use.

► `Server=192.168.3.195`

You can use either an IP address or the fully qualified name of the computer, such as mail.company.com.

► `Port=25`

This item sets the port for mail to be sent on.

► `UseSSL=No`

If using SSL, set this item to `Yes` and change the preceding line to the appropriate port.

► `Organization=Company Name`

This sets the value of the company name used.

► `ReplyToAddress=john@brds2.com`

This sets the reply to address used for outgoing e-mail.

► `UserName=john`

This is the account name used for authentication.

► `Password=password`

This is the password of the account name used for authentication.

4.9 Installing and configuring Insight AddressBook

Insight AddressBook has the look and feel of the Global Address List with the "Show all" feature. With a 50,000 directory user base, Insight AddressBook provides instantaneous lookups when using the "Check name" feature in a new mail message. After Outlook loads Insight AddressBook, queries take less than three seconds for the entire directory. When using department lists, lookups are instantaneous.

4.9.1 Installing Insight AddressBook

This configuration assumes that you have installed a working Bynari Insight Server. Follow these steps to install Insight AddressBook:

1. Go to the Bynari Web site at:

   http://www.bynari.net

   a. From the home page, click **Products-> Insight AddressBook**.
   b. Click **Download Demo** on the left panel.
   c. Click the **BynariInsightAddressBook.zip** file to download it.
   d. Extract the contents using an unzip or decompress utility, such as WinZip.

2. Ensure Outlook and all current services packs and critical updates are installed.

3. Ensure that the client already has an account activated on Insight Server.

4. Disable any antivirus software *and* any services associated with it. Ensure that you close Outlook before you install Insight AddressBook.

5. Locate and launch the executable file for the Insight AddressBook installer package.

6. After the InstallShield initializes and prepares for setup, the Welcome window opens. Click **Next** on this window.

7. On the next window, read the license agreement. If you agree, click **Yes**.

8. The next window asks you for the location of where you want program files to reside, if you desire a specific location, change it. If not, click **Next**.

9. Insight AddressBook is now installed. Enter the license key when prompted, and click **Next**.

10. On the AddressBook Installation window, click **Finish**.

4.9.2 Configuring Insight AddressBook

After you install Insight AddressBook, complete these steps to configure it:

1. Open Outlook.

2. The Bynari LDAP Address Book window (Figure 4-29) opens. Complete the following steps on the General page:

   a. In the LDAP Server box, enter the Insight Server address.

   b. Select the **Send messages to recipients from this server in Rich Text Format** option.

   c. It is not required to add a user name or password.
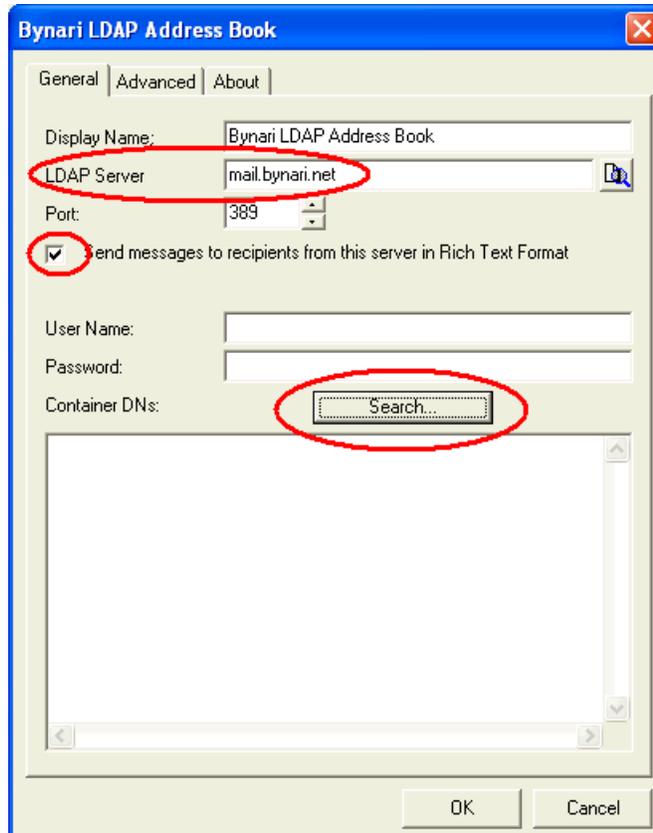
   d. Click the **Search** button.

Figure 4-29   Bynari LDAP Address Book window

3. On the LDAP Containers window (Figure 4-30), follow these steps:

    a. Click the **+** (plus sign) button to expand the **Server Root** container (DN=). It lists all your organizations that are present on that server.

    b. Click the **+** (plus sign) button next to the organizations (o=). It displays any of the groups (ou=) that were created. Here you can select to which groups the user should have access.

    c. To allow a user to have full access, simply select that organization (o=).

    d. Click **OK** when you are done. You then return to the main LDAP AddressBook window. Now you should see all chosen containers.
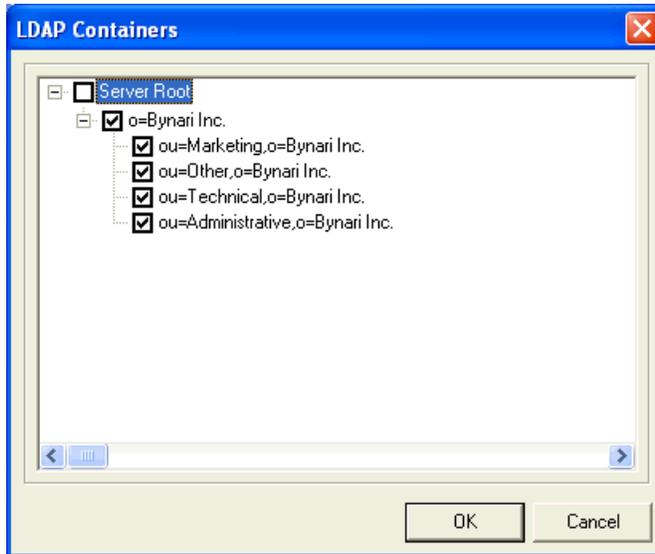

Figure 4-30   LDAP Containers window

4. On the Bynari LDAP Address window, click the **Advanced** tab.

5. On the Advanced page, click the **Detect** button. If it is configured correctly, an information window opens that states that a successful connection was made to the LDAP server.

> **Note:** If you select only the organization, click the **Advanced** tab, and select **Display sub-containers contents of the LDAP containers**. This is an optional step, but it is required for a user to have full access to the LDAP database.

6. Click **OK**. Your LDAP database now displays when you select To from any message that you compose.

If at any point, you need to edit or change your LDAP configuration, click **Tools-> E-mail Accounts-> View or change existing directories or address books**.

4.9.3 Registering Insight AddressBook

Insight AddressBook should automatically register when you enter the license key as explained in 4.1, "Installing Insight Connector" on page 62. If the product fails to register, manual validation may be required.

Normally the license key is passed via the Internet, through port 80, to the Bynari Key Validation Servers. The key is then checked. If it is valid, the product is registered. To check for connectivity, you can ping:

http://register.bynari.net

Note: If the workstation resides behind a firewall and port 80 is blocked, you can configure port 3080 for automatic registration and validation of the license key.

To manually validate a license key, follow these steps:

1. Ensure that the License Key window is opened. For the Insight AddressBook, this normally opens during installation. Or you can open it by clicking **Tools-> E-mail Accounts-> View or change existing directories or address books**. Then click **Next**. Double-click the **Bynari LDAP Server** and click **About-> Register**.

2. On the License Key window (Figure 4-31), ensure that you entered your license key in the Enter your Insight Connector license key field.
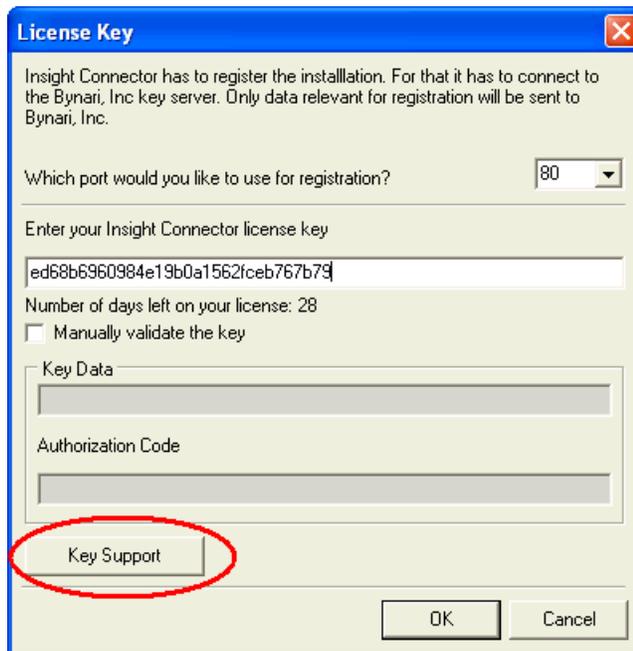
3. Click the **Key Support** button.

Figure 4-31   Key Support button

4. Copy and paste into an e-mail the contents of the window that opens. Then send it to Bynari, Inc. Support at mailto:support@bynari.net.

5. A Bynari representative will contact you as soon as possible and provide validation information to enter into the Key Data and Authorization Code fields (Figure 4-32).

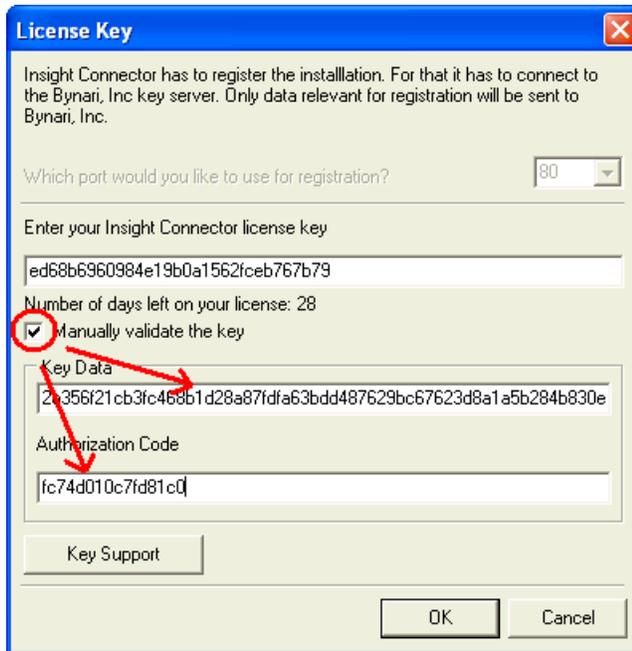6. Click **OK** to finish the registration process.

Figure 4-32   Manually entering the information

5

Insight WebClient

In today's mobile world, instant access to information when you need it is vital to business success. To be competitive with other organizations, your team members must have the ability to access critical data anytime, from anywhere. Whether it be an employee working from home or a sales representative constantly on the run, gaining access to information that traditionally is only available from your office chair has become essential.

For the mobile user, the Web Client is a vital piece to the business process. Through the use of a Web browser and a connection to the Internet, access to e-mail, contacts, and calendar information is a click away.

This chapter discusses Insight WebClient (or simply *Web Client* in this book). This browser-based application reads information from the Internet Message Access Protocol (IMAP) server. Then it displays this information to the user in the form of a Hypertext Markup Language (HTML) page. To reduce the learning curve, the interface of the Web Client is quite similar to common desktop applications, such as Microsoft Outlook. Whether the user is at the office using a desktop application or away from their desk accessing the same data through a Web browser, the experience is quite similar.

5.1 A look at Insight WebClient

Your Insight Server comes pre-configured with IMAP and Apache servers. These two servers are the backbone of the Web Client application. The IMAP server stores the data and the Apache server retrieves and displays the data through the use of Hypertext Preprocessor (PHP) pages. Figure 5-1 shows how the Web Client interfaces with the IMAP server.
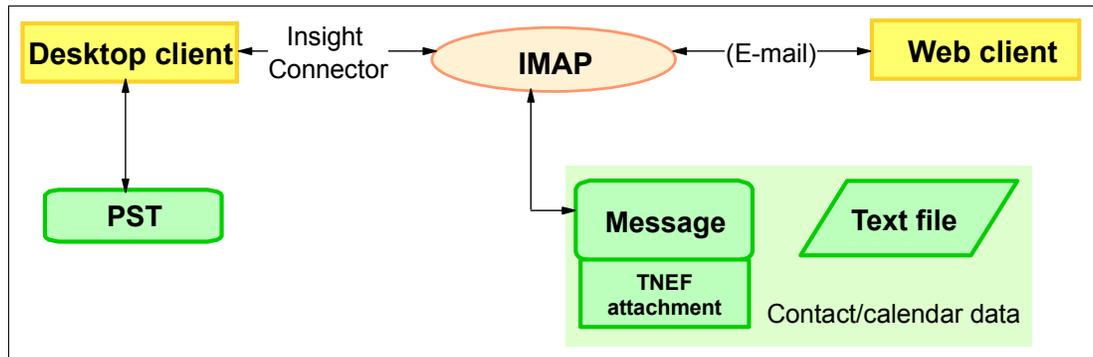

Figure 5-1   Web Client interfacing with the IMAP server

All data is stored on the IMAP server in the form of an e-mail message. Since data is already in the form of an e-mail message, built-in PHP functions are used to access e-mail directly from the IMAP server. This is reflected in Figure 5-1 with the two-sided arrow connecting the IMAP server to the Web Client. Since e-mail data is read directly from the IMAP server, this data is not stored on the Web server.

For non-e-mail data, such as calendar and contact information, the process is more complex. This data is also stored in the form of an e-mail message on the IMAP server, but it is stored as an attachment to the e-mail message. The attachment is a Transport Neutral Encapsulation Format (TNEF) file, which is a proprietary format used by Microsoft for e-mail data. Time constraints in parsing the TNEF file restrict non-e-mail data from being read directly from the IMAP server. Instead, the TNEF file is interpreted and the data is exported to a text file that is stored on the Web server.

A directory structure identical to the folder structure found on the tree (Figure 5-1) is read from the IMAP server and created on the Web server. During the synchronization process, data is transferred from the IMAP server to the Web server. For details about the synchronization process, see 5.5, "Synchronization" on page 94. When the Web Client tree is created, directory types are identified based on the first message in the folder. This record identifies the type of data that is stored in the directory. For example, a contact record is stored in a file named "uid.vcard", where *uid* is the unique identifier for the record. The *vcard* extension tells the Web Client that contact data is stored in the directory. The vcard text file is parsed by a PHP script and the data is displayed to the user in the form of an HTML page.

The process to send data from the Web Client to the IMAP server is similar, only the process is reversed. The Web Client creates a text file, writes data to this file, and stores the file in a directory on the Web server. At the same time, a message and corresponding TNEF attachment are created on the IMAP server. Both servers are updated with the new data instantaneously, so a manual synchronization process is not required.

5.2 Requirements

With browser-based applications, you must enforce requirements to ensure the application functions the same in all environments. Numerous combinations of operating system and browser exist that can force the application to behave differently. As advances are introduced in browser technology, developers are granted access to tools that allow them to create browser-based applications to mirror their desktop counterparts. Unfortunately, these advances in browser technology are not backwards compatible with previous versions, nor are they supported in all browser types. A neutral ground must be found where functionality and browser support can meet.

Every client environment can be unique, so you must set standards to ensure the application functions as intended. The browser that you choose to use must support frames, JavaScript, style sheets, and cookies. If you choose to use a browser that does not support these technologies, the Web Client may not function as intended.

5.3 Setup

The Web Client setup process is relatively simple since a majority of the steps are automated. The setup requires a plug-in on the Insight Server in the form of a Red Hat Package Manager (RPM) package and accessed from the Web Administration Console.

The Apache Web server is already installed, since it is used for the Web Administration Console. The only steps needed for the Web Client setup are to create the directories to store data and script files. These directories include:

► **Bin**: Contains application files
► **Groupware**: Stores all the Web Client PHP scripts
► **Libs**: Stores the Smarty class files
► **Templates**: Stores the Smarty template files that allow the interface to be unique

Note: The data files used to store non-e-mail data are created on the first run of the synchronization process and are not a part of the setup process.

5.4 Security

When critical data is stored in a location that is accessible to the outside world, security is of utmost importance. The Web Client takes security quite seriously. It has integrated measures to ensure that data is accessible to authenticated personnel only.

All pages within the Web Client application have an embedded security check. If a user tries to access a page within the Web Client and they are authenticated, the login page is displayed (Figure 5-2). The user supplies a user name and password. This information is authenticated against user data stored on the IMAP server. If a match is found, a user session is created and the user is granted access to the corresponding account.

Figure 5-2   Bynari login

Precautions have been taken to prevent malicious hackers from accessing the Web server and gaining access to the critical data that is stored there. As mentioned earlier, data is stored on the IMAP server and on disk. Access to data on

the IMAP server is protected via the IMAP login along with the IMAP server's security measures. Access to the data on disk is only available via the Web Client. The PHP code that runs the Web Client validates all user input to make sure the user is not trying to trick the Web Client into revealing another user's sync directory.

5.5 Synchronization

A direct line of communication between the Web Client and the IMAP server is non-existent, so you must implement a synchronization process. The IMAP server is the "meeting place" for data to and from the Web Client and desktop application. As discussed previously, time constraints prohibit the e-mail client from reading data directly from the IMAP server. The Insight Connector has a process that synchronizes data on the IMAP server, and the Web Client has a similar process in place. As long as the data is synchronized to the IMAP server, both the Web Client and desktop client can access the same data.

The synchronization of data for the Web Client is done in two directions, depending on whether data is written or read. Upon logging into the Web Client, behind the scenes processes ensure that data stored on the IMAP server matches data stored on the Web server. Conversely, as updates are made using the Web Client, data is synchronized back to the IMAP server. The Web Client synchronization process ensures that data stored on the Web server always matches data stored on the IMAP server.

The Web Client reads data from text files that reside on the Web server. As a user authenticates, a comparison is made to ensure that the data on the IMAP server matches data on the Web server. If a difference is found, the script parses the message and creates a corresponding text file on the Web server. A program called *phptnef* is used to convert the TNEF file to a text file. The new text file is placed in the proper directory so the Web Client can access its contents.

Similar to data read by the Web Client, new and updated data is written to text files that reside on the Web server. The Web Client synchronization is conducted behind the scenes for written data as well. Simultaneous actions are made to Web server text files and IMAP messages. For new data, a text file is created on the Web server and the data is written to this file. Before data is sent to the IMAP server, it is parsed from the text file and converted to a compatible format. The text file is passed through the TNEF to PHP script that grabs all text file data and places into a TNEF file. A new message is created and the TNEF file is stored as an attachment to the message on the IMAP server. Updates to data follow the same process. The only difference is that the old IMAP message is deleted from the server.

5.6 Features and functions

The Web Client includes many of the basic features of your desktop application. The major features include e-mail, contacts, calendar, and notes. The Web Client version of these features functions similar to the desktop application that you are using, except that you access content with a Web browser. As new versions of the Web Client are released, more items are added to the feature set, but for now here are a few.

5.6.1 Tree

The tree function allows you to navigate from feature to feature within the Web Client. Figure 5-3 shows an example of a Web Client tree. To navigate to a particular area, the user simply clicks the folder name for the feature that they want to view. The corresponding data for the folder selected is shown in the content frame of the page after a folder, or tree item, is selected. This functionality is similar to how a user navigates through Microsoft Outlook.

Since the tree is customizable, the tree that appears on every Web Client may be unique. Depending on the permissions for the current user, different options and folders are displayed. For example, the current user for Figure 5-3 is granted access to a couple of shared folders, such as junkie, mailbox one, or Other Users. When a user is granted access to shared folders, they can navigate through them as though they were their own.

Preferences

By clicking the Preferences icon, the user can adjust preferences for e-mail, contacts, and calendar. Such settings include the E-mail From Address, Signature, whether the user wants to store deleted and sent e-mail messages, the ability to show HTML e-mail messages, and basic Inbox display features. It is necessary to select the "Save" icon after making any changes in Options.

Logout

Select the Logout icon. The user that is currently logged into the system is logged out and brought to the login window (Figure 5-2).

Figure 5-3   Web Client tree

5.6.2 Inbox

The Inbox feature is used to view and manage incoming e-mail. Such functions as reply, reply all, forward, delete, and move can be used on e-mail messages found in the Inbox. Figure 5-4 shows an example of how the Inbox may appear. The Inbox of the Web Client supports the basic functionality of an e-mail program.

The functions of the Inbox include:

▶ **New Message**: Select the New Message icon to create a new e-mail message.

▶ **Page**: The Page feature allows the user to quickly scroll to the next page of e-mail messages. The amount of e-mail messages displayed per page is determined in the Options feature of the Inbox.

▶ **Delete**: To delete multiple e-mail messages at once, select the check box next to the e-mail messages that are to be deleted. Then select the trash can icon in the top left corner of the Inbox.

> **Note:** The Inbox page is continually refreshed. If you select multiple e-mail messages and the page refreshes before the user clicks the trash can icon, you lose your selected delete items. Go to **Options** to increase or decrease the time in which the Inbox page is refreshed.

▶ **Reply**: Select the e-mail by clicking the subject. You can select the Reply icon from the toolbar above the message list and a Reply window is shown.

► **Reply All**: You can select the e-mail by clicking the subject text. To reply to all recipients of the e-mail, simply click the Reply All icon in the toolbar after you select the e-mail.

► **Forward**: To forward an e-mail, you select the e-mail by clicking the subject text as you do for Reply or Reply All. Then, you click the Forward icon in the toolbar.

► **Print**: If you want to print a copy of the e-mail, you simply select the e-mail and click the Print icon located in the toolbar.

► **View Headers**: To track the path that the e-mail has taken before going to the user, select on the View Headers icon in the frame that displays above the e-mail.
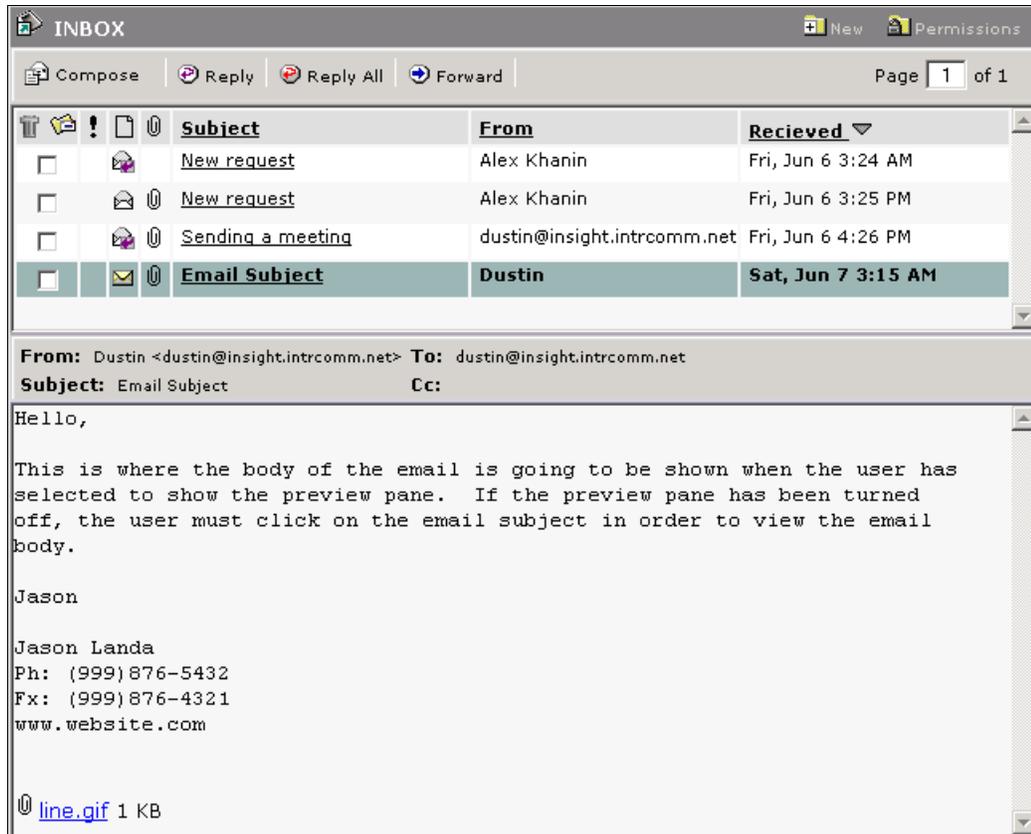
Figure 5-4   E-mail inbox

The user can also compose new e-mail messages and send them to recipients selected from a list of contacts. The recipient list is composed from the contacts list (see 5.6.3, "Contacts" on page 97). To add a recipient to the To, CC, or BCC box, the user simply selects the name from the contact list and then clicks the button for where the recipient should be placed. The e-mail value for the recipient is automatically attached to the name, so there is no need to memorize e-mail addresses. Figure 5-5 shows an example of a new message window.

The top of the new e-mail message allows a user to send, mark the e-mail as important, or save the e-mail in a draft folder located in the tree. See Figure 5-3 for an example of the tree. A user can designate who the e-mail is going to be sent to by selecting names in their contacts list and selecting the To button. Or the user can simply write the e-mail address in the To: field. The same action applies for Cc: and Bcc:. To remove an e-mail recipient selected from the contacts list, select the names in the To: field and click the **<<** button.

You can include attachments to an e-mail. Simply click the **Browse** button at the bottom of the e-mail. Browse for the desired attachment, select the attachment, and then click the **Attach Now** icon.

Figure 5-5   New e-mail message

5.6.3 Contacts

The contacts feature is used to store contact data. In this section, the user can search, add, update, and delete contacts. Multiple folders can be created under the main Contacts folder to help manage the contact list. This is especially helpful if the contact list is quite long. Basic contact data is displayed on the contact list page, as shown in Figure 5-6. By clicking the contact name, you can view extended contact data.
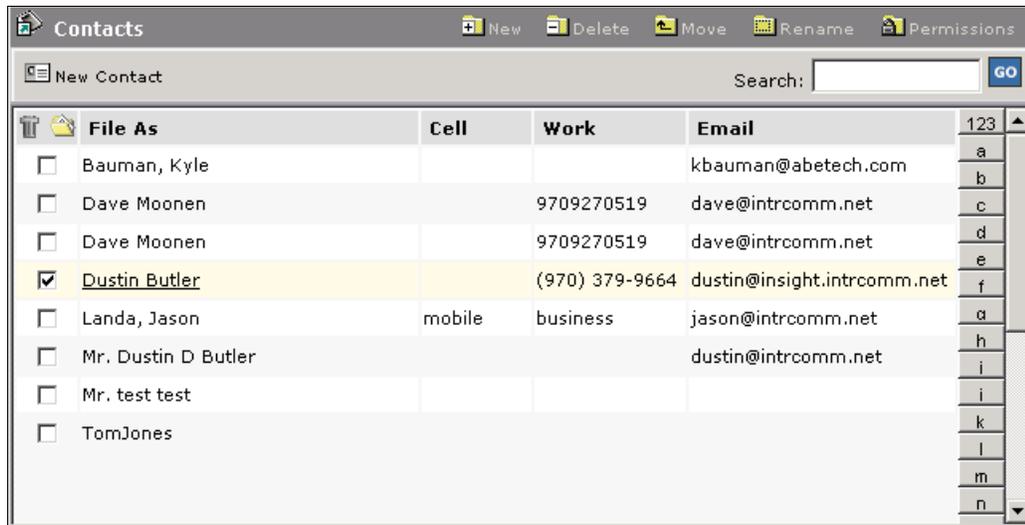
Figure 5-6   Contact list

The functions of Contacts include:

► **New Folder**: The Add New Folder icon allows you to create a new e-mail, contacts, notes, or calendar folder in their desired location. Click Add New Folder. Give the folder a name and select the type of folder to be created.

► **Remove Folder**: You must select the desired folder to be removed from the Tree. Click the **Remove Folder** icon, and a warning message appears. You must click OK to complete the Remove Folder Action.

► **Move Folder**: The Move Folder allows you to move a folder to a different location in the tree.

► **Rename Folder**: You can rename a folder by clicking Rename Folder.

► **Permissions**: Permissions allows account users to give other users access to specific folders in their inbox.

► **New Contact**: Click the New Contact icon. Enter the appropriate information for the contact and click Save.

► **Search**: Search allows you to quickly find a desired contact by entering the name in the search field. You can also search for contacts by selecting a letter or number to the right of the contacts list.

5.6.4 Calendar

The Calendar feature is used to manage appointments and schedule information. Appointments can be found using the Day, Week, Month,. and Year views. Figure 5-7 shows an example of the day view. To see details or update appointments, you click the appointment name. You are then taken to the edit appointment window where you can make changes to the appointment. Such options as reminders, recurring appointments, and meeting requests are also supported in the Web Client.
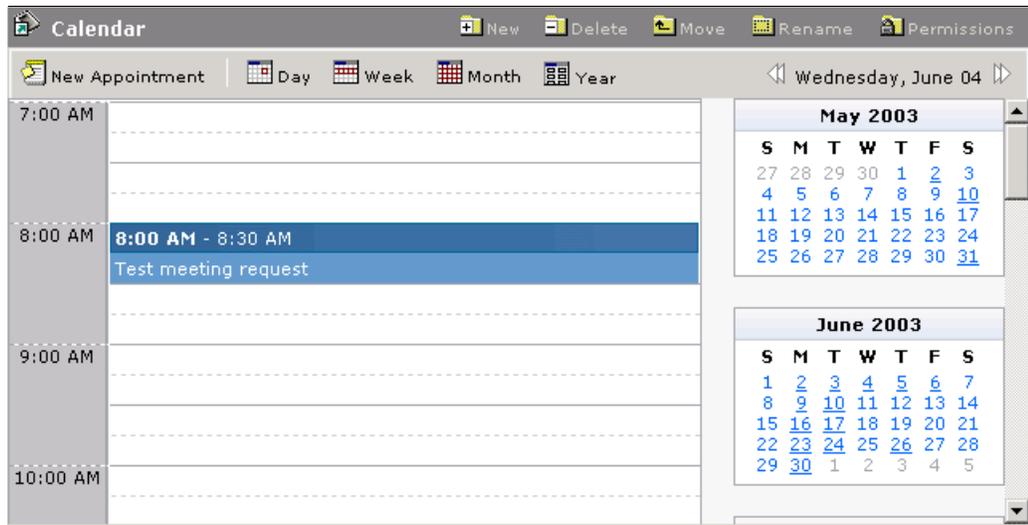
Figure 5-7   Day view of Calendar

Calendar supports the following features:

▶ **New Appointment**: Click the New Appointment icon to create a new setup item.

▶ **Day**: Click this icon to see the day view (see Figure 5-7). This view shows all appointments that occur on the date on the right side of the setup options bar. You can easily navigate to previous or future days by clicking the arrows surrounding this current date.

▶ **Week**: Click the Week icon to view your setup items in a weekly view. The weekly view shows all events that occur during the selected week, with each day of the week as a column header.

▶ **Month**: Click the Month icon to view the setup in monthly view. The monthly view shows the current month and allows you to click items that are assigned to each day within that month.

▶ **Year**: Click this icon to see all the months in the current year. From this view, you can access all the appointments that are scheduled during the current year.

5.6.5 Notes

The Notes feature provides users a digital sticky note function. When using the Notes feature, you can add, update, and delete small snippets of information. Notice that the functionality of this section is similar to that of Outlook's Note feature. When you first comes to the Notes page, the icon along with a concatenated version of the note is shown in the list. To view the contents of the note, you simply click the Note icon and a sticky note opens. From here, you can read the entire contents of the note, or you can edit or delete the note by clicking the corresponding icon. You can hide yellow sticky note contents by clicking the Close icon in the upper right corner of the note. Figure 5-8 shows an example of a Notes page.

To create a new note, click the **New Note** icon. The Add/Edit Note window opens where you can supply text for a new note.
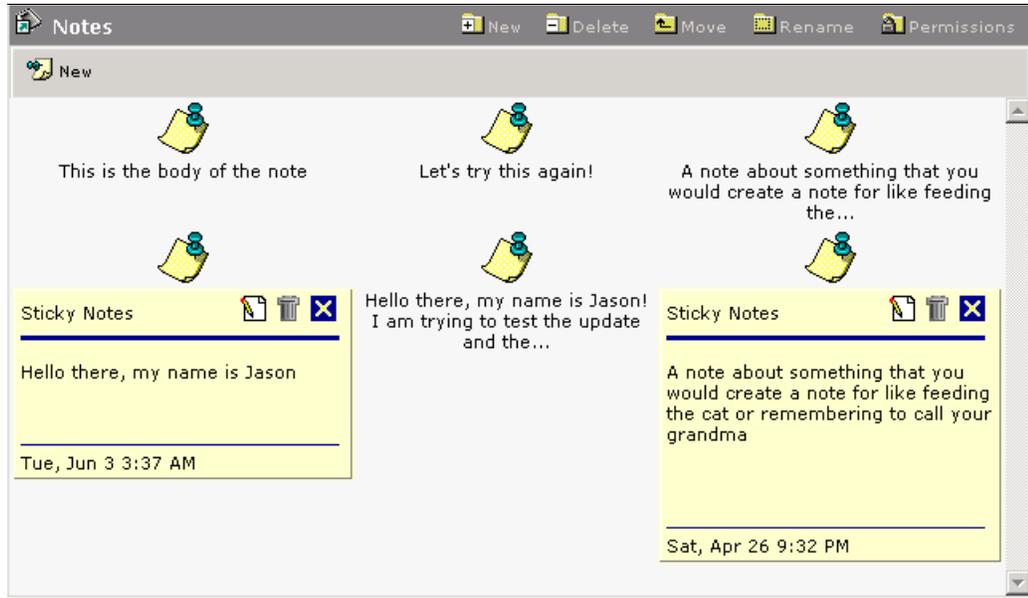
Figure 5-8   Notes

5.7 Technology

The Web Client is based on a technology known as *scripting*. Scripting involves the embedding of PHP script into Hypertext Markup Language (HTML) to create a working application. PHP can best be described as an HTML embedded scripting language. It is responsible for the logic of the application. It is the core programming language behind browser-based applications and is responsible for the presentation or interface of the application.

Taking these technologies a step further, PHP has a built-in add-on called the *Smarty Template Engine* that allows the application logic to be separated from its presentation through the use of templates. For example, the application logic is responsible for such tasks as taking an e-mail from the IMAP server, while the presentation is responsible for the display of this e-mail to the user. Through the use of this technology, multiple presentation layers can be created, allowing organizations to customize the interface design.

Throughout the Web Client application, other Web development technologies are also used. Style sheets are used to maintain a consistent design for the application. Style sheets manage such items as font settings, link colors, table backgrounds, and other interface design issues. By using style sheets, a style setting can be set once and used many times. This allows you to maintain consistency and make design updates relatively easy. Small snippets of Java™ script are also embedded into the application. Java script is a client-side programming language that extends the functionality of browser-based applications. Java script's core competency in this application is to create a client-side feel by eliminating page refreshes and connection-dependent tasks. The Web Client functions whether Java script is enabled or disabled. You will find the experience more pleasing with the Java script additions.

You can learn more about PHP and the Smarty Template Engine on the Web at:

► http://www.php.net
► http://smarty.php.net

6

Migrating mail and user accounts

This chapter explains how to migrate users and their mail from previous versions of Insight Server or from an Exchange Server.

Before you perform any migration or upgrade, we recommend that you have two verified and viable backups of your e-mail and accounts.

Note: If you are migrating from Exchange 5.5, ensure that your administrator or Service Account for Exchange does not have a blank password.

6.1 In place migration from a previous version of Insight Server (no change of hardware)

In some cases, you may want to migrate from one version of Insight Server to another, instead of performing an upgrade. You can do this by following these steps:

1. Stop all services on the previous installation of Insight Server.

2. Install the new version of Insight Server.

> **Note:** Ensure that you register your server and set the Manager password.

3. Navigate to the Migration Wizard page.

4. The Migration Wizard starts now with Step 1, "Specify the existing server type", as shown in Figure 6-1.

Figure 6-1   Specifying the server type

    a. Enter the path to the previous installation of Insight Server:

```
/opt/insight/
```

    b. Click **Next**.

5. Download the script specified in the migration wizard. You can find this on the Web at:

http://www.bynari.net

There is also a set of instructions in the Web Administration Console.

6. Open a terminal session.

7. Log in as `root`.

8. Run the script that was downloaded. Include the path to the previous installation of Insight Server:

```
sh changeports.sh /opt/insight
```

This changes the ports that are used by the services in the previous installation of Insight Server only. Then it starts the services automatically.

9. Exit, but do not close, the terminal session.

10. Return to the Insight Server 4.0 administration interface.

    a. Provide the manager account name and password for the previous installation of Insight Server, and specify the LDAP Search Base Country Code (or region code). For example, you may enter US.

    b. Click **Next**.

11. The migration imports all Lightweight Directory Access Protocol (LDAP) entries and Internet Message Access Protocol (IMAP) mailboxes.

12. A successful operation indicates a status of *Done* at the bottom of the page.

13. Return to the terminal session.

14. Shut down the previous installation of Insight Server by using the following command provided by the script to stop Insight Server:

```
chroot /opt/insight/ /usr/lib/insight/Insight Server stop
```

15. Unmount the /proc located within the previous installation of the Insight Server directory:

```
umount /opt/insight/ /proc
```

It is now safe to remove the previous installation of Insight Server.

6.2 Server to server migration from a previous version of the Insight Server (change of hardware)

This is much less involved than a similar hardware migration where the directory structure doesn't have to be modified or reverted through the running of special scripts.

1. Install the new version of Insight Server.

   Note: Ensure that you register your server and set the Manager password.

2. Navigate to the Migration Wizard page.

3. The Migration Wizard starts with Step 1, "Specify the existing server type" as shown in Figure 6-1.

   a. Enter the path to the Insight Server to be migrated. You may use an IP address as in this example:

      ```
      192.168.3.200
      ```

   b. Click **Next**.

4. On the next page, provide the manager account name and password for previous installation of Insight Server. Specify the LDAP Search Base Country Code (or region code). For example, you may enter US. Click **Next**.

5. The migration wizard imports all LDAP entries and IMAP mailboxes.

A successful operation indicates a status of *Done* at the bottom of the page. It is now safe to remove the previous installation of Insight Server.

6.3 Server-to-server migration from an installation of Exchange Server

This section explains how to migrate from an Exchange server to Insight Server. This includes moving from one set of hardware to a new set of hardware.

1. Install the new version of Insight Server.

   Note: Ensure that you register your server and set the Manager password.

2. Navigate to the Migration Wizard page.

3. The Migration Wizard starts with Step 1, "Specify the existing server type" as shown in Figure 6-1.

    a. Enter the path to the Exchange to be migrated. You may use an IP address as shown in this example:

        192.168.3.200

    b. Click **Next**.

4. On the next page, enter the administrator or service account name and password for previous installation of Insight Server. Specify the LDAP Suffix. Click **Next**.

> **Note:** The Exchange Server must have a password or the Insight Server Migration Wizard will not work. It reset to Step 1 if no password is supplied during this step.

5. The migration wizard imports all LDAP entries and provides instructions on how to use *EXMerge* (available from Microsoft) to import your Exchange mailboxes, which are now in the form of personal folder (PST) files.

    This step creates a PST for each user that is imported using the Insight Server Migration Wizard using ExMerge provided by Microsoft. This is not the same PST that the user may be using on their workstation in Outlook. The user must start with a new PST file after migrating to Insight Server. If the user continues with the previous Outlook PST, there is a possibility of duplicate or lost e-mail.

6. Browse to the location of the ZIP or TAR file with the PST files you want to upload (import) and click **Next**.

A successful operation indicates a status of *Done* at the bottom of the page. It is now safe to remove the previous installation of Exchange Server.

6.4 Outlook characteristics when upgrading from Insight Server 3.5.x to 4.0.x

When using a previous version of Insight Server prior to release 4.0, part of the functionality was to create a new folder as a subfolder of the inbox. With Version 4.0 of Insight Server, this is not possible. This is due to the limitations of the version of Cyrus IMAP that is used.

When migrating from Insight Server Version 3 to Version, users may notice that subfolders that used to reside beneath the inbox are now subfolders of the root folder. This may seem strange to the user at first when they open their inbox and do not see any of their folders. However, when they select the root folder, called Outlook Today, they notice that the new folder synchronizes and that the folders are on the same level as the inbox and that all of their mail is there.

This is scheduled to be changed in future releases of Insight Server since an updated version of Cyrus IMAP will be used.

7

Administration and operations of Insight Server

This chapter explains how to administer the Insight Server through the Web Administration Console. It also explains how to configure services within the operating system so that Insight Server performs its best.

105

7.1 Configuring the Bynari Server services

The Web Administration Console was designed to configure the most commonly used configurations for components used by the server. This helps to avoid command line errors.

7.1.1 Configuring Apache

The Apache server is the Web component of the server for the Web administration interface, such as Web Administration Console, and for the user interface. This server is used for the Insight WebClient. The configuration can be modified to user requirements. The explanation of the configuration parameters can be found by selecting the online help in the Web administration interface.

Navigate to the Apache configuration parameters as shown in Figure 7-1:

1. Log on to the Web Administration Console.
2. Select the **Configuration** option on the main page.
3. Click the **Apache** option.
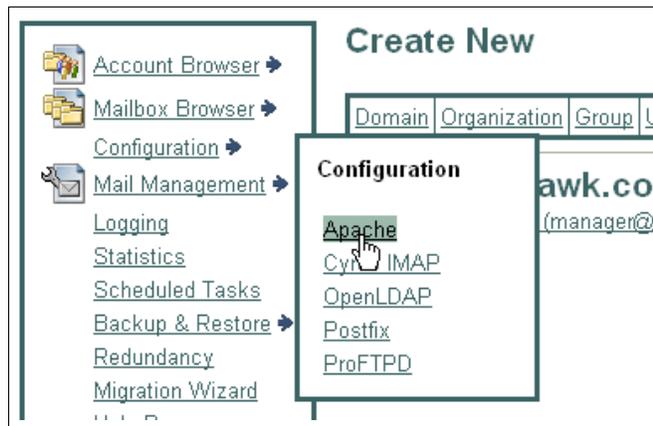
Figure 7-1   Navigating to the Apache Configuration page

Network

The most commonly changed fields are listed later in this section. The Port is the port number that Apache uses to allow connectivity to the Web Administration Console, which is port 80 by default for Web pages. The listen port is used by Apache to listen for connectivity. Both of these settings should be set to the same number. By changing this port, you change the location of accessing the Web Administration Console. If you change the port to 8080, then you must change the listen port to 8080 as well. Then to access the Web Administration Console, you type:

```
http://servername:8080
```

As shown in Figure 7-2, HostnameLookups are disabled (off) so that Apache does not try to look up the server name. It would time out if it can't find the name, which would add delays in displaying the administration interface, such as Web Administration Console.

The remaining options are:

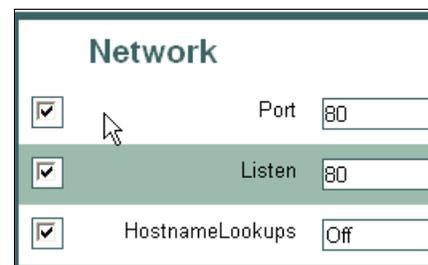▶   **Port**: The Port directive sets the network port on which the server listens.

Figure 7-2   Apache common changes

- ► **Listen**: The Listen directive instructs Apache to listen to more than one IP address or port. By default, it responds to requests on all IP interfaces, but only on the port given by the Port directive.

- ► **HostnameLookups**: The HostnameLookups directive enables Domain Name Server (DNS) lookups so that host names can be logged.

- ► **MinSpareServers**: The MinSpareServers directive sets the desired minimum number of idle child server processes.

- ► **MaxSpareServers**: The MaxSpareServers directive sets the desired maximum number of idle child server processes.

- ► **StartServers**: The StartServers directive sets the number of child server processes created on startup.

- ► **MaxClients**: The MaxClients directive sets the limit on the number of simultaneous requests that can be supported. No more than this number of child server processes are created.

- ► **ServerAdmin**: The ServerAdmin directive sets the e-mail address that the server includes in any error messages it returns to the client.

- ► **ServerSignature**: The ServerSignature directive allows the configuration of a trailing footer line under server-generated documents.

- ► **ErrorDocument**: The ErrorDocument directive specifies a file that is displayed in the event that a user accesses a Web page that has a problem or error.

- ► **Include**: The Include directive allows inclusion of other configuration files from within the server configuration files.

- ► **Log files**: The Apache log files are in /opt/is4/var/log/apache/.

7.1.2 Configuring Cyrus IMAP

Cyrus IMAP is the Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) component of the Insight Server. Cyrus IMAP manages the mail for all the users.

Navigate to the Cyrus IMAP configuration parameters as shown in Figure 7-3:

1. Log on to the Web Administration Console.
2. Click the **Configuration** option on the main page.
3. Click the **Cyrus IMAP** option.
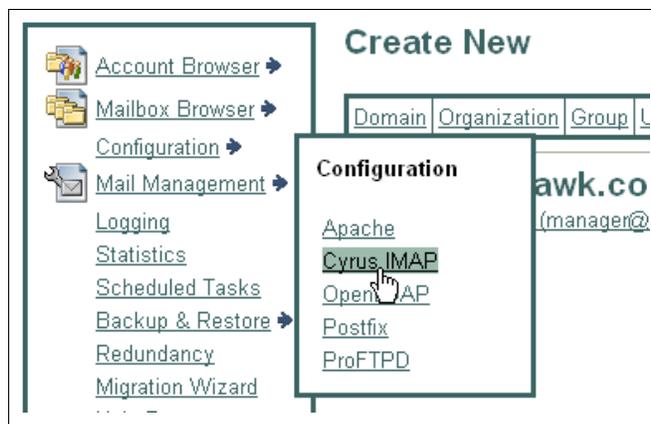
Figure 7-3   Navigating to the Cyrus IMAP configuration page

For an explanation of the configuration parameters, select the online help on the Web Administration Console.

Files/Permissions

The Files/Permissions section (Figure 7-4) configures the appearance of shared folder names as displayed in Outlook.
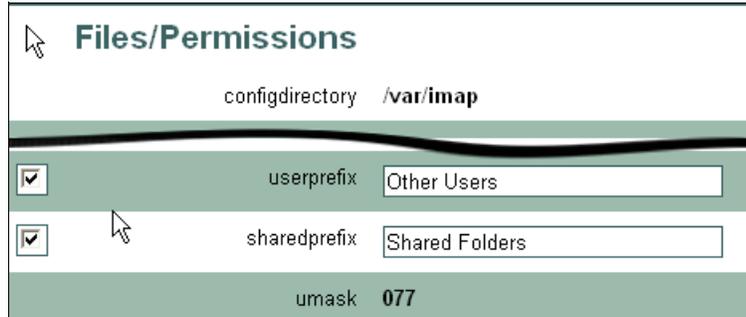

Figure 7-4   Permissions for IMAP

In Outlook, the folder names are listed as shown in Figure 7-5. The options in the Files/Permissions section include:

► **configdirectory**: This is the path name of the IMAP configuration directory. This field is required.

► **partition-default**: This is the partition name used by default for new mailboxes.

► **unixhierarchysep**: Use the UNIX separator character (/) to delimit levels of mailbox hierarchy. The default is to use the netnews separator character (.).

► **altnamespace**: Use the alternate IMAP namespace, where personal folders reside at the same level in the hierarchy as INBOX. This option *only* applies where interaction takes place with the client/user. Currently this is limited to the IMAP (imapd) and sieve scripts (lmtpd).

Figure 7-5   IMAP folder naming

This option does *not* apply to administration tools, such as cyradm (admins *only*), reconstruct, quota, etc. Nor does it affect Local Mail Transfer Protocol (LMTP) delivery of messages directly to mailboxes via plus-addressing.

► **userprefix**: If you are using the alternate IMAP namespace, this is the prefix for the other users' namespace. The hierarchy delimiter is automatically appended.

► **sharedprefix** (Shared Folders): If you are using the alternate IMAP namespace, this is the prefix for the shared namespace. The hierarchy delimiter is automatically appended.

► **umask (077)**: This is the umask value used by various Cyrus IMAP programs.

► **allowsubscribe**: There is no available information for this option.

► **allowanonymouslogin**: This option permits logins by the user anonymous using any password. It also allows use of the SASL ANONYMOUS mechanism.

► **allowplaintext**: This option allows use of the SASL PLAIN mechanism.

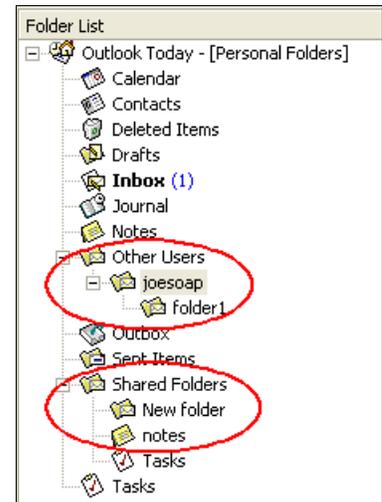► **quotawarn**: This is the percent of quota utilization over which the server generates warnings.

► **timeout**: This option indicates the length of the IMAP server's inactivity autologout timer, in minutes. The minimum value is 30, the default.

► **imapidlepoll**: This is the interval (in seconds) for polling the mailbox for changes while running the IDLE command. This option is used when idled cannot be contacted or when polling is used exclusively. The minimum value is 1. A value of 0 disables polling (and disable IDLE if polling is the only method available).

► **imapidresponse**: If enabled, the server responds to an ID command with a parameter list containing version, vendor, support-url, os, os-version, command, arguments, and environment. Otherwise the server returns NIL.

► **poptimeout**: Set the length of the POP server's inactivity autologout timer, in minutes. The minimum value is 10, the default.

► **popminpoll**: Set the minimum amount of time in minutes that the server forces users to wait between successive POP logins. The default is 0.

► **popexpiretime**: This is the number of days advertised as being the minimum a message may be left on the POP server before it is deleted (via the CAPA command, defined in the POP3 Extension Mechanism, which some clients may support). %22NEVER%22, the default, may be specified with a negative number. The Cyrus POP3 server never deletes mail, regardless of the value of this parameter. However, if a site implements a less liberal policy, it needs to change this parameter accordingly.

► **admins**: This is the list of user IDs with administrative rights. Separate each user ID with a space. Sites using Kerberos authentication may use separate %22admin%22 instances. Note that accounts used by users should not be administrators. Administrative accounts are not recommended for common mail use, such as with Outlook or the Web Client.

► **defaultacl** (anyone lrs): This is the access control list (ACL) placed on a newly-created (non-user) mailbox that does not have a parent mailbox.

► **autocreatequota**: If nonzero, normal users may create their own IMAP accounts by creating the mailbox INBOX. The user's quota is set to the value if it is positive. Otherwise, the user has an unlimited quota.

► **logtimestamps**: Include notations in the protocol *telemetry logs* indicating the number of seconds since the last command or response.

► **plaintextloginpause**: This specifies the number of seconds to pause after a successful plaintext login. For systems that support strong authentication, this option permits users to perceive a cost of using plaintext passwords. This does not affect the use of PLAIN in SASL authentications.

► **loginuseacl**: If enabled, any authentication identity that has rights on a user's inbox may log in as that user.

► **singleinstancestore**: If enabled, lmtpd attempts to only write one copy of a message per partition and create hard links. This results in a potentially large disk savings.

► **duplicatesuppression**: If enabled, lmtpd suppresses delivery of a message to a mailbox if a message with the same message-id or resent-message-id is recorded as already being delivered to the mailbox. This option records the mailbox and message-id or resent-message-id of all successful deliveries.

► **reject8bit**: If enabled, lmtpd rejects messages with 8-bit characters in the headers. Otherwise, 8-bit characters are changed to "X". A proper solution to non-ASCII characters in headers is offered by RFC 2047 and its predecessors.

► **maxmessagesize**: This option specifies the maximum incoming LMTP message size. If set, lmtpd rejects messages larger than maxmessagesize bytes. The default allows messages of any size.

- ► **lmtp_overquota_perm_failure**: If enabled, lmtpd returns a permanent failure code when a user's mailbox is over quota. By default, the failure is temporary.
- ► **sieve_maxscriptsize**: This is the maximum size (in kilobytes) that any sieve script can be. It is enforced at submission by timsieved.
- ► **sieve_maxscripts**: This is the maximum number of sieve scripts that any user can have. It is enforced at submission by timsieved.
- ► **deleteright**: This is the right that a user needs to delete a mailbox.
- ► **sieveusehomedir**: If enabled, lmtpd looks for sieve scripts in the user's home directories ~user/.sieve.
- ► **lmtp_allowplaintext**: This option allows the use of the SASL PLAIN mechanism for LMTP.
- ► **hashimapspool**: If enabled, the partitions are hashed, in addition to the hashing done on configuration directories. This is recommended if one partition has a bushy mailbox tree.
- ► **sasl_pwcheck_method**: This is the mechanism used by the server to verify plaintext passwords. Possible values include saslauthd and pwcheck.
- ► **tls_cert_file**: This is the file that contains the global certificate used for all services (imap, pop3, lmtp, sieve).
- ► **tls_key_file**: This file contains the private key that belongs to the global server certificate.
- ► **tls_require_cert**: Require a client certificate for all services (imap, pop3, lmtp, sieve).
- ► **tls_ca_file**: This file contains one or more Certificate Authority (CA) certificates.
- ► **tls_ca_path**: This option species the path to the directory with the CA certificates.
- ► **tls_ca_file**: This file contains one or more CA certificates.
- ► **tls_ca_path**: This option specifies the path to the directory with the CA certificates.
- ► **tls_session_timeout**: This option specifies the length of time (in minutes) that a TLS session is cached for later reuse. The maximum value is 1440 (24 hours), which is the default. A value of 0 disables session caching.
- ► **tls_cipher_list**: The list of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) ciphers to allow. The format of the string is described in ciphers(1).
- ► **mupdate_retry_delay**: This option specified the time to wait between connection retries to the mupdate server.
- ► **proxy_authname**: This is the SASL username (Authentication Name) to use when authenticating to the mupdate server (if needed). You cannot change this option. It is set to "manager" by default.

7.1.3 Configuring OpenLDAP

The Insight Server uses an OpenLDAP server and its database to store all the user information and is used to authenticate all the mail users. Navigate to the OpenLDAP configuration parameters as shown in Figure 7-6:

1. Log on to the Web Administration Console.
2. Click the **Configuration** option on the main page.
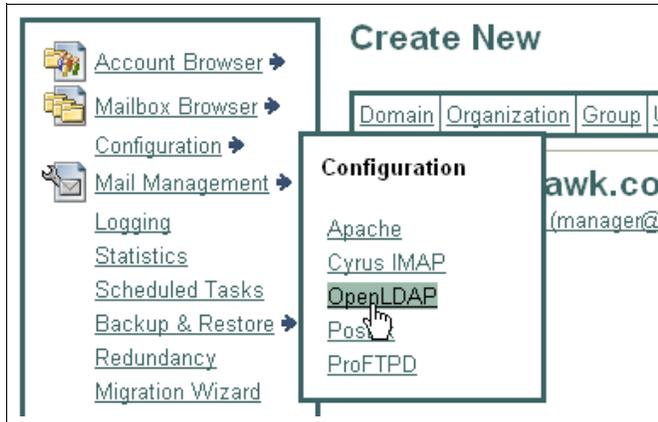3. Click the **OpenLDAP** option.

Figure 7-6 Navigating to the OpenLDAP configuration page

The options for OpenLDAP include:

► **allow**: Specifies a set of features (separated by white space) to allow (default none).

  – *bind_v2* allows acceptance of Lightweight Directory Access (LDAP) V2 bind requests.

  – *bind_anon_cred* allows anonymous bind creditials that are not empty, for example, when DN is empty.

  – *bind_anon_dn* allows unauthenticated (anonymous) bind when DN is not empty.

► **disallow**: Specifies a set of features (separated by white space) to disallow (default none).

  – *bind_anon* disables acceptance of anonymous bind requests.

  – *bind_simple* disables simple (bind) authentication.

  – *bind_krbv4* disables Kerberos V4 (bind) authentication.

  – *tls_2_anon* disables Start TLS from forcing a session to anonymous status (see also tls_authc).

  – *tls_authc* disables StartTLS if authenticated (see also tls_2_anon).

► **idletimeout**: Specifies the number of seconds to wait before forcibly closing an idle client connection. An idletimeout of 0 disables this feature. The default is 0.

► **include**: Reads additional configuration information from the given file before continuing with the next line of the current file.

► **pidfile**: This is the (absolute) name of a file that will hold the slapd server's process ID (see getpid) if it is started without the debugging command line option.

► **argsfile**: There is no available information for this option.

► **password-hash**: The hash to use for userPassword generation. It is one of {SSHA}, {SHA}, {SMD5}, {MD5}, and {CRYPT}. The default is {SSHA}.

► **schemacheck**: Turn schema checking on or off. The default is on { on | off }.

► **sizelimit**:

  – *integer*: Specifies the maximum number of entries to return from a search operation. The default size limit is 500.

  – *threads integer*: Specifies the maximum size of the primary thread pool. The default is 32.

- **timelimit**: *Integer* specifies the maximum number of seconds (in real time) that slapd spends answering a search request. The default time limit is 3600.

- **TLSCipherSuite**: *Cipher-suite-spec* allows configuration of the ciphers that will be accepted and the preference order. It should be a cipher specification for OpenSSL, for example TLSCipherSuite HIGH:MEDIUM:+SSLv2. To see which ciphers a spec selects, use:

```
openssl ciphers -v cipher-suite-spec
```

- **TLSCertificateFile**: Specifies the file that contains the slapd server certificate.

- **TLSCACertificateFile**: Specifies the file that contains certificates for all of the CAs that slapd recognizes.

- **TLSCertificateKeyFile**: Specifies the file that contains the slapd server private key that matches the certificate stored in the TLSCertificateFile file. Currently, the private key must not be protected with a password, so it is critical that it is protected carefully.

- **database**: *Databasetype* marks the beginning of a new database instance definition. It should be one of bdb, ldbm, shell, or passwd depending on which serves the database.

- **lastmod**:
  - *on | off*: Controls whether slapd automatically maintains the modifiersName, modifyTimestamp, creatorsName, and createTimestamp attributes for entries. By default, lastmod is on.
  - *readonly on | off*: This option places the database into read-only mode. Any attempts to modify the database return an "unwilling to perform" error message. By default, readonly is off.

- **rootdn**: DN specifies the distinguished name that is not subject to access control or administrative limit restrictions for operations on this database. This DN may or may not be associated with an entry. An empty root DN (the default) specifies no root access is to be granted. We recommend you specify the rootdn only when needed (such as when initially populating a database). If rootdn is within a naming context (suffix) of the database, a simple bind password may also be provided using the rootpw directive.

- **rootpw password**: Specifies a password (or hash of the password) for the rootdn. If the rootdn is not within the naming context of the database, the provided password is ignored. This option accepts all RFC 2307 userPassword formats known to the server (see the password-hash description) and cleartext. You may also use slappasswd to generate a hash of a password. Cleartext and {CRYPT} passwords are not recommended. If empty (the default), authentication of the root DN is by other means (for example, SASL). Use of SASL is encouraged.

- **suffix**: The *dn suffix* specifies the DN suffix of queries that are passed to this backend database. Multiple suffix lines can be given and at least one is required for each database definition.

- **updatedn**: The dn option is only applicable in a slave slapd. It specifies the DN allowed to make changes to the replica. Typically, this is the DN slurpd binds as when making changes to the replica.

- **cachesize**: *Integer* specifies the size in entries of the in-memory cache maintained by the LDBM backend database instance. The default is 1000 entries.

- **dbcachesize**: *Integer* specifies the size in bytes of the in-memory cache associated with each open index file. If not supported by the underlying database method, this option is ignored without comment. The default is 100000 bytes.

- **directory**: Specifies the directory where the LDBM files containing this database and associated indexes live. A separate directory must be specified for each database. The default is /var/db/openldap/openldapdata.

► **index**: {attrlist|default} [pres,eq,approx,sub,special] Specifies the indexes to maintain for the given attribute (or list of attributes). Some attributes only support a subset of indexes. If only an attr is given, the indexes specified for default are maintained. Note that setting a default does not imply that all attributes will be indexed. Several special index parameters may be specified. The index type sub can be decomposed into subinitial, subany, and subfinal indices. The special type nolang may be specified to disallow use of this index by language subtypes. The special type nosubtypes may be specified to disallow use of this index by named subtypes.

> **Note:** Changing index settings requires rebuilding indexes. See slapindex.

► **mode**: *Integer* specifies the file protection mode that newly created database index files should have. The default is 0600.

7.1.4 Configuring Postfix

The Mail Transport Agent (MTA) that is used is Postfix. This is the component that sends and receives all e-mail for the server. Postfix passes the incoming mail onto Cyrus, which in turn, delivers the e-mail to the correct mailboxes.

Navigate to the Postfix configuration parameters as shown in Figure 7-7:

1. Log on to the Web Administration Console.
2. Highlight the **Configuration** option on the main page.
3. Click the **Postfix** option.
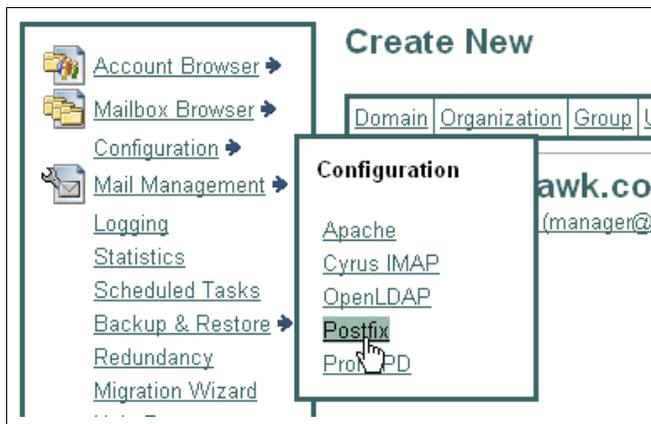
Figure 7-7   Navigating to the Postfix configuration page

The options are:

► **myhostname**: Describes the fully-qualified domain name of the machine running the Postfix system.

   – *$myhostname* appears as the default value in many other Postfix configuration parameters.

   – *mydomain* specifies the parent domain of $myhostname. By default, it is derived from $myhostname by stripping off the first part (unless the result is a top-level domain).

► **myorigin**: Specifies the domain from which locally-posted mail appears to come. The default is to append $myhostname, which is good for small sites. If you run a domain with multiple machines, you should change this to $mydomain and set up a domain-wide alias database that aliases each user to user@that.users.mailhost.

- **mydestination**: Specifies the list of domains for which this machine considers itself the final destination. That includes sendmail-style virtual domains hosted on this machine. Do not include Postfix-style virtual domains. Such domains are specified elsewhere (see sample-virtual.cf, and sample-transport.cf). The default is $myhostname + localhost.$mydomain. On a mail domain gateway, you should also include $mydomain. Do not specify the names of domains for which this machine is the backup mail exchange (MX) host. Specify those names via the relay_domains or permit_mx_backup settings for the Simple Mail Transfer (SMTP) server (see sample-smtpd.cf). The local machine is always the final destination for mail addressed to user@[the.net.work.address] of an interface on which the mail system receives mail (see the inet_interfaces parameter). Specify a list of host or domain names, /file/name or type:table patterns, separated by commas, white space, or both. A /file/name pattern is replaced by its contents. A type:table is matched when a name matches a lookup key. Continue longlines by starting the next line with a white space.

- **mynetworks**: Lists all networks that this machine trusts. This information can be used by the anti-UCE features to recognize trusted SMTP clients that are allowed to relay mail through Postfix.

- **relay_domains**: Controls the behavior of the reject_unauth_destination and permit_auth_destinationrestrictions that can appear as part of a recipient address restriction list.

- **relayhost**: Specifies the default host to send mail to when no entry is matched in the optional transport table. When no relayhost is given, mail is routed directly to the destination. On an intranet, specify the organizational domain name. If your internal DNS uses no MX records, specify the name of the intranet gateway host instead. In the case of SMTP, specify a domain, host, host:port, [host]:port, [address], or [address]:port. The form [host] turns off MX lookups. If you're connected via UUCP, see also the default_transport parameter.

- **soft_bounce**: Provides a limited safety net for testing. When soft_bounce is enabled, mail remains queued that otherwise bounces. This parameter disables locally-generated bounces. It also prevents the SMTP server from rejecting mail permanently (by changing 5xx replies into 4xx replies). However, soft_bounce is not a cure for address rewriting mistakes or mail routing mistakes.

- **queue_directory**: Specifies the location of the Postfix queue. This is also the root directory of Postfix daemons that run chrooted. See the files in examples/chrootsetup for setting up Postfix chroot environments on different UNIX systems.

- **command_directory**: Specifies the location of all postXXX commands. The default value is $program_directory. daemon_directory Specifies the location of all Postfix daemon programs (for example, programs listed in the master.cf file). The default value is $program_directory. This directory must be owned by root.

- **mail_owner**: Specifies the owner of the Postfix queue and of most Postfix daemon processes. Specify the name of a user account that *does not share* its user or group ID with other accounts and that *does not own* other files or processes on the system. Specifically, don't specify *nobody* or *daemon*. Use a dedicated user.

- **local_recipient_maps**: Specifies optional lookup tables with all names (not addresses) of users that are local with respect to $mydestination and $inet_interfaces. If this parameter is defined, then the SMTP server rejects mail for unknown local users. If you use the default Postfix local delivery agent for local delivery, uncomment the definition for alias_maps.

> **Important:** If the Postfix SMTP server runs chrooted, you may have to copy the passwd (not shadow) database into the jail. This is system dependent.

- ▶ **in_flow_delay**: Implements mail input flow control. This feature is turned on by default, although it still needs further development. A Postfix process pauses for $in_flow_delay seconds before accepting a new message, when the message arrival rate exceeds the message delivery rate. With the default 50 SMTP server process limit, this limits the mail inflow to 50 messages a second more than the number of messages delivered per second. Specify 0 to disable the feature. Valid delays are 0 to 10.

- ▶ **alias_maps**: Specifies the list of alias databases used by the local delivery agent. The default list is system dependent. On systems with NIS, the default is to search the local alias database and then the NIS alias database. See aliases for syntax details. If you change the alias database, run `postalias /etc/aliases` (or wherever your system stores the mail alias file), or simply run `newaliases` to build the necessary DBM file type or database file. It take a minute or so before changes become visible. Use `postfix reload` to eliminate the delay.

- ▶ **alias_database**: Specifies the alias database that is built with newaliases or sendmail -bi. This is a separate configuration parameter, because alias_maps may specify tables that are not necessarily all under control by Postfix.

- ▶ **mailbox_transport**: Specifies the optional transport in master.cf to use after processing aliases and .forward files. This parameter has precedence over the mailbox_command, fallback_transport and luser_relay parameters. Specify a string of the form *transport*:nexthop, where *transport* is the name of a mail delivery transport defined in master.cf. The :nexthop part is optional. For details, see the sample transport configuration file.

- ▶ **fallback_transport**: Specifies the optional transport in master.cf to use for recipients that are not found in the UNIX passwd database. This parameter has precedence over the luser_relay parameter. Specify a string in the form *transport*:nexthop, where *transport* is the name of a mail delivery transport defined in master.cf. The *:nexthop* part is optional.

- ▶ **luser_relay**: Specifies an optional destination address for unknown recipients. By default, mail for unknown local recipients is bounced. The following expansions are done on luser_relay:

  - – $user (recipient username)
  - – $shell (recipient shell)
  - – $home (recipient home directory)
  - – $recipient (full recipient address)
  - – $extension (recipient address extension)
  - – $domain (recipient domain)
  - – $local (entire recipient localpart)
  - – $recipient_delimiter

  Specify ${name?value} or ${name:value} to expand the value only when $name does (does not) exist. luser_relay works only for the default Postfix local delivery agent.

- ▶ **smtpd_banner**: Specifies the text that follows the 220 code in the SMTP server's greeting banner. Some people like to see the mail version advertised. By default, Postfix shows no version.

- ▶ **local_destination_concurrency_limit**: How many parallel deliveries go to the same user or domain? With local delivery, it does not make sense to do massively parallel delivery to the same user, because mailbox updates must happen sequentially. Also, expensive pipelines in .forward files can cause disasters when too many are run at the same time. With SMTP deliveries, 10 simultaneous connections to the same domain can be sufficient. Each message delivery transport has its XXX_destination_concurrency_limit parameter. The default is $default_destination_concurrency_limit for most delivery transports. For the local delivery agent, the default is 2.

- **default_destination_concurrency_limit**: Check help for local_destination_concurrency_limit.

- **debug_peer_level**: Specifies the increment in verbose logging level when an SMTP client or server host name or address matches a pattern in the debug_peer_list parameter.

- **disable_mime_input_processing**: While receiving, give no special treatment to Content-Type: message headers. All text after the initial message headers is considered to be part of the message body.

- **disable_mime_output_conversion**: Disable the conversion of 8BITMIME format to 7BIT format when the remote system does not advertise 8BITMIME support.

- **disable_vrfy_command**: This stops some spammers from trying to extract valid e-mail address. By default, it is set to *Yes* and cannot be changed here.

- **mime_boundary_length_limit**: This specifies the amount of space that is allocated for MIME multipart boundary strings. The MIME processor is unable to distinguish between boundary strings that do not differ in the first $mime_boundary_length_limit characters.

- **mime_nesting_limit**: The maximal nesting level of multipart mail that the MIME processor can handle. Refuse mail that is nested deeper.

- **strict_8bitmime**: Reject mail with 8-bit text in content that claims to be 7-bit, or in content that has no explicit content encoding information. This blocks mail from poorly written mail software. Unfortunately, this also breaks majordomo approval requests when the included request contains valid 8-bit MIME mail. It also breaks bounces from mailers that do not properly encapsulate 8-bit content (for example, bounces from qmail or from old versions of Postfix).

- **strict_mime_domain_encoding**: Reject mail with invalid Content-Transfer-Encoding: information for message/* or multipart/*. This blocks mail from poorly written software.

- **always_bcc**: Address to send a copy of each message that enters the system.

- **hash_queue_depth**: This is the number of subdirectory levels for hashed queues.

- **hopcount_limit**: Limit the number of Received: message headers.

- **max_idle**: Limit the time in seconds that a child process waits between service requests.

- **max_use**: Limit the number of service requests handled by a child process.

- **delay_warning_time**: This option specifies after how many hours a warning is sent that mail is not yet delivered. By default, no warning is sent.

- **initial_destination_concurrency**: Controls the number of messages that are initially sent to the same destination before adapting delivery concurrency. Of course, this setting is effective only as long as it does not exceed the process limit and the destination concurrency limit for the specific mail transport channel.

- **maximal_backoff_time**: This is the maximum amount of time that a message is not looked at after a delivery failure.

- **maximal_queue_lifetime**: This is the maximum amount of time that a message is not looked at after a delivery failure.

- **minimal_backoff_time**: This is the minimal amount of time that a message is not looked at and the minimal amount of time to stay away from a dead destination.

- **queue_run_delay**: This option specifies how often the queue manager scans the queue for deferred mail.

- **bounce_size_limit**: This option specifies how much of an undelivered message is sent back to the sender.

- **default_process_limit**: This is the default limit for the number of simultaneous child processes that provide a given service

- **fork_attempts**: This value indicates the number of times to attempt to create a new process before giving up.

- **fork_delay**: This is the delay between attempts to create a new process.

- **deliver_lock_attempts**: This option indicates the number of times to try locking a file before giving up.

- **deliver_lock_delay**: This option specifies how long to wait between attempts to lock a file.

- **duplicate_filter_limit**: Limits the number of envelope recipients that are remembered.

- **header_size_limit**: Limits the amount of memory in bytes used to process a message header.

- **line_length_limit**: How long a line of text can be before it is broken into pieces. All Postfix perimeter programs (SMTP server, SMTP client, local pickup, and local delivery) enforce this line length limit when reading data from an untrusted source. Long lines are reconstructed upon delivery.

- **message_size_limit**: This is the maximum size of a Postfix queue file, including envelope information (sender, recipient, etc.).

- **queue_minfree**: This option specifies the number of bytes of free space that is needed in the queue file system. The SMTP server declines inbound mail delivery requests when there is insufficient space. The mail is accepted after enough space becomes available). There is no default limit. However, it seems like a good idea to require at least several times $message_size_limit so that the mail system won't be stuck on a single large message.

- **transport_retry_time**: This is the amount of time between queue manager attempts to contact an apparently defunct Postfix delivery service.

- **stale_lock_time**: This value specifies how old an external lock file may be before it is forcibly removed.

- **allow_percent_hack**: Changes the percent character to the at (@) character, rewriting user%domain to user@domain.

- **fallback_relay**: This option specifies hosts to hand off mail to if a message destination is not found or if a destination is unreachable.

- **ignore_mx_lookup_error**: When a name server fails to respond to an MX query, search for an A record instead deferring mail delivery smtp_connect_timeout Timeout for completing a TCP connection. When no connection can be made within the deadline, the SMTP client tries the next address on the mail exchanger list.

- **smtpd_timeout**: Limit the time to send a server response and to receive a client request.

- **smtpd_tls_auth_only**: Setting this option to *no* requires that the passwords used for authentication cannot be sent on a secure channel.

- **smtpd_tls_cert_file**: Sets the path to the TLS certificate.

- **smtpd_tls_key_file**: Sets the path to the TLS private key.

- **smtpd_tls_CAfile**: Sets the path to the CA Certificate.

- **smtpd_use_tls**: Globally enables/disables TLS.

- **smtpd_enforce_tls**: This is set to *no* by default. If it is set to *yes*, the server cannot communicate with the clients unless they use TLS and configured with the appropriate certificates.

- ► **smtpd_tls_cipherlist**: Set as the default, this list provides certificates when a client is authenticating with the server.
- ► **smtpd_starttls_timeout**: Limits the time in seconds to write and read operations during TLS start and stop handshake procedures.
- ► **smtpd_sasl_auth_enable**: Enables SASL for SMTP-AUTH checking.
- ► **smtpd_recipient_restrictions**: Specifies restrictions on recipient addresses that clients can send in RCPT TO commands.
- ► **virtual_maps**: This option list virtual mapping tables.
- ► **ldapsource_server_host**: Specifies the LDAP server.
- ► **ldapsource_server_port**: Specifies the LDAP server port.
- ► **ldapsource_timeout**: This limits the response time in seconds for search operations during a client query.
- ► **ldapsource_query_filter**: Sets what results are returned after a query of the OpenLDAP database.
- ► **ldapsource_result_attribute**: Sets how results are returned after a query of the OpenLDAP database.
- ► **ldapsource_bind**: Ensures that the client is not bound to the server, allowing other users to perform queries.

7.1.5 Configuring ProFTPD

ProFTPD is used to receive the free/busy information for e-mail users. ProFTPD is configured for authentication only. Outlook users must authenticate to ProFTPD to publish the free/busy information via File Transfer Protocol (FTP). The free/busy information is saved in a directory /opt/is4/home/freebusy, which in turn, is published via Apache for Outlook.

Settings
You can find an explanation of the configuration parameters by selecting the online help in the Web Administration Console.

Figure 7-8 shows the typical settings for free/busy in Outlook2000.

Figure 7-8   Outlook free/busy configuration

Add a free/busy user to the server for everyone to use for authentication. You can use a resource to create the free/busy user since no mailbox is needed for this user.

See Chapter 4, "Configuring Insight Connector and Insight AddressBook" on page 61, to learn how to configure the Outlook 2002 free/busy feature.

Navigate to the ProFTPD configuration parameters as shown in Figure 7-9:

1. Log on to the Web Administration Console.
2. Select the **Configuration** option on the main page.
3. Click the **ProFTPD** option.
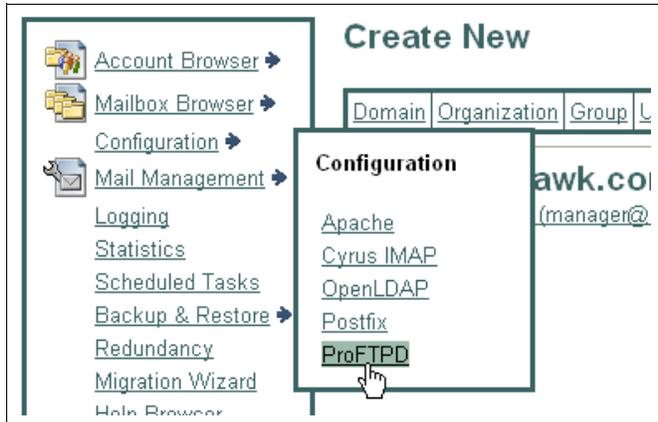
Figure 7-9   Navigating to the ProFTPD configuration page

The options for ProFTPD are:

- ► **ServerName**: Configures the name displayed to connecting users.
- ► **ServerType**: Sets the mode in which ProFTPD runs.
- ► **DefaultServer**: Sets the default server.
- ► **RequireValidShell**: Allows connections based on /etc/shells.
- ► **Port**: Sets the default port to *listen*.
- ► **Umask**: Sets the default *umask*.
- ► **User**: Sets the user that the daemon will run as.
- ► **Group**: Sets the group in which the daemon will run.
- ► **DefaultRoot**: Sets the default chroot directory.
- ► **AllowOverwrite**: Enables files to be overwritten.
- ► **MaxInstances**: Sets the maximum number of child processes to be spawned.
- ► **UseReverseDNS**: Toggles rDNS lookups.
- ► **IdentLookups**: Toggles ident lookups.
- ► **TimeoutLogin**: Sets the login timeout.
- ► **TimeoutIdle**: Sets the idle connection timeout.
- ► **TimeoutNoTransfer**: Sets the connection without transfer timeout.
- ► **TimeoutStalled**: Sets the timeout on stalled downloads MaxClients. Limits the number of users that can connect.

7.2 User preferences

When the user logs into Web Administration Console with their user ID and password, the User Configuration window opens.

7.2.1 User preference configuration

On the login display, enter the user ID and password. The window now shows all the user information that can be changed (Figure 7-10).
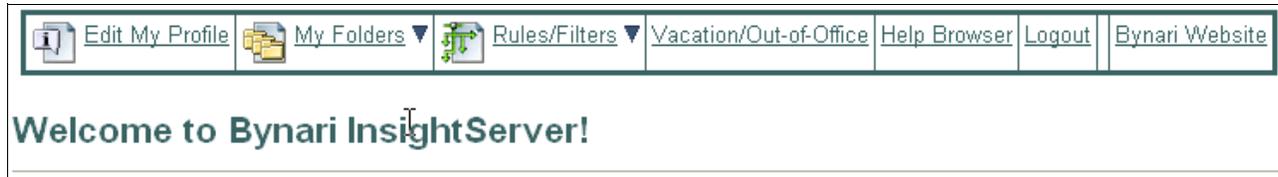
Figure 7-10   User-specific configuration

7.2.2 Edit My Profile

This changes the personal information that is displayed in the LDAP directory (Global Address Listing) or can be used to change the password.

7.2.3 My Folders

Users can view or create new folders that appear in Outlook on the server. When viewing folders, all the folders are displayed that the user can view.

7.2.4 Rules/Filters

Incoming e-mail rules are created that manipulate the incoming e-mail to the specified rule. You can see this on the Rules Configuration panel (Figure 7-11). The configuration panel is user friendly. You can easily create a new rule.

Figure 7-11   User rule created on the server

7.2.5 Vacation/Out of Office

This section allows for the customization of a vacation/out-of-office message for the specified number of days. Enter the desired message, and all in coming e-mail receives a reply with the message entered. No incoming e-mail is lost.

7.2.6 User Search

You can search for user information for quicker access. Highlight the account browser option. Click **User Search** and enter the search criteria.

7.3 Security

Due to the installation mode of Insight Server in a Chroot environment, the operating system is harder to breach. The server is installed in its own virtual system, creating a secure e-mail server. No system accounts are created, so hacking on e-mail user IDs is fruitless, because more security is added to the e-mail server. E-mail authentication is achieved via the LDAP server. It maintains its own database by creating a secure authenticating mechanism for all e-mail accounts.

7.4 Backup and restore

The server's data can be backed up to a file through the Web interface. Select **Backup and Restore**. Then choose either **Create backup** or **Restore and Upload**.

7.4.1 Backing up configuration files, LDAP, Mailstore

Backups can be done of the servers configuration, LDAP database, and mail store. Select the section to backup and then select the type of file format:

- ► TAR
- ► TGZ
- ► TBZ2

All the files that were backed up are displayed when the backup procedure is selected. This allows the user to select which files need to be restored.

The files that are created include the following types:

- ► **Configuration**: Files of Apache, ProFTP, Postfix. The file name listed is cfg_date_time.compressiontype.

- ► **LDAP file**: Files that are the used by the LDAP server. The file name listed is ldap_date_time.compressiontype.

- ► **Mail Data file**: All the mailboxes used by the server. The name listed is mail-date_time.compressiontype.

7.4.2 Restoring configuration files, LDAP, Mailstore

Restoring configuration files overwrites the existing files on the system. When restore is selected, the files are displayed that were created to select for restoration. The files are the configuration files for Apache, LDAP, ProFTP, and Postfix.

When you restore the mail store, a list box appears that shows all the users that can be restored. The user's mailbox is restored as a whole. Individual files cannot be selected by the Web interface. After mail is restored, Insight Server automatically reconstructs the user's folders. A system message is returned indicating that the mailbox has been reconstructed, which is the Cyrus command to rebuild the databases used by Cyrus.

7.4.3 Uploading and replacing existing or older configuration files

Other files can be uploaded to the server for the purpose of restoring. Click **Browse** to select the file to upload. The file is displayed. Then select the file on the Restore page to restore it. Finally, click **Upload**.

7.5 Redundancy

Bynari Insight Server can be configured to have redundancy by creating a slave server. The slave server has a copy of the original configuration from the master. In the event of the master failing, the slave continues to be functional. A master server must be established by selecting the role in the Selection panel. The slave server cannot communicate with the master. User accounts created on the slave are verified with the master to prevent any duplication from occurring.

7.5.1 Single role

All user e-mail data and login information is on a single server. This is the default installed mode of the Insight Server.

7.5.2 Master role

In the master/slave role, all the accounts are stored on the master server and all e-mail data is stored on the slave server. The master maintains user information in the LDAP directory, which is for e-mail authentication. It also accepts the logon and redirects the request to the slave to retrieve e-mail data. Users can log into the slave server but cannot share contacts with everyone listed on the master server, only with users on the slave server.

The master server can have multiple slave servers and the user load distributed among the slaves. When adding a user, you have can choose to which slave server the user account must be created.

7.5.3 Slave role

The slave server maintains all the e-mail data that is directed from the master. It polls the master server for all the data and user accounts created. The master polls the slave when user accounts are created on the master.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see "How to get IBM Redbooks" on page 123. Note that some of the documents referenced here may be available in softcopy only.

► *Linux on the IBM @server iSeries Server: An Implementation Guide*, SG24-6232

► *Linux Integration with OS/400 on the IBM @server iSeries Server*, SG24-6551

► *LPAR Configuration and Management: Working with IBM @server iSeries Server Logical Partitions*, SG24-6251

Online resources

These Web sites are also relevant as further information sources:

► Bynari Web site

http://www.bynari.net

► Linux Online

http://www.linux.org/docs/index.html

► SuSE

http://www.suse.com

► RedHat

http://www.redhat.com

► PHP

http://www.php.net

► Smarty Template Engine

http://smarty.php.net

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Symbols

/opt/is4/var/log/apache   107
/opt/is4/var/log/apache/   107

A

access control list (ACL)   4
Account Browser   48
ACL (access control list)   4
AddressBook   6
admins   109
alias_database   115
allow   111
allow_percent_hack   117
allowanonymouslogin   108
allowplaintext   108
allowsubscribe   108
altnamespace   108
always_bcc   116
anti-spam software   4
anti-spamming   4
Apache   3
Apache log file location   107
Apache server configuration   106
argsfile   111
autocreatequota   109

B

bounce_size_limit   116
bulk mail protection   4
Bynari benefits
    cost efficiency   3
    enhanced management tools   4
    migration   4
    reliability   3
    security   4
Bynari Insight Server   10

C

cachesize   112
calendar   98
check name   6
CN (common name)   55
command_directory   114
common name (CN)   55
configdirectory   108
contacts   97
corporate workgroup mode   2, 5
cost efficiency   3
Create Ethernet Line (CRTLINETH) command   27
Create Network Server Description (CRTNWSD) command   25
CRTLINETH command   27

CRTNWSD command   25
Cyrus IMAP   3, 104, 107

D

dbcachesize   112
debug_peer_level   116
default_destination_concurrency_limit   116
default_process_limit   117
defaultacl   109
DefaultServer   119
delay_warning_time   116
deliver_lock_attempts   117
deliver_lock_delay   117
directory   112
disable_mime_input_processing   116
disable_mime_output_conversion   116
disable_vrfy_command   116
disallow   111
disk storage requirements   10
distinguished name (DN)   52
DN (distinguished name)   52
duplicate_filter_limit   117
duplicatesuppression   109

E

e-mail traffic scanning   4
encryption   4
enhanced management tools   4
enterprise-level messaging services   1
ErrorDocument directive   107
EXMerge   104

F

fallback_relay   117
fallback_transport   115
Files/Permissions   108
folder sharing   73
fork_attempts   117
fork_delay   117
free/busy
    configuration   77
    information   118

G

GAL (Global Address List)   6
Global Address List (GAL)   6
Global Unique Identifier (GUID)   71
group creation   51
GUID (Global Unique Identifier)   71

H

hash_queue_depth   116

125

IBM

Bynari Insight Server V4 for Linux on the IBM @server iSeries Server

Bynari Insight Server V4 for Linux

on the IBM *e*server iSeries Server

IBM®

Redbooks

Get to know the Bynari Insight product family of messaging services

Learn how to install and configure the Insight Server and clients

Explore administration and operations tips

In this world of e-business on demand computing, server consolidation in the right fashion becomes critically important. You need reliability, availability, and rich functionality, while maintaining the lowest total cost of ownership (TCO). IBM *e*server iSeries is proven to be one of the best platforms for server consolidation. Linux on iSeries provides an excellent choice to build the infrastructure of Web-based dynamic mission-critical applications. On top of its well functioning and reliable open source-based solutions, it provides ready-to-use business applications. The Bynari Insight Server, along with its Insight product family, is a fine example of business applications that run on Linux on iSeries.

Bynari Insight Server V4 provides enterprise-level messaging services within and among the various parts of an organization's network of people and resources. It also provides a safe harbor for an organization's messaging needs by using the Internet mail model. Using Insight Server V4 and running on the iSeries server, users can replace the Microsoft Exchange Server. This allows them to achieve higher reliability, availability, scalability, and even reduce the total cost.

This IBM Redbook is designed to help system administrators and information technology (IT) managers to understand the main benefits of Bynari Insight Server V4 and its product family. It explains how to install, configure, and administer the Insight Server and its products. Plus this redbook offers tips for operating the Bynari Insight Server.