Novell
Open Workgroup Suite Small Business Edition

2.0

May 2, 2008

INSTALLATION AND
ADMINISTRATION GUIDE

Novell®

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

Novell® Open Workgroup Suite Small Business Edition (NOWS SBE) is the first workgroup suite for small businesses to provide organizations with a flexible solution based on proven open standards-based software. The Novell suite features a simple yet customizable installation process along with remote management capabilities. This means that solution providers can remotely manage their small business customers' IT infrastructures, thus reducing costs and improving service.

Audience

This guide is intended for Novell Open Workgroup Suite Small Business Edition 2.0 administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell Open Workgroup Suite Small Business Edition Administration and Installation Guide*, visit the Novell Documentation Web site (http://www.novell.com/documentation/nows/).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Understanding NOWS SBE 2.0

1

1.1 Overview

Novell® Open Workgroup Suite Small Business Edition (NOWS SBE) is the first workgroup suite for small businesses to provide a flexible solution based on proven open standards-based software. The Novell suite features a simple yet customizable installation process along with remote management capabilities. This means that solution providers can remotely manage their small business customers' IT infrastructures, thus reducing costs and improving service.

The Novell Open Workgroup Suite Small Business Edition also has a newly developed integration layer that makes it easier for resellers and service providers to integrate their specialized products into a solution. The suite is supported by popular business software applications certified to work with SUSE® Linux Enterprise Server (SLES). Novell Open Workgroup Suite Small Business Edition includes Novell Groupwise® for e-mailing and calendaring; Novell Open Enterprise Server (OES) for advanced storage management, user and rights administration, and clustering and failover capabilities; SUSE Linux Enterprise Desktop (SLED) from Novell for complete desktop productivity; and the Novell edition of the popular office productivity suite, OpenOffice.org, for Windows* and Linux.

1.2 NOWS SBE 2.0: What's New?

NOWS SBE 2.0 represents an upgrade from SLES 9 to SLES 10 SP1 as well as an upgrade from OES 1 to OES 2. All updates are made through the Novell Customer Center.

For information about upgrading to NOWS SBE 2.0, see the Upgrading Readme (http://www.novell.com/documentation/nows_sbe_20/nows_upgrade_readme_20/data/nows_upgrade_readme_20.html).

For more information about SLES 10, see the Novell SLES 10 SP1 Web site (http://www.novell.com/documentation/sles10/index.html).

For more information about OES 2, see the Novell OES 2 Web site (http://www.novell.com/documentation/oes2/index.html).

For more information about the Novell Customer Center, see the Customer Center Web site (http://www.novell.com/customercenter/).

These Novell components are new to NOWS SBE 2.0:

- iFolder® 3.6
- iPrint

- GroupWise 7.0.2
- GroupWise Messenger 2.0.2

These open source components are also new to NOWS SBE 2.0:

- Amanda 2.6.0
- ClamAV* 0.92.1
- OpenOffice.org* 2.3
- HylaFAX* 4.4.4
- MailScanner 4.67.4-1
- TightVNC 1.3.9
- OpenVPN* 2.1
- pGina 1.8.8
- jHylaFAX 1.3.10
- PuTTY 0.60

1.3 Product Components

Novell Open Workgroup Suite Small Business Edition 2.0 includes a comprehensive collection of services and applications that provide small offices with all the networking capabilities that are in a corporate setting. The following solutions and features are part of the suite:

1.3.1 Backup, Restore, and Recovery

- **Personal File Backup (iFolder):** Novell iFolder is a simple and secure storage solution that enables you to back up, access, and manage your personal files from anywhere, at any time. After you have installed iFolder, you simply save your files locally—as you have always done—and iFolder automatically updates the files on your network server and delivers them to the other machines you use.

- **Network Backup (Amanda):** Amanda allows you to set up a single backup server to back up multiple hosts to a tape-based or disk-based storage system. Amanda uses native dump and GNU tar facilities and can back up a large number of workstations and servers running various versions of Linux, UNIX or Microsoft* Windows operating systems.

1.3.2 Business Applications

- **OpenOffice.org:** OpenOffice.org is a full-featured office suite. It includes word processing, presentation, spreadsheet, and database applications.

1.3.3 Collaboration Groupware and Messaging

- **E-Mail and Collaboration (GroupWise):** GroupWise is a set of tools that keeps your employees connected to clients and each other. The system comes with e-mail, calendaring, and instant messaging to be set up according to your company needs.

1.3.4 File, Print, and Fax

- **Print Services (iPrint):** iPrint is a network printing service that allows everyone to print at a centralized location. iPrint extends print services securely across multiple networks and operating systems.
- **Windows File and Print Sharing (Samba):** The Samba file and print sharing service for Windows enables you to configure your network with the security of Linux and still be able to access files on your Windows servers.
- **Fax Server (HylaFAX):** HylaFAX is the leading fax server for UNIX-like computer systems. It uses a client-server design and supports the sending and receiving of faxes, as well as text pages, on any scale from low to very high volumes, making use of large numbers of modems if necessary.

1.3.5 Security Management

- **Anti-Virus (ClamAV):** Clam AntiVirus is an anti-virus toolkit for UNIX designed especially for e-mail scanning on mail gateways. It provides a number of utilities, including a flexible and scalable multi-threaded daemon, a command line scanner, and an advanced tool for automatic database updates. The core of the package is an anti-virus engine available in the form of a shared library.
- **VPN Server (OpenVPN):** OpenVPN is a component that enables users to work remotely. A Virtual Private Network (VPN) allows users to connect securely to your internal business network and conduct business transactions with the same functionality as they do within the office.
- **Firewall (IPTables):** A firewall is a hardware or software device configured to permit, deny, or proxy data through a computer network that has different levels of trust. Novell Open Workgroup Suite Small Business Edition 2.0 includes a fully-configurable firewall service to keep out unwanted traffic and intruders.

1.3.6 Systems Management

- **Dynamic Local User:** If you have Windows on desktops, you can use the Dynamic Local User component to synchronize the Novell Client™ with the Windows client so that login is seamless to your users.
- **Directory Services (eDirectory):** eDirectory™ manages user identities and is the core of all rights and privileges in your NOWS SBE network.
- **Helpdesk:** Helpdesk aids administrators in tracking trouble calls and giving end users the ability to submit trouble tickets without picking up the phone.
- **Management Tools (iManager):** This is a role-based tool for network and systems management of your environment through a consolidated Web interface.

- **DHCP:** Dynamic Host Configuration Protocol (DHCP) enables your server to dynamically assign IP addresses as clients need them instead of statically assigning an IP address to each of the clients.
- **DNS:** Dynamic Name Server (DNS) is a service used to link a common name to an IP address for easy location and searching of resources over TCP/IP.
- **VPN Server (OpenVPN):** Remote access software used to connect securely to your company files when you are away from the office.
- **Remote Desktop (TightVNC):** This software gives your administrators the ability to remotely manage and assist end users with questions and tasks.

1.4 Requirements

The hardware used for installation must be in the tested and approved hardware list. Support is available only to those who install on the tested and approved hardware.

- Section 1.4.1, "Approved and Tested Hardware List," on page 14
- Section 1.4.2, "Server Requirements," on page 14
- Section 1.4.3, "Desktop Operating System and Browser Requirements," on page 15

1.4.1 Approved and Tested Hardware List

- For a list of tested and approved hardware, see YES CERTIFIED (http://developer.novell.com/yessearch/).

1.4.2 Server Requirements

The following server requirements are based on OES 2 server requirements.

Table 1-1 *Server Requirements*

Server Components	Minimum Requirements	Recommended Requirements
Server	Server-class computer with Pentium* II or AMD* K7 450 Mhz processor (Bootable DVD-ROM drive)	Server-class computer with Pentium III, Pentium III Xeon*, Pentium 4, Intel* Xeon 700 Mhz, AMD K8 CPUs (Athlon64 and Opteron*), Intel EM64T or higher processor (Bootable DVD-ROM drive)
Memory	512 MB of RAM	1 GB of RAM
Disk Space	10 GB of unpartitioned disk space	Additional disk space might be required, depending on which OES components are selected and how they are used.

1.4.3 Desktop Operating System and Browser Requirements

Table 1-2 *Desktop and Browser Requirements*

Desktop Operating System	Browser
Windows 2000	NA
Windows XP	Internet Explorer* 7 or higher
Windows Vista*	Internet Explorer 7 or higher
SUSE Linux Desktop (SLED) 10	Mozilla* Firefox* 2.0x
Mac OS* X	Mozilla Firefox for Macintosh* 2.0x

NOTE: IE 6 is not supported.

1.5 Planning for the NOWS SBE Install

When planning your installation of Novell Open Workgroup Suite Small Business Edition, keep the following items in mind:

1.5.1 Server

By accepting the default partitioning information, the installation overwrites all existing files on the server. Change this configuration if you plan to install NOWS SBE 2.0 on an existing partition. Verify that the server does not see any partitions or devices that you do not want formatted and wiped. If components are installed while connected to a Storage Area Network (SAN), there is the potential to wipe out any partitions and data that it sees.

You also need to make sure that your server is plugged into a network where DHCP is installed.

1.5.2 Firewall (IPTables)

Below is a table with the typical ports that need to be opened on your firewall for each component.

Table 1-3   *Port numbers*

Component	Port Type	Port Number
Amanda	UPD	10080
iManager	TCP	80, 443
Samba	UDP	631, 135, 137, 138, 139, 445
Samba	TCP	137, 138, 139
iFolder	TCP	80, 443
GroupWise	TCP	25, 80, 443, 110, 143, 993, 1677, 7100, 7101, 7102, 7180, 71, 81, 8200, 8312, 8300, 9850
DNS	UDP, TCP	53, 953
ClamAV	TCP	3310
OpenVPN	NA	NA
HylaFAX	TCP	4557, 4559
Helpdesk	TCP	80, 443
iPrint	TCP	80, 443, 631
IPTables	TCP	8181, 22, 8182
eDirectory	NCP	389, 636, 427, 524, 8008, 8009, 8028, 8030, 8180, 9009
eDirectory	TCP	524
DHCP	UDP	67

1.5.3 Component Install Order

Begin component installation with eDirectory, then install iManager. You need iManager to manage iPrint, iFolder, Helpdesk, and GroupWise, (as well as eDirectory).

If you chose to install both MailScanner and GroupWise, be sure to install GroupWise first.

1.5.4 Creating a New Directory

Before you create a new eDirectory tree, you should define a naming standard. A consistent naming scheme provides a guideline for network administrators who will add, modify, or move objects within the eDirectory tree. For additional information, see the eDirectory Documentation Web site (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/acavuil.html).

1.5.5 NetWork Backup (Amanda)

If you choose to install Amanda with a tape drive instead of installing on your hard drive, you might need information about supported tape drives. See the Amanda Documentation Web site (http://www.amanda.org/docs/AMANDA-docs.html).

1.5.6 E-Mail and Collaboration (GroupWise)

If you are installing GroupWise and MailScanner, when you install the GroupWise Internet Agent you are given the opportunity to assign the Internet Agent a different port (the default is 26) so that the two programs do not conflict. Incoming mail from the Internet to the GroupWise system is then accepted by MailScanner on port 25 (SMRP's default), scanned, and delivered to the Internet Agent, which accepts non-standard mail on port 26.

1.5.7 Helpdesk

You need an e-mail account designated for notifications and workflows for the Helpdesk component. You can use an existing account or create one named support@yourdomain.com or helpdesk@yourdomain.com.

Getting Started

2

2.1 Installing Novell Workgroup Suite Small Business Edition

Verify that you have one disk with the Novell® Open Workgroup Suite Small Business Edition 2.0 installation files, or download the installation ISO from http://www.download.novell.com to a location of your choice and burn it to a DVD. The download is 5 GB and takes a moment to complete.

If you use a VMware* or other virtualized environment session instead of a physical server, make sure to designate the boot sequence to boot from the CD-ROM.

2.1.1 Beginning the Installation

1 Insert the NOWS SBE DVD into the DVD drive.

2 Boot the server. You are presented with a splash screen. Using the Down-arrow key, select `Installation`, then press Enter.

3 The first page is the End User License Agreement (EULA). Read through the agreement and click *I Agree* to advance to the next page.

4 After the initial files have been loaded into the system, you are prompted to set up the initial configuration of your server on the Installation Settings window. You now have the following two options:

   ◆ If you do not want to change any of the settings and choose to keep the defaults, just click *Accept* in the lower right corner of the window. A Confirm Installation message appears; if you are satisfied with the default, click *Install*.

   ◆ If you want to change any of the settings, click *Change* and select the setting you want to modify. Repeat this task until all changes are complete. If you are satisfied with your changes, click *Accept* in the lower right corner of the Installation Settings main window. A Confirm Installation message appears; if you are satisfied with your changes, click *Install*.

IMPORTANT: Do not change the configurations for the Software settings. Doing so causes your install to fail.

---

5 On the Network Configuration window, if you want to change any of the network settings, click *Change* and select the setting you want to modify. If you do not want to make any changes, click *Next*.

You are then presented with an IP address at the server prompt so you can move to the browser-based portion of the installation and configuration. Make a note of the IP address; you need it to access the Web site where you continue the installation. You have now completed the base installation of the server.

6 If you receive an IP address of https://127.0.0.1:8181 or https://:8181 instead of a valid IP address, DHCP is not functioning. Complete the following steps:

  6a Verify that you are connected to the network with your DHCP server.

  6b At the command line, log in as `root` without a password. The default password is `novell`.

  6c Enter the following command: `/etc/init.d/network restart`. You can also enter `rcnetwork restart`

2.1.2 Web Installation and Configuration

IMPORTANT: You must begin your component download with eDirectory™ and iManager. These two software components help you to manage many of the remaining components.

If you want to install GroupWise and MailScanner on the same server, use the *Add/Remove* function to add MailScanner only after GroupWise is installed. Adding these two applications simultaneously at the initial install might cause the GroupWise install to fail.

1 Type the link supplied at the end of your server installation in your Web browser and press Enter to bring up the first page of the Web installation.

2 The first page you see is the End User License Agreement (EULA). Read through the agreement and click *I Agree* to advance to the next page.

3 The next page is Network Settings. Verify the settings or add the correct information.

    ◆ **IP Address:** The address should be the one from the initial setup of your server operating system. Verify that this is accurate.

    ◆ **Netmask:** Verify the netmask from your network.

    ◆ **Gateway:** Verify the gateway from your network.

    ◆ **DNS Entry:** Verify the IP address of your DNS server.

    ◆ **Host:** Specify a name for your server. The hostname should be the same as your server. You should not include special characters in the name of your server.

    ◆ **Domain:** The Domain should match the name of your Internet domain name.

4 After you have specified the correct information, click *Next*.

5 You are then advanced to the License Key page. Specify your contact e-mail address and the license keys that were provided to you, then click *Next*.

6 Click *Check for Updates*. If updates are found, select *Install Updates*. After the check is complete, click *Next*.

7 On the User Information page, specify the password information for the administrator login. You have two options:

- ◆ **Basic Setup:** Specify a password for the NOWS SBE Administrator. The server root password will be the same.

- ◆ **Advanced Mode:** Click *Advanced Mode*. This allows you to specify a separate password for the NOWS SBE Administrator (sbsadmin) and for the server admin.

> **IMPORTANT:** The difference between these two passwords is that the NOWS Administrator password enables you to add, remove, or configure components on your NOWS server from the NOWS Admin console. The server password is what you use to configure or update your server from the console. If you do not choose to make each password different, then the passwords are the same as the NOWS Administrator password you have chosen. Passwords must be at least five characters long and cannot include any special characters.

When you are at the Install Additional Components page, you can install some, all, or none of the components. If you choose to install none of the components at this time, you can add components from the NOWS Admin GUI later. The components have been grouped together with similar software types for easy location, often appearing in multiple locations.

8 Do one of the following:

- ◆ If you choose not to install components, click *Next*, and then on the Install Additional Components page, click *Next* again. On the Component Installation page, click *Install*. Click *Continue to Administration*. To log out, click the red button next to *You are logged in as*.

- ◆ If you do choose to install components now, select components on the Install Additional Components page. Click *Continue to Administration* to begin the configuration of your chosen NOWS components.

2.1.3 Configuration and Basic Administration

This section assumes that you have completed Section 2.1.1, "Beginning the Installation," on page 19 and Section 2.1.2, "Web Installation and Configuration," on page 20.

1 Log in to the administration page with the username of sbsadmin and the password you chose during the installation.

At the administration console, you can install, uninstall, configure, and update components. Help links are also here to assist you with questions about your new NOWS server.

From this page, you can also manage your server, environment, and users. If you grant users access to the NOWS SBE administration console with user privileges, they can get needed resources for their desktop computers.

For more information on using the administration page, see Section 2.2, "Administering the Novell Open Workgroup Suite Small Business Edition," on page 22.

2 To log out, click the red button in the upper left-hand corner of the Web page next to *You are logged in as*. This logs you out of the session and brings you back to the login screen.

2.2 Administering the Novell Open Workgroup Suite Small Business Edition

The NOWS SBE 2.0 administration page gives you the tools to install, uninstall, configure, and update components. In addition, it provides you with Help links to assist you with any questions you might have about your new NOWS SBE server.

2.2.1 Components Panel

The *Components* panel lists the following menu items:

- *Products and Services* enables you to view installed components.
- *Add/Remove* enables you to install and uninstall components.
- *Desktop Downloads* enables you and your business community to install products and services on their individual computers.
- *Help Links* provides access to documentation.
- *Management Links* provides access to management consoles used to manage your Novell Open Workgroup Suite Small Business Edition 2.0 environment.

Products and Services

When you click *Products and Services,* you can view additional information on installed components. Under *Select Component*, click the component's name to populate *Desktop Downloads*, *Help Links*, *Management Links*, and *Remote Administration*.

Add/Remove

This link allows you to add and remove components. To view all components, click *All* under *Available Software*. You can also view components in the following categories: *Backup Restore and Recovery*, *Business Applications*, *Collaboration Groupware and Messaging, File Print and Fax*, *Security Management*, and *Systems Management*. To uninstall a component, click *Uninstall* under *Installed Software*.

Desktop Downloads

This link allows you to search for desktop applications that can be installed on user desktops. Under *Choose Operating System*, specify the appropriate operating system. Under *Choose Component*, select the component you are searching for. You can also specify a keyword for your search. For a list of available components, see Section 1.3, "Product Components," on page 12.

Help Links

Click *Help Links* to view additional links to documentation sites. Under *Choose Component*, specify a component. You can also specify a keyword for your search.

Management Links

Click *Management Links* to view helpful management links. Under *Filter Component*, specify the desired component. You can also specify a keyword for your search.

2.2.2 Tasks Panel

Manage License Keys

The license key for your copy of Novell Open Workgroup Suite Small Business Edition 2.0 is saved here.

To update your key or add a key for the first time, specify your e-mail address and current license key, then click *Validate Key*.

Upload Packages

To receive component downloads and updates, or to add an SBU file, click *NOWS SBE Components*, *Third-Party Components*, or *Upload*.

To add a new update package, browse for the desired package, then click *Start Upload*.

NOTE: Updates should be done only through the administrative interface.

Remote Administration

Manage remote access and desktop downloads here.

View Logs

Manage and view users and groups here.

Set Language

Specify the language for the NOWS SBE 2.0 administration console.

2.2.3 Basic View Panel

Normal users see this panel after users log in to eDirectory. Only non-privileged user downloads are found here. This page can help in assisting your end users with desktop download questions.

2.2.4 Updates Panel

Novell Open Workgroup Suite Small Business Edition 2.0 administration server updates are available at the *Updates* panel. Click *Check now* to check for updates for all components.

NOWS SBE System

Use this menu panel to check for recent system updates, including partches.

NOWS SBE Components

Use this menu panel to check for recent updates for Novell components.

Third-Party Components

Use this menu panel to check for component updates from third-party clients.

2.3 Configuring Components

Use the components interface to add components to or remove components from your server. Under *Components*, select *Add/Remove*. Under *Available Software*, click *All*. A list of possible component installations appears. To install a component, click *Install* for that component.

IMPORTANT: You must begin your component download with eDirectory and iManager. These two software components help you to manage many of the remaining components.

Directory Services (eDirectory)

3

To start the eDirectory™ component install, click *Add/Remove* under *Components*, then click *All* and select eDirectory. Finally, decide which installation type you want to use:

- ◆ **Basic:** Installs a new eDirectory tree.
- ◆ **Advanced - New Tree:** Installs a new eDirectory tree with more options.
- ◆ **Advanced - Existing Tree:** Installs this server into an existing eDirectory tree.
- ◆ **Advanced - Use Remote Tree:** Use this option when there is already an eDirectory installed on a dedicated server and you want components that depend on eDirectory to point to the existing tree.

3.1 Installing eDirectory Basic

This option installs a new eDirectory tree on your server with default options.

1. In the *Components* panel of the NOWS SBE administration page, click *Add/Remove*, then click *All* in the Add/Remove console, then click *Install* in the eDirectory panel.

2. A Recommended Components page appears. Read it and click *Continue.*

3. Select *Basic* installation, then click *Next*.

4. Specify a name for the new eDirectory tree. Do not use special characters when naming your tree.

5. Specify an organization name for your eDirectory.

   This will be the name of the eDirectory container that the server is installed into. Do not use special characters when specifying your organization name.

6. Review the settings. To make changes, click the *Back* button. To proceed with the installation, click *Next*. Wait for the eDirectory files to unpack.

7. Basic eDirectory installation is now complete. Click *Finish* to return to the available software page. eDirectory is now listed on the installed software list and can be launched from the eDirectory administration link.

3.2 Installing eDirectory Advanced - New Tree

This option installs a new eDirectory tree on your server and allows you to specify many of the parameters, such as server context and LDAP ports.

1. In the *Components* panel of the NOWS SBE administration page, click *Add/Remove*, then click *All* in the Add/Remove panel, then click *Install* in the eDirectory panel.

2 A Recommended Components page appears. Read it and click *Continue*.

3 Click *Advanced-New Tree*, then click *Next*.

4 Specify the eDirectory tree name. Do not use special characters when specifying your tree name.

5 Specify your organization name. This will be the name of the eDirectory container that the server is installed into. Do not use special characters when specifying your organization name.

6 Specify your administrative information. Do not use special characters when specifying your password.

- **Admin Password:** Password of the eDirectory administrator user.
- **Admin Password Confirm:** Retype the password for the eDirectory administrator user.
- **SBS Admin Password:** The password for the SBS administrator user.
- **SBS Admin Password Confirm:** Retype the password for the SBS administrator user.

7 Specify the advanced settings for your server. Do not use special characters, except for hyphens, when specifying the server name.

- **Server Name:** Specify the name of the server you are adding to the tree.
- **Server Context:** Specify the server context. The server will be added to the tree in the specified context.
- **Path for DIB:** Specify the directory path where the database files are to be stored.
- **LDAP Port:** Specify the TCP port number on the LDAP server, such as 389. Fill in the field only if you know the correct information; otherwise, leave it blank.
- **Secure LDAP Port:** Specify the secure port number on the LDAP server, such as 636. Fill in the field only if you know the correct information; otherwise, leave it blank.
- **HTTP Port:** Specify the HTTP clear port number, such as 8028. Fill in this field only if you know the correct information; otherwise, leave it blank.
- **HTTPS Port:** Specify the HTTP secure port number, such as 8030. Fill in this field only if you know the correct information; otherwise, leave it blank.

8 Specify NCP settings if you want to enable access to NCP™ volumes via the Novell Client™ or other NCP-aware utilities.

- **NCP Support:** Enables NCP support on native Linux file systems (not NSS).
- **Name for Default NCP Volume:** If NCP support is enabled, a volume with this name is created.
- **NCP Volume Mount Point:** Specify the location on the file system where the NCP volume will reside if NCP support is enabled.

9 Review the settings. To make changes, edit the XMPL text directly to specify additional advanced settings.

10 To proceed with the installation, click *Next*. Wait for the eDirectory files to unpack.

11 The Advanced eDirectory - New Tree install is now complete. Click *Finish* to return to the available software page. eDirectory is now listed on the installed software list.

3.3 Installing eDirectory Advanced - Existing Tree

1 In the *Components* panel of the NOWS SBE administration page, click *Add/Remove*, click *All* in the *Add/Remove* panel, then click *Install* in the eDirectory panel.

2 A Recommended Components page appears. Read it and click *Continue.*

3 To proceed with the Advanced installation, click *Advanced - Existing Tree*, then click *Next*.

4 Specify existing tree information.

- **Tree Name:** Specify the name of your existing eDirectory tree.

- **IP Address of Existing Server:** Specify the IP address of the server that is already hosting the tree.

5 Specify the organization name.

6 Specify your administrative information. Do not use special characters when specifying your password.

- **Admin Password:** Password of the eDirectory administrator user.

- **Admin Password Confirm:** Retype the password for the eDirectory administrator user.

- **SBS Admin Password:** The password for the SBS administrator user.

- **SBS Admin Password Confirm:** Retype the password for the SBS administrator user.

7 Specify the advanced settings for your server. Do not use special characters, except for hyphens, when specifying the server name.

- **Server Name:** Specify the name of the server you are adding to the tree.

- **Server Context:** Specify the server context. The server will be added to the tree in the specified context.

- **Path for DIB:** Specify the directory path where the database files are to be stored.

- **LDAP Port:** Specify the TCP port number on the LDAP server, such as 389. Fill in the field only if you know the correct information; otherwise, leave it blank.

- **Secure LDAP Port:** Specify the secure port number on the LDAP server, such as 636. Fill in the field only if you know the correct information; otherwise, leave it blank.

- **HTTP Port:** Specify the HTTP clear port number, such as 8028. Fill in this field only if you know the correct information; otherwise, leave it blank.

- **HTTPS Port:** Specify the HTTP secure port number, such as 8030. Fill in this field only if you know the correct information; otherwise, leave it blank.

8 Specify additional advanced settings for your server, such as Time Server IP. Do not use special characters, except for hyphens, when specifying the server name.

- **Admin FDN:** The name of the user object that has supervisory rights to add the server.

- **Port to Bind:** The default port on which a particular instance should listen.

- **Existing port to bind:** The port on which the server that is already hosting the tree accepts connections.

- **Time Server IP:** Synchronizes your local server with the server that is hosting the tree.

- **Clear Text Passwords:** Enables clear text passwords for LDAP objects.

9 Specify NCP settings if you want to enable access to NCP volumes via the Novell Client or other NCP aware utilities.

   ◆ **NCP Support:** Enables NCP support on top native Linux file systems (not NSS)

   ◆ **Name for Default NCP Volume:** If NCP support is enabled, a volume with this name is created.

   ◆ **NCP Volume Mount Point:** Specify the location on the file system where the NCP volume will reside if NCP support is enabled.

10 Review the settings. To make changes, edit the XMPL text directly to specify additional advanced settings. To proceed with the installation, click *Next*.

11 The Advanced eDirectory - Existing Tree install is complete. Click *Finish* to return to the available software page. eDirectory is now listed on the installed software list.

3.4 Installing eDirectory Advanced - Remote Tree

1 In the *Components* panel of the NOWS SBE administration page, click *Add/Remove*, then click *All* in the *Add/Remove* panel, then click *Install* in the eDirectory panel.

2 A Recommended Components page appears. Read it and click *Continue*.

3 To proceed with the Advanced installation, click *Advanced - Use Remote Tree*, then click *Next*.

4 Specify existing tree information.

   ◆ **Tree Name:** Specify the name of your existing eDirectory tree.

   ◆ **IP Address:** Specify the IP address of the server that is already hosting the tree.

5 Specify the organization name.

6 Specify your administrative user information. Do not use special characters when specifying your password.

   ◆ **Admin Password:** Password of the eDirectory administrator user.

   ◆ **Admin Password Confirm** Retype the password for the eDirectory administrator user.

   ◆ **SBS Admin Username:** The username for the SBS administration user.

   ◆ **SBS Admin Password:** The password for the SBS administrator user.

   ◆ **SBS Admin Password Confirm:** Retype the password for the SBS administrator user.

7 Specify LDAP settings. Do not use special characters, except for hyphens, when specifying the server name.

   ◆ **LDAP Port:** Specify the TCP port number on the LDAP server, such as 389. Fill in the field only if you know the correct information; otherwise, leave it blank.

   ◆ **Secure LDAP Port:** Specify the secure port number on the LDAP server, such as 636. Fill in the field only if you know the correct information; otherwise, leave it blank.

8 Review the settings. To make changes, edit the XMPL text directly to specify additional advanced settings. To proceed with the installation, click *Next*.

9 The Advanced eDirectory - Remote Tree install is now complete. Click *Finish* to return to the available software page. eDirectory is now listed on the installed software list.

3.5 Post-Installation

eDirectory is managed with iManager, which is accessed through the *Add/Remove* link in the *Components* panel.

NOTE: To uninstall eDirectory™, you must first uninstall iManager.

3.5.1 Desktop Download

1 Log in to the NOWS SBE Administration console.

2 Click *Products and Services*.

3 On the *Select Component* panel, click *Directory Services (eDirectory)*.

4 Under *Desktop Downloads*, click the appropriate operating system link.

5 To save the install to your computer, click *Save to Disk*, then click *OK*.

6 After the download is complete, click the new `ISO` file on your desktop, then burn this to a blank CD.

7 Put the CD into the workstation that you want to install into.

8 Double-click the `ncl_install` file.

9 Select *Run in Terminal*.

3.5.2 ConsoleOne

ConsoleOne® is an alternate tool for managing eDirectory. It is also provided if a needed task is not available in iManager.

ConsoleOne resides on the server in the `/usr/ConsoleOne/bin` directory.

1 Click the tree icon to log in to ConsoleOne.

3.5.3 Helpful Links

For additional information on administering eDirectory, see the *eDirectory Administration Guide* (http://www.novell.com/documentation/edir88/index.html).

For additional information on administering eDirectory with ConsoleOne, see the ConsoleOne online documentation (http://www.novell.com/documentation/consol13/).

For additional information on the Novell Windows Client, see the Novell Windows Client online documentation (http://www.novell.com/products/clients/windows/xp2000/overview.html).

Management Tools (iManager)

<div style="text-align: right; font-size: 3em;">4</div>

iManager is the administration interface for eDirectory™ and many other Novell services. This is a role-based tool for network and systems management in your environment.

4.1 Installing iManager Basic

1 Select Management Tools (iManager) under *Add/Remove*, then click *Install*.

2 Click *Basic,* then click *Next*.

3 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

4 The Basic iManager installation is now complete. Click *Finish* to return to the available software page. iManager is now listed on the installed software list and can be launched from the *iManager* administration link.

4.2 Installing iManager Advanced

1 Select Management Tools (iManager) under *Available Software*, then click *Install*.

2 Click *Advanced*, then click *Next*.

3 Specify the tree iManager should connect to.

- **Admin DN:** The admin DN formatted with dots, for example: cn=admin.o=mycompany.
- **Tree Name:** The name of the tree to connect to.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The Advanced iManager install is now complete. To proceed to the available software page, click *Finish*. iManager is now listed on the installed software list and can be launched from the *iManager* administration link.

4.3 Post-Installation

4.3.1 iManager Features

iManager is launched with rights to perform specific tasks from the following links (if the required component is installed). Select *Management Tools (iManager)* under *Select Component*, then select *iManager Administration* under *Admistrative Console*.

- ◆ *Users and Groups*
- ◆ *iFolder Administration*
- ◆ *eDirectory Administration*
- ◆ *iPrint Administration*
- ◆ *Samba Administration*

iManager can be launched with all available roles and tasks from the *iManager Administration* link; however, you must authenticate as an administrator to access all available tasks.

iManager can also be launched directly from the iManager Web site (http://www.novell.com/documentation/imanager27/index.html).

4.3.2 Creating Users and Groups, and Designating the NOWS SBE Administrator

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Component*, click *Management Tools (iManager),* then click *iManager Administration*. This launches the iManager login page.

4 Log in to iManager with your network admin login, for example cn= admin., o= localdomain.

5 After login, you are taken to the iManager console. Follow the links to create users, groups, and designate the NOWS SBE Administrator. A NOWS SBE Administrator has administrator access for all NOWS SBE components.

For more information on how to designate users, see the iManager Web Site (http://www.novell.com/documentation/imanager27/imanager_admin_27/index.html?page=/documentation/imanager27/imanager_admin_27/data/b8im2s7.html).

4.3.3 Helpful Links

For additional administrator information, see the iManager Administration Guide Web site (http://www.novell.com/documentation/imanager27/imanager_admin_27/index.html?page=/documentation/imanager27/imanager_admin_27/data/hk42s9ot.html).

Personal File Backup (iFolder)

5

Novell® iFolder™ is a simple and secure storage solution that enables you to back up, access, and manage your personal files from anywhere, at any time. After you have installed iFolder, you simply save your files locally as you have always done, and iFolder automatically updates the files on your network server and delivers them to the other machines you use.

5.1 Installing iFolder Basic

1 Click *Add/Remove,* click *All*, select *Personal File Backup (iFolder)* from *Available Software*, then click *Install*.

2 Click *Basic*, then click *Next*.

3 Specify your iFolder server name.

  ◆ **System Name:** The name assigned to the iFolder sever.

  ◆ **System Description:** An optional description of this iFolder server.

4 Review the settings. If you need to make a change, click *Back*. To proceed with the installation, click *Next*.

5 The iFolder install is complete. Click *Finish* to proceed to the available software page. iFolder is now listed on the installed software list and can be administered from the *iFolder* administration link.

5.2 Installing iFolder Advanced

1 Click *Add/Remove*, click *All*, select *Personal File Backup (iFolder)* from *Available Software*, then click *Install*.

2 Select *Advanced*, then click *Next*.

3 Specify your iFolder server name.

  ◆ **System Name:** The name assigned to the iFolder sever.

  ◆ **System Description:** An optional description of this iFolder server.

4 Specify the settings for your LDAP services. LDAP is used for user authentication and authorization.

  ◆ **LDAP URL:** The LDAP URL is the server address that iFolder authenticates against.

  ◆ **LDAP Admin DN:** The admin user DN for the LDAP server. For example: cn= admin, o=treename.

  ◆ **LDAP Proxy:** Where iFolder should create its proxy user in the directory.

  ◆ **System Admin DN:** The distinguished name for an iFolder administrator user. This user will be created if it does not exist.

5 Click *Next* to continue your iFolder install.

6 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

7 The iFolder installation is now complete. Click *Finish* to proceed to available software page. iFolder is now listed on the installed software list and can be administered from the *iFolder* administration link.

5.3 Post-Installation

- Section 5.3.1, "iFolder Web Client Desktop Download," on page 34
- Section 5.3.2, "iFolder Administration Desktop Download," on page 34

5.3.1 iFolder Web Client Desktop Download

1 Log in to the NOWS SBE console.

2 Select *Products and Services*.

3 Under *Select Component*, click *Personal File Backup (iFolder)*.

4 Under *Administrative Console*, click *iFolder Client*. You are directed to the iFolder Web Client login page.

5 Specify the username and password, then click *Log In*.

5.3.2 iFolder Administration Desktop Download

1 Log in to the NOWS SBE console.

2 Select *Products and Services*.

3 Under *Select Component*, click *Personal File Backup (iFolder)*.

4 Under *Administrative Console*, click *iFolder Administration*. You are directed to the iFolder Administration page.

For additional iFolder information, see the iFolder online documentation (http://www.novell.com/documentation/ifolder3/index.html?page=/documentation/ifolder3/user/data/prerequisites.html).

Network Backup (Amanda)

6

Amanda, or Advanced Maryland Automatic Network Disk Archiver, is an archiving tool that backs up data residing on a single server, or multiple computers on a network, to a tape-based or disk-based storage system. Amanda uses native dump and GNU tar facilities, and it can back up a large number of workstations and servers running various versions of Linux, UNIX, or Microsoft Windows operating systems.

For more information, see the Amanda documentation site (http://www.amanda.org/docs/amanda-docs.html).

6.1 Installing Amanda Basic

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to Network Backup (Amanda) and click *Install*.

2 Select *Hard-Disk Backup (basic),* then click *Next*.

3 Specify your network backup configurations.

- **Mail To:** A comma-separated list of recipients for e-mail reports.
- **Organization:** Title of backup reports.
- **Days to Backup:** Select the days backups will run.
- **Hour to Run:** Select the hour that backups will run.

4 Specify your disk backup.

- **Maximum Backup Size (GB):** The size of the virtual backup tapes in gigabytes. This is the maximum amount of data that can be backed up during each cycle.
- **Number of Backups to Keep:** This is the total number of backups to store at one time.
- **Path to Store Backups:** The Linux path to your storage device.

5 Review the settings of the installation. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The Amanda Basic installation is now complete. Click *Finish* to proceed to the installed software page. Amanda is now listed on the installed software list and can be administered from the *Amanda* administration link.

6.2 Installing Amanda Advanced

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to Network Backup (Amanda) and click *Install*.

2 Select *Tape Backup (Advanced)*, then click *Next*.

3 Specify your network backup configurations for Amanda.

- **Mail To:** A comma-separated list of recipients for e-mail reports.

- **Organization:** Title of backup reports.
- **Days to Backup:** Select the days the backups will run.
- **Hour to Run:** Select the hour that backups will run.

4 Specify the properties for your particular tape type. You can use the Amanda Web site (http://amanda.sourceforge.net/cgi-bin/fom?file=46) as a resource.

- **Tape Device:** The path to the local tape device.
- **Tape Length (mbytes):** The Filemark in megabytes of your tape media.
- **Tape Filemark (kbytes):** The Filemark in kilobytes of your tape media.
- **Tape Speed (kbytes):** The Filemark in kilobytes of your tape media.
- **Tape Count:** The number of tapes in your Filemark in kilobytes of your tape media.

5 Review the settings of the installation. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The Amanda Advanced installation is now complete. Click *Finish* to proceed to the available software page. Amanda is now listed on the installed software list and can be administered from the *Amanda* administration link.

6.3 Post-Installation

6.3.1 Labeling Tapes

Do this after installation of Amanda in tape mode.

1 `su` to user amandabackup.

2 Write `DailySet1-`*XX* on the tape, where *XX* is the number of the tape.

3 Load the tape into the drive.

4 Run the command `amlabel DailySet DailySet1-XX`.

You need to change tapes manually before backup time. Amanda does not overwrite the wrong tape, so the appropriate tape must be inserted prior to the selected backup time.

If you are using a tape changer, you need to set the tape changer manually. Setting up the tape changer is very specific to the device. For more information, see the Amanda manual (http://www.amanda.org/docs/tapechangers.html).

6.3.2 Backup Scheduling and Configuration

For more information about administering software, see the Amanda documentation site (http://www.amanda.org/docs/install.html#id325444).

OpenOffice.org 7

OpenOffice.org is a full-featured office suite. It includes word processing, presentation, spreadsheet, and database applications.

7.1 Installing OpenOffice.org Basic

Installation for OpenOffice.org copies the installation files to the server, making them available for easy client access.

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to OpenOffice and click *Install*.

2 Select *Basic Install Only,* then click *Next*.

3 Review settings, then proceed with the installation by clicking *Next*.

4 The OpenOffice.org installation is now complete. Click *Finish* to return to the available software page. OpenOffice.org is now listed on the installed software list and shows up as an available application in the *Desktop Downloads* panel for your users.

7.2 Post-Installation

OpenOffice.org is also now available from Desktop Downloads for installation to a Windows client.

NOTE: There is no desktop download for the Linux client, because SUSE® Linux Enterprise Desktop (SLED) includes OpenOffice.org.

For additional information regarding OpenOffice.org installation, see the OpenOffice online documentation (http://documentation.openoffice.org/).

E-Mail Collaboration and Groupware (GroupWise)

8

GroupWise® has a set of tools that keep your employees connected to clients and each other. The system comes with e-mail, calendaring, and instant messaging to set up according to your company needs.

IMPORTANT: If you want to install Groupwise and MailScanner on the same server, use the *Add/Remove* function to add MailScanner only after Groupwise is installed. Adding these two applications simultaneously in the initial installer might cause the Groupwise install to fail.

For additional GroupWise information, see the GroupWise documentation Web site (http://www.novell.com/documentation/gw7/index.html).

8.1 Installing GroupWise Basic

1 Click *Install* under *Available Software*.

2 Select *Basic*, then click *Next*.

3 Select your GroupWise configuration items.

- **Base GroupWise System:** The basic GroupWise system includes the mail server with thick client support.
- **Internet Agent:** Required for sending e-mail.
- **Web Access:** Web-based mail client.
- **Monitor:** Administrative monitoring of server activity.
- **Messenger:** Instant messenger server.

4 Specify your GroupWise LDAP settings.

- **Tree Name:** Specify a name for your eDirectory™ tree.
- **IP Address:** Specify the IP address for your eDirectory tree.
- **Tree Context:** Specify a name for your eDirectory domain.
- **Admin User:** Specify the name of your admin user.
- **Admin Password:** Specify a password for your admin user.
- **gwSysName:** Specify the name of your GroupWise system.

5 Specify your Internet Domain. For example: novell.com.

6 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

7 The GroupWise basic install is now complete. Click *Finish* to proceed to the Available Software page. GroupWise is now listed on the installed software list.

8.2 Installing Groupwise Advanced

1 Click *Install* under *Available Software*.

2 Select *Advanced*, then click *Next*.

3 Select your GroupWise configuration items.

- **Base GroupWise System:** The base GroupWise system includes the mail server with thick client support.
- **Internet Agent:** Required for Internet e-mail addresses.
- **Web Access:** Web-based mail client.
- **Monitor:** Administrative monitoring of server activity.
- **Messenger:** Instant messenger server.

4 Specify your GroupWise LDAP settings.

- **Tree Name:** Specify a name for your eDirectory tree.
- **IP Address:** Specify the IP address for your eDirectory tree.
- **Tree Context:** Specify a name for your eDirectory domain.
- **Admin User:** Specify the name of your admin user.
- **Admin Password:** Specify a password for your admin user.
- **gwSysName:** Specify the name of your GroupWise system.

5 Specify your Internet Domain. For example: novell.com.

6 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

7 The GroupWise advanced install is now complete. Click *Finish* to proceed to the Available Software page. GroupWise is now listed on the installed software list. The GroupWise client now appears in the *Desktop Downloads* panel for end users.

8.3 Post-Installation

8.3.1 GroupWise Client Desktop Download

1 Log in to the NOWS SBE console.

2 Select *Products and Services*.

3 Under *Select Component*, click *E-Mail and Collaboration (GroupWise)*.

4 Under *Desktop Downloads*, click the *GroupWise Client* appropriate to your operating system.

5 To save the install file to your computer, click *Save to Disk*, then click *OK*.

6 After download is complete, click the file ending in `.gz` on your desktop, then click *Extract* when prompted. The GroupWise Client Software component is now downloaded to your desktop.

8.3.2 GroupWise Instant Messenger Desktop Download

1 Log in to the NOWS SBE console.

2 Select *Products and Services*.

3 Under *Select Component*, click *E-Mail and Collaboration (GroupWise)*.

4 Under *Desktop Downloads*, click *Groupwise Messenger*.

5 To save the install file to your computer, click *Save to Disk*, then click *OK*.

6 After download is complete, click the file ending in `.gz` on your desktop, then click *Extract* when prompted. The Instant Messenger Software component is now downloaded to your desktop.

8.3.3 Installing ConsoleOne for Advanced Administrative Tasks

GroupWise is administered by using ConsoleOne®, a Java*-based tool for managing your network and its resources. When you create your GroupWise system, GroupWise snap-ins are added to your ConsoleOne installation and GroupWise objects are created in Novell® eDirectory. As you manage your GroupWise system, you use ConsoleOne to create additional GroupWise objects, modify GroupWise object properties, and so on.

NOTE: Because the GroupWise snap-ins to ConsoleOne are required in order to work with GroupWise objects, you cannot use other network management tools, such as Novell iManager, to administer your GroupWise system. Also, you should not use older network management tools, such as NetWare® Administrator, to administer your GroupWise system, unless your GroupWise system includes legacy gateways that require such tools to administer the corresponding Gateway objects and their properties.

Because GroupWise is a cross-platform product, you might have components of your GroupWise system located on NetWare servers, Linux servers, and Windows servers. You can run ConsoleOne on Windows or Linux to manage GroupWise domains and post offices located on any of these platforms.

For more information, follow these links:

- ConsoleOne on Windows (http://www.novell.com/documentation/gw7/gw7_admin/ index.html?page=/documentation/gw7/gw7_admin/data/bwmb48w.html)
- ConsoleOne on Linux (//www.novell.com/documentation/gw7/gw7_admin/index.html?page=/ documentation/gw7/gw7_admin/data/bwmb48w.html)
- ConsoleOne in a Multi-Platform Environment (http://www.novell.com/documentation/gw7/ gw7_admin/index.html?page=/documentation/gw7/gw7_admin/data/bwmb48w.html)

8.3.4 Configuring WebAccess

During setup, you are given the opportunity to assign the Internet Agent a different port (26) so that GroupWise and MailScanner do not conflict. Incoming mail from the Internet to the GroupWise system is then accepted by MailScanner on port 25 (SMRP's default), scanned, and delivered to the Internet Agent, which accepts non-standard mail on port 26.

For directions on component configuration, see the GroupWise Administration Guide Web site (http://www.novell.com/documentation/gw7/gw7_userweb/data/front_page.html).

8.3.5 Using GroupWise Monitor

For administrative information on using the GroupWise Monitor, see the GroupWise Documentation Web site (http://www.novell.com/documentation/gw7/gw7_admin/index.html?page=/documentation/gw7/gw7_admin/data/a7q51ga.html)

Print Services (iPrint)

9

iPrint extends print services securely across multiple networks and operating systems.

For more information, see the iPrint online documentation (http://www.novell.com/documentation/oes2/print-services.html#print-services).

- Section 9.1, "Installing iPrint," on page 43
- Section 9.2, "Post-Installation," on page 43

IMPORTANT: Both iPrint and CUPS are print services that are compatible with NOWS SBE; however, they are not compatible with one another. You must choose only one of these services to install.

9.1 Installing iPrint

NOTE: There is no Advanced Install option for iPrint.

1 Click *Add/Remove*, then select *All*. Under *Available Software*, scroll down to *Print Services (iPrint)* and click *Install*.

2 *Basic* is preselected, so click *Next*.

3 Review the settings.

4 iPrint installation is now complete. Click *Finish* to proceed to the available software page. iPrint is now listed on the installed software list and can be administered from the *iPrint* administration link.

9.2 Post-Installation

- Section 9.2.1, "Creating a Driver Store," on page 43
- Section 9.2.2, "Creating a Print Manager," on page 44
- Section 9.2.3, "Creating a Printer," on page 44
- Section 9.2.4, "Installing Printer from /ipp and Print," on page 44

9.2.1 Creating a Driver Store

You need only one Driver Store for your iPrint system; however, depending on your network setup, you can add additional Driver Stores. A Driver Store must be created in order to create a Print Manager.

1 In iManager, click *iPrint > Create Driver Store*.

2 Fill in the fields.

Click *Help* for explanations about the fields.

3 Click *OK*.

After the Driver Store is created, the daemon is loaded on the server, and you can start uploading drivers.

9.2.2 Creating a Print Manager

You need to create at least one Print Manager for your print system; however, depending on your network setup, you can create additional Print Managers, for example, across a WAN link. The Print Manager must be running in order to create printers.

NOTE: The Print Manager creates a URL for each printer based on the print manager configuration. When you create the print manager, you can specify an IP address or DNS name for the iPrint Service. You should always use a DNS name because using an IP address causes users to delete and reinstall printers if the IP address changes.

---

1 In iManager, click *iPrint > Create Print Manager*.

2 Fill in the fields. Click the help for explanations about the fields.

3 Leave the *Start Print Manager after Creation* check box checked.

If you do not do this, you must start the Print Manager by using *Manage Print Manager > Manager Control* in iManager or entering `/etc/init.d./novell-ipsmd start` at a command prompt.

4 Click *OK*.

After the Driver Store is created, the daemon is loaded on the server and you can start adding printer drivers.

9.2.3 Creating a Printer

Before you can create a printer, you must first create a Print Manager on your server.

1 In iManager, click *iPrint > Create Printer*.

2 Follow the prompts and fill in the fields. Click the help for explanations about the fields.

3 Click *Next*, then select the drivers for this printer.

If the printer drivers for this printer are not listed, you can still create the printer. After the printer is created, add the printer drivers to the Driver Store and then associate the drivers to the printer by clicking *Manage Printer > Drivers*.

4 Click *Next* to create the printer.

9.2.4 Installing Printer from /ipp and Print

To install and distribute iPrint printers, see Novell iPrint documentation (http://www.novell.com/documentation/oes2/iprint_lx/index.html?page=/documentation/oes2/iprint_lx/data/front.html).

Windows File and Print Sharing (Samba) 10

The Samba file and print sharing service for Windows enables you to configure your network with the security of Linux as well as to access your Linux servers via Windows workstations.

For more information, see the Samba online documentation (http://www.novell.com/documentation/oes2/file_samba_cifs_lx/index.html?page=/documentation/oes2/file_samba_cifs_lx/data/bookinfo.html#bookinfo).

- Section 10.1, "Installing Samba Basic," on page 45
- Section 10.2, "Installing Samba Advanced," on page 45
- Section 10.3, "Post-Installation," on page 46

10.1 Installing Samba Basic

1 Click *Install* under *Available Software*.

2 Click *Basic*, then click *Next*.

3 Specify basic configurations for your system.

- **Workgroup or Domain Name:** Specify the name of the workgroup that your server belongs to.

- **User Container:** Specify the base LDAP container for users. This is where the Samba domain object is stored.

- **Emulate NT4 Domain Controller:** Specify if Samba should act as the Primary Domain Controller (PDC).

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The Samba installation is now complete. Click *Finish* to proceed to the available software page. Samba is now listed on the installed software list and can be administered from the *Samba* administration link.

10.2 Installing Samba Advanced

1 Click *Install* under *Available Software*.

2 Click *Advanced*, then click *Next*.

3 Specify the LDAP configurations for your system.

- **NetBIOS Name:** Specify the NetBIOS name of the server. The first part of the host's DNS name can be used as the NetBIOS name.

- **Workgroup or Domain Name:** Specify the name of the workgroup or domain that your server belongs to or will host.

- **LDAP Admin Name:** Specify the name of the LDAP admin that has supervisory rights.

- **LDAP Context:** Specify the context of the admin user in your eDirectory™ tree.

- **LDAP Admin Password:** Specify the password for the LDAP admin whose distinguished name is specified above.

- **User Container:** Specify the base LDAP container for users. This is where the sambaDomain object is stored

- **Emulate NT4 Domain Controller:** Select this option to enable Samba to emulate an NT4 Primary Domain Controller.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The Samba advanced installation is now complete. Click *Finish* to proceed to the available software page. Samba is now listed on the installed software list and can be administered from the *Samba* administration link.

10.3 Post-Installation

- Section 10.3.1, "Creating a Samba User," on page 46
- Section 10.3.2, "Creating a Group," on page 46
- Section 10.3.3, "Assigning Passwords," on page 46
- Section 10.3.4, "Enabling Groups for LUM (Linux User Management)," on page 47
- Section 10.3.5, "Enabling a User for LUM," on page 47
- Section 10.3.6, "Enabling a User for Samba," on page 47
- Section 10.3.7, "Enabling a Domain," on page 47

10.3.1 Creating a Samba User

1 Open iManager.

2 In the Roles and Tasks menu on the left, click *Users > Create User*.

3 Specify user information, then click *OK*.

10.3.2 Creating a Group

1 In iManager, click *Groups > Create Group*.

2 Specify the group name and context. The context is the location in the eDirectory tree. The user should have the same context as the group.

3 Click *OK*.

10.3.3 Assigning Passwords

1 In iManager, click *Passwords > Password Policies*.

2 Click *Samba Default Password Policy*.

3 Click the *Policy Assignment* tab.

4 Click the *Object Selector* icon.

5 Assign the password policy to either the Organizational Unit that the user is in or assign it to the specific user object.

6 Click *OK*.

7 Click *Apply*.

10.3.4 Enabling Groups for LUM (Linux User Management)

1 In iManager, click *Linux User Management*, then click *Enable Groups for Linux*.

2 Click the *Object Selector* icon and choose the group that you want to enable for LUM.

3 Select *Linux-enable all users in these groups*, then click *Next*.

4 Click *Object Selector*, then locate your Linux Workstation object.

5 Click *OK*.

6 Click *Next*.

7 Click *Finish*, then click *OK*.

10.3.5 Enabling a User for LUM

1 In iManager, click *Linux User Management*, then click *Enable Users for Linux*.

2 Click the *Object Selector* icon and choose the user that you want to enable for LUM.

3 Click *OK*.

4 Click *Next*.

5 Specify the user's primary group.

6 Click *Next*.

7 Select *Linux Workstation*, then click *Next*.

8 Click *Finish*, then click *OK*.

10.3.6 Enabling a User for Samba

1 In iManager, click *Samba Management*, then click *Enable Linux User for Samba*.

2 To select a LUM user, click the *Object Selector* icon.

3 Select the user, then click *OK*.

4 To have the user authenticate to Samba through eDirectory, click *OK*. Otherwise, click *Cancel*.

5 Specify that Universal Password to be used for Samba login. Confirm the password, then click *OK*.

10.3.7 Enabling a Domain

Complete this procedure if you chose to set up this server as a Primary Domain Controller.

1 Log in to the NOWS SBE console.

2 Click *Products and Services*, then click *Windows File and Print Sharing (Samba)*.

3 Click the *Novell Samba Wiki* link under *Help Links*. Follow the directions from the Novell documentation site.

Fax Server (HylaFAX)

11

HylaFAX is the leading fax server for UNIX-like computer systems. It uses a client-server design and supports the sending and receiving of faxes and text pages on any scale from low to very high volumes, making use of large numbers of modems if necessary.

At this time, there is no advanced install for HylaFAX.

HylaFAX requires that Java is already installed. For additional information, see the Java Web site (http://java.sun.com).

For more information, see the HylaFAX documentation site (http://www.hylafax.org/content/How-To).

- Section 11.1, "Installing HylaFAX," on page 49
- Section 11.2, "Post-Installation," on page 50

11.1 Installing HylaFAX

1 Click *Add/Remove* under *Components*, click *All* under *Available Software*, then select *Fax Server (HylaFAX)*.

2 Click *Basic*, then click *Next*.

3 Specify the HylaFAX configuration settings.

- **Machine Type:** Select *Send and Receive* if you are using this machine to both send and receive faxes. Select *Send Only* if you do not have a dedicated phone line or only want to send faxes from your machine.
- **Fax Identification String:** This is the identification that is sent out with each Fax; a good choice would be your company name.
- **Country Code:** Country code of your fax server.
- **Area Code:** Area code of your fax server.
- **Long Distance Prefix:** Long-distance prefix for your fax server.
- **International Prefix:** The prefix you need for an international call.
- **Dial Out Prefix:** Specify a number here if the fax modem needs to specify a number to go outside of your internal phone network.

4 Specify the modem configurations.

- **Modem Device:** The TTY port of your fax modem is a serial port modem. It is probably something like /dev/ttyS1. If this is an internal or built-in modem, Linux modem drivers need to be configured.
- **Phone Number of the Fax-modem:** Phone number of the fax modem.

5 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The HylaFAX installation is now complete. Click *Finish* to proceed to the installed software page. HylaFAX is now listed on the installed software list and can be administered from the *HylaFAX* administration link.

11.2 Post-Installation

11.2.1 Desktop Download for Linux

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Component*, click *Fax Server (HylaFAX)*.

4 Under *Desktop Downloads and Linux*, click *JHylaFAX*.

5 Open a command prompt and enter `java -jar jhylafax-1.3.10-app.jar` to launch JHylaFAX.

11.2.2 Desktop Download for OS X and Windows

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Component*, click *Fax Server (HylaFAX)*.

4 Under *Desktop Downloads*, click *JHylaFAX* for OS X or Windows.

5 Follow download procedures to download JHylaFax to your desktop.

6 To launch JHylaFAX, click the *JHylaFAX* icon.

Anti-Virus (ClamAV)

12

Clam AntiVirus is an anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. It provides a number of utilities, including a flexible and scalable multi-threaded daemon, a command line scanner, and an advanced tool for automatic database updates. The core of the package is an anti-virus engine available in the form of a shared library.

For additional information, see the ClamAV documentation site (http://www.clamav.net/doc/latest/clamdoc.pdf).

12.1 Installing ClamAV Basic

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Anti-Virus (ClamAV)* and click *Install*.

2 Select *Basic*, then click *Next*.

3 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

4 The Basic ClamAV install is now complete. Click *Finish* to return to the available software page.

12.2 Installing ClamAV Advanced

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Anti-Virus (ClamAV)* and click *Install*.

2 Select *Advanced*, then click *Next*.

3 Select the security options most suitable for your business needs. By default, AntiVirus uses the most common recommended options. These options allow you to customize your installation.

- **Portable Executable Support:** PE stands for Portable Executable, which is an executable file format used in all 32-bit versions of Windows operating systems. This option allows ClamAV to perform a deeper analysis of executable files and it is also required for decompression of popular executable packers such as Petite.

- **Detect Broken Executables:** Select the check box to allow detection of broken executables.

- **Microsoft Office Document Scanner:** Select the check box to enable scanning of Microsoft Office document macros.

- **Clam Mail Scanner:** Select the check box to enable the internal e-mail scanner.

- **Clam Mail URL Scanner:** Select the check box to enable the downloading and scanning of e-mail that contains URLs.

- **Clam MS HTML Script Scanner:** Select the check box to enable HTML normalization and decryption of MS and Script Encoder code.

4 Set your scanner options for archival file support.

- **Clam Archive Max File Size:** Specify the maximum file size to scan.

- **Clam Archive Max Recursion:** Specify the Clam archive maximum compression ratio. Any file that has a compression ratio above this value is marked as a virus. A value of 0 disables this limit.
- **Clam Archive Max Files to Scan:** Specify the maximum number of files to scan within an archive. A value of 0 disables this limit.
- **Clam Archive Max Compression Ratio:** Specify the Clam compression ratio. Any file that has a compression ratio above this value is marked as a virus. A value of 0 disables this limit.
- **Clam Archive Limit Memory Usage:** Select the check box to enable a slower but more memory-efficient decompression algorithm. This only affects the bzip2 decompressor.
- **Clam Block Encrypted Archives:** Select the check box to mark encrypted archives as viruses.
- **Clam Archive Block Max:** Select the check box to mark archives as viruses when the archive max files, archive max file size, or archive max recursion limit is reached.

5 Click *Next* to continue.

6 Select the appropriate runtime parameters.

- **Clam Max Connection Queue Length:** Specify the maximum length for the queue of pending connections.
- **Clam Stream Max Length:** Specify that the Clam stream maximum length connection is closed when the data size limit is exceeded. The value should match your mail transport agent's (MTA) limit for a maximum attachment size.
- **Clam Max Threads:** Specify the maximum number of threads running at the same time.
- **Clam Data Read Timeout:** Specify the time in seconds to wait for data from a client socket before going to timeout.
- **Clam Idle Job Timeout:** Specify the time in seconds to wait for a new job before going into timeout.
- **Clam Max Directory Scan Recursion:** Specify the maximum depth to which directories are scanned.
- **Clam Self Check of Software:** Specify the time in seconds to perform internal sanity checks, such as database integrity and freshness.
- **Clam Run as User:** Run as a selected user (Clam must be started by `root`).
- **Clam Virus Event Command Execution:** Enable the execution of a command when a virus is found.
- **Clam Follow File Symlinks:** Select the check box to enable following of regular file symlinks.
- **Clam Follow Directory Symlinks:** Select the check box to enable following of directory symlinks.
- **Clam Allow Supplementary Groups:** Select the check box to allow the initialization of supplementary group access (Clam must be started by `root`).
- **Clam Exit if Out of Memory Condition Exists:** Select the check box to enable stopping the daemon when libclamav reports an out-of-memory condition.

7 Click *Next* to continue.

8 Select the appropriate network configuration.

- ◆ **Clam Path to Local Socket File:** Specify the path to a local socket file for the daemon to listen on.

- ◆ **Clam TCP Port Number:** Specify the TCP port address.

- ◆ **Clam IP Bind Address:** Specify the TCP address to bind to.

- ◆ **Clam Fix Stale Socket:** Select the check box to enable the removal of a stale socket after an unclean shutdown.

9 Click *Next* to continue.

10 Select the appropriate logging options.

- ◆ **Clam Log File Path:** Specify the full path of the log file. The log file must be writable for the user running the daemon.

- ◆ **Clam Log File Maximum Size:** Specify the maximum size of a log file. A value of 0 disables the limit. You can use modifiers to specify log size in megabytes (M or m) or kilobytes (K or k). To specify the size in bytes, do not use modifiers.

- ◆ **Clam Log Syslog Facility:** Specify the type of syslog message. Refer to `man syslog` for facility names.

- ◆ **Clam Log File Unlock:** Select the check box to disable log file locking. By default, the log file is locked for writing to protect against running ClamAV multiple times. If you want to run another ClamAV, copy the configuration file, change the Log File variable, and run the daemon with the -config-file option.

- ◆ **Clam Log Event Time:** Select the check box to enable an event's time to be logged.

- ◆ **Clam Log Event Messages to Syslog:** Select the check box to use the system logger. This can work together with LogFile.

- ◆ **Clam Verbose Logging:** Select the check box to enable verbose logging.

11 Click *Next* to continue.

12 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

13 The ClamAV advanced install is now complete. Click *Finish* to return to the available software page.

12.3 Post-Installation

- ◆ Section 12.3.1, "ClamAV Client Desktop Download," on page 53
- ◆ Section 12.3.2, "Scan Scheduling," on page 54
- ◆ Section 12.3.3, "Helpful Links," on page 54

12.3.1 ClamAV Client Desktop Download

The ClamAV client is now available for installing to Windows client components from *Desktop Downloads*. There is no desktop download for the Linux client, because SUSE® Linux Desktop (SLED) includes ClamAV.

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 In the *Select* Component panel, click *Anti-Virus (ClamAV)*.

4 Under *Desktop Downloads*, click *ClamAV Client for Windows*.

5 To save the install file to your computer, click *Save File to Disk*, then click *OK*.

6 After the download is complete, click the *clamAV.msi* file on your desktop. The ClamAV Client Software component is now downloaded to your desktop.

NOTE: During the client install, you have the option of updating your virus signatures online. It is recommended that you do so.

12.3.2 Scan Scheduling

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 In the *Select Component* panel, click *Anti-Virus (ClamAV)*.

4 Under *Administrative Console*, click *Scan Scheduling*.

5 Select the days and times you want automatic virus scans to occur.

6 Click *Save*.

12.3.3 Helpful Links

See also scan scheduling information (http://www.clamav.net/).

Anti-Spam (MailScanner)

13

MailScanner scans all e-mail for viruses, spam, and attacks against your network's security. After the install is complete, no additional configuration is necessary. Be sure to install GroupWise® and ClamAV before installing MailScanner.

IMPORTANT: If you want to install Groupwise and MailScanner on the same server, use the *Add/Remove* function to add MailScanner only after Groupwise is installed. Adding these two applications simultaneously at the initial installation might cause the Groupwise install to fail.

For additional information, see the MailScanner documentation site (http://www.nk.ca/mailscanner/docs.html).

13.1 Installing MailScanner Basic

Use the basic install when GroupWise is already installed on the same server as MailScanner.

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Anti-Spam (MailScanner)* and click *Install*.

2 Click *Basic*, then click *Next*.

3 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

4 The MailScanner basic installation is complete. Click *Finish* to proceed to the available software page. MailScanner is now listed on the installed software list and can be administered from the *MailScanner* administration link.

13.2 Installing MailScanner Advanced

Use the advanced install when GroupWise is installed on a server separate from MailScanner.

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Anti-Spam (MailScanner)* and click *Install*.

2 Select *Advanced*, then click *Next*.

3 Specify SMTP Relay Host settings, then click *Next*.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The MailScanner advanced installation is complete. Click *Finish* to proceed to the available software page. MailScanner is now listed on the installed software list and can be administered from the *MailScanner* administration link.

13.3 Post-Installation

13.3.1 Helpful Links

For information on using MailScanner with GroupWise, see the MailScanner documentation site (http://www.nk.ca/mailscanner/docs.html).

Firewall (IPTables)

14

A firewall is a hardware or software device that is configured to permit, deny, or proxy data through a computer network that has different levels of trust.

14.1 Installing IPTables Basic

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Firewwall (IPTables)* and click *Install*.

2 Select *Basic*, then click *Next*.

3 Specify your IPTable configurations.

- **External Interface:** The network interface connected to the Internet.

- **Internal Interface:** The internal network interface. If you are using NAT, it routes from the external interface to the internal interface.

- **NAT:** Network Address Translation shares the firewalled Internet connection with the network on the internal network interface. This is a must if you are using this server as your network firewall.

4 Review the settings. If you need to make a change, click *Back*. To proceed with the installation, click *Next*.

5 The firewall install is complete. Click *Finish* to proceed to the available software page. IPTables is now listed on the installed software list.

14.2 Installing IPTables Advanced

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to *Firewall (IPTables)* and click *Install*.

2 Click *Advanced*, then click *Next*.

3 Specify your firewall configurations.

- **External Interface:** The network interface connected to the Internet.

- **Internal Interface:** The internal network interface. If you are using NAT, it routes from the external interface to the internal interface.

- **NAT:** Network Address Translation shares the firewalled Internet connection with the network on the internal network interface. This is a must if you are using this server as your network firewall.

4 Specify your firewall port setup. See Section 1.5, "Planning for the NOWS SBE Install," on page 15 for typical ports that should be open for TCP and UDP.

- **Additional Ports (TCP):** Specify a comma-separated list of additional TCP ports to open on the firewall. Port ranges can be specified with a hyphen.

- **Additional Ports (UDP):** Specify a comma-separated list of additional UDP ports to open on the firewall. Port ranges can be specified with a hyphen.

5 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The firewall install is complete. Click *Finish* to proceed to the available software page. Firewall is now listed on the installed software list.

14.3 Post-Installation

Further firewall configuration is necessary to secure your system. Without further configuration, the administration interface is exposed to all other networked interfaces.

14.3.1 Firewall Configuration

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Component*, click *Firewall (IPTables)*.

4 Under *Administrative Console*, click *Firewall Administration*.

5 Specify the port configuration, then click *Save Changes*. You should disable outside access to this administration interface.

For additional recommendations for setting firewall rules, see the Firewall Documentation Web site (http://www.fwbuilder.org/pages/cd/contrdoc3.html).

VPN Server (OpenVPN) 15

OpenVPN is a Virtual Private Network (VPN) package for creating point-to-point encrypted tunnels between host computers. A VPN allows users to authenticate and connect securely to the internal business network. Although it is not required, you should install IPTables before installing OpenVPN.

For additional information, see the OpenVPN documentation site (http://openvpn.net/howto.html).

15.1 Installing OpenVPN Basic

1 Click *Add/Remove > All*, then scroll down to *VPN Server (OpenVPN)* and click *Install*.

2 Click *Basic*, then click *Next*.

3 The following network specifications are automatically configured:

- **Virtual IP Address Network:** Virtual IP network range (such as 192.168.1.0) to use for VPN network or automatic network detection.
- **VPN Network Mask:** Network mask (such as 225.225.255.0) of the VPN network or auto for automatic detection.
- **Allow VPN Clients Access to Internal Network:** This determines whether to allow VPN clients to route through the VPN server to the internal network or not.

4 Review the settings of the installation. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The OpenVPN installation is now complete. Click *Finish* to proceed to the available software page. OpenVPN is now listed on the installed software list.

15.2 Installing OpenVPN Advanced

1 Click *Add/Remove > All*, then scroll down to *VPN Server (OpenVPN)* and click *Install*.

2 Click *Advanced*, then click *Next*.

3 Specify the OpenVPN advanced network configuration.

- **Server IP Address for VPN Interface:** The IP address to be set to the assigned address of the interface that will be accepting VPN connections. If a system has multiple network interfaces, only one of them can be used for the VPN server.
- **Virtual IP Address Network:** Virtual IP network range (such as 192.168.1.0) to use for VPN network or auto for automatic network detection
- **VPN Network Mask:** Network mask (such as 255.255.255.0) of the VPN network or auto for automatic detection.
- **Port to Use for VPN Traffic:** Port to use for VPN traffic. The default is 1194, but it can be anything above 1024 (1194 is highly recommended for best results).

- **Protocol to Use for VPN Traffic:** The protocol to use for VPN traffic, either UDP or TCP (the default is UDP for better performance).
- **IP Address or FQDN of VPN Server:** IP address or fully qualified domain name that VPN clients will connect to (such as vpn.yourcompany.com or 192.168.1.1).
- **Allow Multiple VPN Clients to Share a Certificate:** OpenVPN can allow multiple simultaneous connections from clients using the same certificate, but this is not advised.
- **Allow VPN Clients Access to Internal Network:** Select this option to enable access.

4 Specify your OpenVPN certificate configuration.
- **Country of VPN Server:** Your country.
- **City of VPN Server:** The city of your VPN server.
- **The State or Province of Your VPN Server:** The state of your VPN server.
- **Organization Name:** The name of your organization.
- **Hostname for Key:** Unique hostname for this server, which will be embedded in the key.
- **E-mail Address for Certificate:** An e-mail address to be displayed with the certificate.
- **Key Size in bits for Diffie Helman Key:** The Diffie Helman Key Size determines the size of the key used for the initial handshake between the VPN client and server. The larger the key, the more secure it is, but it also takes much longer to generate during install and takes slightly more time for each VPN client to connect. 2048 provides the best balance between security and speed. 1024 is less secure but faster.

5 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The OpenVPN advanced installation is now complete. Click *Finish* to proceed to the available software page. OpenVPN is now listed on the installed software list and can be administered from the OpenVPN administration page.

15.3 Post-Installation

- Section 15.3.1, "Creating the OpenVPN Certificates for Clients in the Key Management Interface," on page 60
- Section 15.3.2, "Monitoring Clients Connected to OpenVPN," on page 61
- Section 15.3.3, "Installing the Windows OpenVPN," on page 61

15.3.1 Creating the OpenVPN Certificates for Clients in the Key Management Interface

OpenVPN Key Management allows you to create a new key/certificate pair, revoke an existing key/certificate pair, and download client configurations for Windows and Linux clients.

1 Follow the post-installation instructions that appear at the end of your OpenVPN install, or log in to the NOWS SBE console.

2 If you choose to log in to the NOWS SBE console, click *Products and Services*.

3 Under *Select Component*, click *VPN Server (OpenVPN)*.

4 Under *Administrative Console*, click *OpenVPN Key Management*.

5 You can now generate a client key, revoke a client, or download a client.

15.3.2 Monitoring Clients Connected to OpenVPN

The Connection Status window shows what clients are connected and displays their addresses.

1 Follow the post-installation instructions that appear at the end of your OpenVPN install or log in to the NOWS SBE console.

2 If you choose to log in to the NOWS SBE console, click *Products and Services*.

3 Under *Select Component*, click *VPN Server (OpenVPN)*.

4 Under *Administrative Console*, click *OpenVPN Connection Status*.

5 Monitor client activity.

15.3.3 Installing the Windows OpenVPN

Follow these steps to install Windows OpenVPN.

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Component*, click *VPN Server (OpenVPN)*.

4 Click *OpenVPN Key Management*.

5 Click *Windows Client and Configuration*.

6 Specify the username in *Unique Name* field, then click *Generate*. This downloads a ZIP file to your desktop.

7 Open the ZIP file and extract the contents to a folder on your system.

8 To install the OpenVPN client and set up the client configuration, double-click the `install.bat` file. This loads the OpenVPN GUI Client Installation.

9 All default values can be used during the installation. Under some versions of Windows, a warning prompts the user to allow installation of a non-secure driver. Click *Continue*.

10 After the installation completes, a new program is visible in the taskbar. Click the new icon to launch OpenVPN with the new configuration; a status window displays, showing the connection progress.

When the connection is fully established, the status window disappears and the taskbar briefly shows the new VPN address. At this point the VPN tunnel has been established and VPN has been successfully downloaded. The VPN tunnel can be broken by right-clicking the taskbar icon and selecting *disconnect*.

Dynamic Local User

16

Dynamic Local User enables you to authenticate to Windows by using your Novell® eDirectory™ User ID through LDAP, which gives you a single place to manage and synchronize user IDs and passwords.

- Section 16.1, "Installing DLU Basic," on page 63
- Section 16.2, "Installing DLU Advanced," on page 63
- Section 16.3, "Post-Installation," on page 63

16.1 Installing DLU Basic

1 Click *Add/Remove > All*, then select Dynamic Local User.

2 Select *Basic*.

3 Configure your DLU LDAP settings.

   LDAP User Container: Specify the LDAP user container. For example, if your user context is cn=jdoe, ou=users, o=mycompany, then your LDAP user container is ou=users,o=mycompany.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The DLU install is now complete. Click *Finish* to return to the available software page.

16.2 Installing DLU Advanced

1 Click *Add/Remove > All*, then select Dynamic Local User.

2 Select *Advanced*, then click *Next*.

3 Configure your DLU LDAP settings.

- **LDAP Naming Attribute:** Specify the LDAP Naming Attribute. For example, if your user context is cn=jdoe, ou=users, o=mycompany, then your LDAP Naming Attribute is cn.
- **LDAP User Container:** Specify the LDAP User Container. For example, if your user context is cn= jdoe, ou= users, o=mycompany, then your LDAP User Container is ou=users,o=mycompany.
- **LDAP Server IP:** Specify the IP address of your LDAP server.
- **LDAP Server Port:** Specify the port of the LDAP server.
- **Secure Connection:** Specify port 636 to ensure that the authentication method is secure LDAP.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The DLU install is now complete. Click *Finish* to return to the available software page.

16.3 Post-Installation

- Section 16.3.1, "DLU Windows Desktop Download," on page 64

16.3.1 DLU Windows Desktop Download

After the installation, complete the following for DLU desktop download for Windows.

1 Log in to the NOWS SBE console.

2 Click *Desktop Downloads*.

3 Under the *Choose Component* drop-down menu, select *Dynamic Local User*, then click *Search*.

4 Under *Search Results*, click *dlu- Dynamic Local User Client* and *dlu- pGina LDAP Registry* files.

5 For both downloads, click *Save File*.

6 Install dlu-Dynamic Local User Client from Windows workstation.

7 Click the *pGina LDAP Plugin* icon.

8 Specify pGina user information, then click *Next* to proceed with installation.

9 Follow the screen prompts to define your computer's architecture type.

- ◆ Enter 1 for x86 architecture type.
- ◆ Enter 2 for x86-64 architecture type.
- ◆ Enter 0 to abort install.

10 Continue as directed by screen prompts.

11 Verify that the plug-in path in the `pgina-ldap-regedit.reg` file is correct. It should point to `ldapath_plus.dll`.

12 Import the `pgina-ldap-regedit.reg registry` file by using the Windows Registry Editor.

> **12a** From your Windows workstation, click *Start > Run*.
>
> **12b** Type `regedit`, then click *OK*.
>
> **12c** Next, click *File > Import* and browse for pgina-ldap-regedit.

13 After installation is complete, test your pGina installation. To test the plug-in from your Windows workstation, click *Start > All Programs > pGina > Plugin Tester*.

14 Specify your directory administrator username and password, then click *Login*.

15 After the LDAP plug-in is successfully configured, restart your Windows workstation for changes to take effect.

After the reboot, the login window is DLU instead of the standard Windows login screen. DLU is automatically configured by the `pgina-ldap-regit.reg` file that has been copied to each Windows workstation's registry settings.

Helpdesk

17

Helpdesk provides an online resource for administrators to monitor issues, check status incident tickets, allocate work, and personalize settings to fit best their company's needs. This reassures users that their incidents have been received by support teams.

17.1 Installing Helpdesk Basic

1 Click *Add/Remove > All*. Select Helpdesk by clicking *Install*.

2 Click *Basic*, then click *Next*.

3 Specify settings for your LDAP services. LDAP is for user authentication and authorization.

- **Helpdesk Administrator User Name:** The login ID for the default administrator of your Helpdesk application.

- **Password for Helpdesk Admin:** The password to which the default administrator login is linked.

- **Admin FDN:** The fully distinguished name of the eDirectory™ tree's admin user, such as cn= admin, o= tree.

- **Admin User Password:** The password you use for your eDirectory tree's admin user.

- **Helpdesk Proxy Username:** For security purposes, a separate proxy user is created for the back-end helpdesk.

- **Helpdesk Proxy User Password:** The password to use for the Helpdesk proxy user.

- **MySQL User:** The username used for Helpdesk database connections.

- **MySQL User Password:** The password to use for the Helpdesk proxy username. For security purposes, the root password in MySQL* is also set to this.

- **Helpdesk Mail User Name:** The login name of the Helpdesk support e-mail account.

- **Helpdesk Mail Password:** The password used to log in to the Helpdesk support e-mail account.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The Helpdesk basic installation is now complete. Click *Finish* to proceed to the available software page. Helpdesk is now listed on the installed software list and can be administered from the *Helpdesk* administration link.

17.2 Installing Helpdesk Advanced

1 Click *Add/Remove > All*. Select Helpdesk by clicking *Install*.

2 Click *Advanced*, then click *Next*.

3 Specify the settings for your LDAP services.

- ◆ **LDAP Host:** Specify the IP address for your eDirectory server. In most cases this is the same as the server on which you are installing Helpdesk

- ◆ **LDAP Port:** The default port for LDAP services is 389. However, this is a non-secure port and all authentication should use a secure connection. Change this to port 636, which is for LDAP over SSL.

- ◆ **LDAP Base Organization:** The base context your Helpdesk application will look to authenticate users. Typically it is the o of the eDirectory tree.

- ◆ **Helpdesk Object:** The eDirectory Helpdesk object's fully distinguished name, such as cn=___, ou=___.

- ◆ **Admin FDN:** The fully distinguished name of the eDirectory tree's admin user, such as cn= admin, o= tree.

- ◆ **Admin User Password:** The password you use for your eDirectory tree's admin user.

4 Click *Next*.

5 Specify the settings for your Helpdesk environment.

- ◆ **Helpdesk Administrator User Name:** The login ID for the default administrator of your Helpdesk application.

- ◆ **Password for Helpdesk Admin:** The password to which the default administrator login is linked.

- ◆ **Helpdesk Tree:** The name of your eDirectory tree.

- ◆ **Helpdesk Upload Path:** The path from which all Helpdesk uploads occur. Use the default to ensure that you receive updates from Novell®.

- ◆ **Helpdesk Download Path:** The path from which all Helpdesk downloads occur. Use the default to ensure that you receive updates from Novell.

- ◆ **Helpdesk Title:** The name you want employees to see when they log in to the Helpdesk application.

- ◆ **Helpdesk Proxy Username:** For security purposes, a separate proxy user is created for the back-end helpdesk.

- ◆ **Helpdesk Proxy User Password:** The password to use for the helpdesk proxy user.

- ◆ **Helpdesk Admin E-Mail:** The e-mail address to be used when users submit tickets, such as support@yourdomainname.com

6 Click *Next*.

7 Specify the settings for MySQL.

- ◆ **MySQL User:** The user that will manage the database.

- ◆ **MySQL User Password:** The password used by your eDirectory tree's administrator.

8 Click *Next*.

9 Specify the Advanced Helpdesk configurations.

- ◆ **Helpdesk Send User Queue Change:** Keep 0 to not notify users of a change in their queue association. Change to 1 to turn on notification.

- ◆ **Helpdesk Send User Priority Change:** Keep 0 to not notify users of a change in the priority of their incident. Change to 1 to turn on notification.

- **Helpdesk Send User Tech Change:** Keep 1 to activate notification. Change to 0 to not notify users of a change to the technician assigned to their incident.
- **Helpdesk Send User Status Change:** Keep 1 to activate notification. Change to 0 to not notify users of a change in their incident's status.
- **Helpdesk Send User Close:** Keep 1 to activate notification. Change to 0 to not notify users of a change in their incident's status to Close.
- **Helpdesk Web Helpdesk Page:** The address for your Helpdesk services.
- **E-mail Address of Queue Changes:** Specify the e-mail address to be used to send notifications of reassignments of queues.
- **E-mail Address for Machine Changes:** E-mail address for machine changes.
- **Helpdesk Technician Change E-Mail:** Specify the e-mail address to be used to send notifications of reassignments of technicians.
- **Helpdesk Solution Change E-Mail:** Specify the e-mail address to be used to send notifications of incident solutions.
- **Helpdesk Status Change E-Mail:** Specify the e-mail address to be used to send notifications of a change to incident status.
- **Helpdesk Priority Change E-Mail:** Specify the e-mail address to be used to send notifications of a change to incident priority.
- **Helpdesk Default Technician:** Specify the default technician name for unassigned Helpdesk incidents.
- **Helpdesk Auto Assign:** Keep 0 to not automatically assign incidents. Change to 1 to enable this feature.
- **Helpdesk Allow Technician Assign:** Keep 0 to not allow technicians to assign incidents. Change to 1 to enable this feature.
- **Helpdesk Check Sleep Time:** The interval in seconds that the system polls for incidents submitted by e-mail.
- **Helpdesk Ticket Sleep Time:** The interval in seconds that the system polls for new incidents submitted through the Helpdesk interface.

10 Click *Next*.

11 Specify any additional Advanced Helpdesk configurations.

- **Helpdesk Log Location:** The directory location on the server for log files.
- **Helpdesk Log Level:** FINE, NORMAL, VERBOSE. *FINE* is the default.
- **Helpdesk Machine Change E-mail:** The time between e-mail reminders.
- **Helpdesk Report Closure:** Keep at 0 to not report on closed reports. Change to 1 to activate notification.
- **Helpdesk Mail Digest:** Keep at 0 to not send out a report of all incidents daily. Change to 1 to activate this notification.
- **Helpdesk Send Notifications:** Keep 1 to send out notifications. Change to 0 to deactivate this notification.
- **Helpdesk Mail Password:** The password used to log in to the designated Helpdesk mail account.
- **Helpdesk Mail User Name:** The user name of the designated Helpdesk mail account.

- ◆ **Helpdesk Return Address:** The e-mail address used by the Helpdesk for responding to user inquiries.
- ◆ **Helpdesk Mail Provider:** The mail service used by your company.
- ◆ **Helpdesk Incoming Mail Port:** The port on which the server is listening for incoming mail.
- ◆ **Helpdesk Incoming Mail Server:** The incoming mail server.
- ◆ **Helpdesk Outgoing Mail Server:** The address of your mail server.
- ◆ **Helpdesk Database Port:** The port that the database uses.
- ◆ **Helpdesk Database Host:** The host that is running the MySQL server.

12 Click *Next*.

13 Review your settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

14 The Helpdesk advanced installation is now complete. Click *Finish* to proceed to the available software page. Helpdesk is now listed on the installed software list and can be administered from the *Helpdesk* administration link.

17.3 Post-Installation

Additional information on administering Helpdesk can be found in the Helpdesk online documentation (http://www.novell.com/documentation/nows/nows_helpdesk_admin/index.html?page=/documentation/nows/nows_helpdesk_admin/data/bookinfo.html).

DHCP

18

The Dynamic Host Configuration Protocol (DHCP) enables your server to provide IP addresses as clients need them instead of manually assigning addresses to client computers.

For additional information, see the Novell® DHCP site (http://www.novell.com/documentation/oes2/ntwk_dnsdhcp_lx/index.html?page=/documentation/oes2/ntwk_dnsdhcp_lx/data/bookinfo.html#bookinfo).

18.1 Installing DHCP

1 Click *Add/Remove > All*. Scroll down to *DHCP* and click *Install*.

2 Click *Basic*, then click *Next*.

3 Confirm that the default settings for DHCP configuration are appropriate or change them as needed, then click *Next*.

- **Subnet:** Specify the network's subnet IP address.

- **Netmask:** Specify the network's subnet mask.

- **IP Range Start:** Specify beginning number of the range of your network's IP addresses (0 is usually the network address).

- **IP Range End:** Specify the ending number of the range of your network's IP addresses (255 is usually the broadcast address).

- **Network Interface:** Interface for the DHCP server to use.

- **DNS 1:** Specify the IP addresses of your DNS server.

- **DNS 2:** Specify the IP address of an alternative DNS server.

- **Default Route:** Specify the default route for DHCP clients. This is the IP address of the next hop router that the clients would go for any traffic off their network. If your server is the NAT/internal gateway, use the server's internal IP address for this setting.

- **Domain:** This is your company's domain name.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The DCHP basic installation is now complete. Click *Finish* to return to the available software page.

18.2 Post-Installation

After installation, there are no modifications or maintenance necessary. Custom tasks can be done from the command line by logging in to the server through SSH.

DNS

19

DNS, or Domain Name System, is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. However, the Internet is actually based on IP addresses. Every time you use a domain name, a DNS service must translate that name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

For additional information, see the Novell DNS online documentation (http://www.novell.com/documentation/oes2/ntwk_dnsdhcp_lx/index.html?page=/documentation/oes2/ntwk_dnsdhcp_lx/data/bookinfo.html#bookinfo).

19.1 Installing Basic DNS

1 Click *Add/Remove* under *Components* then select *All*. Scroll down to DNS and click *Install*.

2 Select *Basic*, then click *Next*.

3 Specify your DNS configurations. To proceed, click *Next*.

   * **DNS Domain Name:** Specify your DNS domain name.

   * **DNS Forwarder 1:** Specify your DNS forwarder. This should be obtained from your ISP.

   * **DNS Forwarder 2:** Specify another DNS forwarder.

   * **DNS Server Type:** The DNS server type can be a master or a slave.

   * **Internal MX Record Hostname:** The hostname tells e-mail servers where to route incoming e-mail.

   * **Internal MX Record Priority:** Identifies which MX record is the primary one and which are the backup ones.

   * **Internal A Record x Hostname:** Add the hostname of the servers you want your DNS server to be able to resolve for your network.

   * **Internal A Record x IP:** Add the IP address of the servers specified for your network.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The DNS Basic installation is now complete. Click *Finish* to proceed to the available software page. DNS is now listed on the installed software list.

19.2 Installing Advanced DNS

1 Click *Add/Remove* under *Components*, then select *All*. Scroll down to DNS and click *Install*.

2 Select *Advanced*, then click *Next*.

3 Specify your DNS configurations.

   * **DNS Domain Name:** Specify your DNS domain name.

   * **DNS Forwarder 1:** Specify your DNS forwarder. This should be obtained from your ISP.

- **DNS Forwarder 2:** Specify another DNS forwarder.
- **DNS Server Type:** The DNS server type can be a master or a slave.
- **Internal MX Record Hostname:** The hostname tells e-mail servers where to route incoming e-mail.
- **Internal MX Record Priority:** Identifies which MX record is the primary one and which are the backup ones.
- **Internal A Record x Hostname:** Add the hostname of the servers you want your DNS server to be able to resolve for your network.
- **Internal A Record x IP:** Add the IP address of the servers specified for your network.

4 Click *Next*.

5 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

6 The DNS Advanced installation is now complete. Click *Finish* to proceed to the available software page. DNS is now listed on the installed software list.

Remote Desktop (TightVNC)

20

TightVNC, or Virtual Network Computing, is a graphical desktop-sharing software that allows a user to remotely control another computer. It transmits local keyboard and mouse events and movements to the remote host, allowing the user to control a remote computer from a local one.

For more information, see the TightVNC online documentation (http://www.tightvnc.com/docs.html).

20.1 Installing TightVNC Basic

1 Click *Add/Remove > All*. Scroll down to *TightVNC* and click *Install*.

2 Select *Basic*, then click *Next*.

3 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

4 The TightVNC installation is now complete. Click *Finish* to proceed to the available software page. TightVNC is now listed on the installed software list.

20.2 Installing TightVNC Advanced

1 Click *Add/Remove > All*. Scroll down to *TightVNC* and click *Install*.

2 Select *Advanced*, then click *Next*.

3 Specify advanced service options.

- **Automatically Start Service:** Indicate here if the service should start automatically.
- **Connection Password:** Set a password for admistrator (root) VNC connections.

4 Review the settings. To make a change, click *Back*. To proceed with the installation, click *Next*.

5 The TightVNC installation is now complete. Click *Finish* to proceed to the available software page. TightVNC is now listed on the installed software list.

20.3 Post-Installation

20.3.1 TightVNC Desktop Download for Linux

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Components*, click *Remote Desktop (TightVNC)*.

4 Under *Desktop Downloads*, select *TightVNC for Linux*.

5 Click *Save to Disk*, then click *OK*.

6 On your desktop, right-click the `tightvnc-server-1.2.9-1.i386.rpm` file, then click *Extract Here*.

7 To complete the download, open a terminal and run `rpm-Uvh-tightvnc-server`

20.3.2 TightVNC Desktop Download for Windows

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Components*, click *Remote Desktop (TightVNC)*.

4 Under Desktop Downloads, select *TightVNC for Windows*.

5 Click *Save to Disk*, then click *OK*.

6 On your desktop, right-click the `tightvnc-1.2.9-setup.exe` file, then click *Extract Here*.

7 To complete the download, double-click the `tightvnc-1.2.9-setup.exe` file on your desktop.

20.3.3 TightVNC Desktop Download for MAC OS X

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Components*, click *Remote Desktop (TightVNC)*.

4 Under *Desktop Downloads*, select *VNC for MAC OS X*.

5 Click *Save File*.

6 To complete the download, double-click the `OSXvnc1.71.dmd` file on your desktop.

20.3.4 TightVNC Desktop Download for the Putty SSH Client for Windows

1 Log in to the NOWS SBE console.

2 Click *Products and Services*.

3 Under *Select Components*, click *Remote Desktop (TightVNC)*.

4 Under *Desktop Downloads*, select *Putty SSH Client for Windows*.

5 Click *Save File*.

6 To complete the download, double-click the `putty.exe` file on your desktop.

20.3.5 Helpful Links

For additional information see the Putty online documentation (http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html).

Uninstalling Components

21

The uninstall tool allows you to perform a component uninstall. Removing a component is the same whether you used a Basic or Advanced install.

NOTE: To uninstall eDirectory™, you must first uninstall iManager.

Uninstall does not always completely remove a package. Manual removal of configuration files and binaries might be required. However, this should not affect your system's performance.

---

1 To uninstall a component, click *Add/Remove*.

2 Click *Uninstall* beside the component you want to remove.

3 Click *Uninstall* again to proceed with the uninstall. Click *Cancel* to stop the uninstall.

4 The component uninstall is now complete. Click *Finish* to return to the available software page.