Novell ZENworks® for Desktops

3.2

www.novell.com

DEPLOYMENT GUIDE

October 30, 2002

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

ZENworks for Desktops 3.2 Deployment Guide
October 30, 2002

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
Internetwork Packet Exchange is a trademark of Novell, Inc.
IPX is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare is a registered trademark of Novell, Inc. in the United States and other countries.
NLM is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Application Launcher is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.
Novell Cluster Services is a trademark of Novell, Inc.
Novell Support Connection is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Technical Services is a service mark of Novell, Inc.
SFTIII is a trademark of Novell, Inc.
snAppShot is a trademark of Novell, Inc.
SMS is a trademark of Novell, Inc.
Storage Management Services is a trademark of Novell, Inc.
ZENworks is a registered trademark of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

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

Contents

About This Guide

This Deployment document includes information about the methods that network adminstrators can use to deploy the components of ZENworks® for Desktops (ZfD) on a live network. Chapters in this document include the following topics:

Documentation Updates

See the ZfD documentation Web site (http://www.novell.com/documentation/lg/zdfs/docui/index.html) for more information.

You should continually check the Web site for updated or additional information.

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.

1 Upgrading from an Older Version of ZfD

If you have an older version of ZENworks for Desktops® (ZfD) that you want to upgrade to ZfD 3.2, you can check for unique migration issues in the following section:

- "ZfD Version Upgrade Issues" on page 11

Before you deploy ZENworks for Desktops 3.2 in a production environment, refer to the following information to help you to adequately plan for a ZfD 3.2 installation:

- "ZfD 3.2 Space Requirements" on page 12

If you want to upgrade an existing ZENworks for Desktops 2 installation to ZfD 3.2, the following information will help you to plan for the upgrade:

- "Upgrading from ZfD 2 to ZfD 3.2" on page 12

NOTE: The upgrade and migration procedures detailed in this document were tested with the ZfD 2 International release.

If you are upgrading from ZfD 3.2 to ZfD 3.2 Support Pack 1 (SP1), the following information will help provide references to the things you need to know:

- "ZfD 3.2 Support Pack 1" on page 25

ZfD Version Upgrade Issues

If you are currently using ZENworks 1.0, ZENworks 1.1 (full), either of the ZENworks Starter Packs, ZfD 2 (full) without the Support Pack installed, ZfD 2 (full) with Support Pack 1, or ZfD 3 with or without the Support Pack installed, the following table provides information about migration issues from an older version of ZfD to ZfD 3.2:

Installed Version of ZfD You Want to Upgrade to Version 3.2	Upgrade Issues and Instructions
Z.E.N.works 1.0	No migration issues. Install ZfD 3.2 to obsolete old version.
Z.E.N.works 1.1 (full), or Starter Pack	No migration issues. Install ZfD 3.2 to obsolete old version > run RMINV1X.EXE, found in \PUBLIC\MGMT\CONSOLEONE\1.2\BIN, to remove the 1.1 attributes (not used in ZfD 3.2) from DS. For more information, see Removing the ZENworks 1.x Inventory Attributes from Workstations in Understanding Workstation Inventory in *Administration*.
ZENworks for Desktops 2 (full), or Starter Pack	Use the instructions for upgrading ZfD 2 International in "Upgrading from ZfD 2 to ZfD 3.2" on page 12.

Installed Version of ZfD You Want to Upgrade to Version 3.2	Upgrade Issues and Instructions
ZENworks for Desktops 2 updated with Support Pack 1	Use the instructions for upgrading ZfD 2 International, in "Upgrading from ZfD 2 to ZfD 3.2" on page 12.
ZENworks for Desktops 3	No issues.
ZENworks for Desktops 3 updated with Support Pack 1	No issues.

ZfD 3.2 Space Requirements

Before you deploy a ZfD 3.2 installation, it may be helpful to have a general idea of the byte size of the most common ZfD 3.2 objects added during a complete installation. With this information, you can predict future disk space needs on the NDS® partition. The following table lists those sizes:

ZfD 3.2 Installed Item	Size
NDS Schema	Approximately 29,129 bytes
Single Registered Workstation	2,471 bytes (may vary if multivalued attributes have multiple values)
Single Application Object	6,396 bytes minimum (varies depending on the size of .FIL files)
Data for Single Workstation in Inventory Database	Approximately 3,000 bytes (varies depending on installed hardware)

Upgrading from ZfD 2 to ZfD 3.2

Before you upgrade from ZfD 2 to ZfD 3.2, you should be aware of the Novell® software products that are required by ZfD 3.2 and the features that are different from version 2 and before. The following sections contain more information:

Novell Software Required for Use With ZfD 3.2

Before you can upgrade from ZfD 2 to ZfD 3.2, you should be aware of some Novell software that you will be required to use with ZfD 3.2. These include:

- "Novell ConsoleOne" on page 13
- "NIS Installation" on page 13
- "Novell Clients" on page 13

Novell ConsoleOne

Although ZfD 2 and earlier versions of the product required the NetWare® Administrator console to administer policies, packages, and Application objects, ZfD 3.2 requires Novell ConsoleOne® version 1.3.2 or newer. ConsoleOne is the Java*-based management console that is the current standard for all Novell administrative products. ConsoleOne 1.3.2 is available on the *Companion* CD that ships with ZfD 3.2.

NIS Installation

ZfD 3.2 installation is accomplished with the Novell Installation Service (NIS), which allows each software component or component group to be separately installed. NIS is automatically launched from the ZfD 3.2 *Program* CD.

Novell Clients

ZfD 3.2 requires the use of the Novell Client™. The following client versions are required:

Workstation Platform	Novell Client Version Required
• Windows* NT*/2000	Novell Client for Windows NT/2000 version 4.81 or later
• Windows 95/98	Novell Client for Windows 95/98 version 3.31 or later

You can obtain the Novell Client you need from the ZENworks for Desktops 3.2 *Companion* CD. For more information, see Obtaining and Installing the Novell Client in *Getting Started*.

Differences in ZfD 2 and ZfD 3.2

Before you upgrade from ZfD 2 to ZfD 3.2, you should be aware of the features that are different from version 2 and earlier. These features were first incorporated in ZfD 3. The following sections contain more information:

- "The Automatic Workstation Import/Removal Component in ZfD 3.2" on page 14
- "Differences in Workstation/Policy Management" on page 14
- "Differences in the Application Management Component" on page 16
- "The Workstation Imaging Component" on page 17
- "Differences in the Remote Management Component" on page 18
- "Differences in the Workstation Inventory Component" on page 18

The Automatic Workstation Import/Removal Component in ZfD 3.2

Before a workstation could be imported in a ZfD 2 environment, it first had to be registered, a cookie for it placed in NDS, then the system administrator had to manually run a tool to actually import it. The import process would create a workstation object in NDS and the workstation could log on as a workstation entity. Much of this manual work required in ZfD 2 is now accomplished automatically in ZfD 3.2 in a one-step process when the workstation is logged in to the network (this feature was first introduced with ZfD 3).

The Automatic Workstation Import service creates the Workstation object in NDS. The object can then be viewed from ConsoleOne the first time the workstation is registered. Subsequent workstation registration updates the Workstation object's properties, freeing the import service from the Workstation object unless the object is renamed, moved, or deleted.

Automatic Workstation Removal is just as simplified. You set a policy and unused Workstation objects are automatically removed from the tree.

For more information, see Automatic Workstation Import in *Administration*.

Differences in Workstation/Policy Management

As with ZfD 3, policies for ZfD 3.2 are organized into fewer policy packages than in ZfD 2. This design lets you manage new platforms more easily because they are under a package's umbrella. For example, all of the platforms under a User Package can benefit from the general user policies.

Most of the ZfD 2 policies now exist in either the User Package or in the Workstation Package.

The different policy packages for ZfD 3.2 include:

- "Container Package" on page 14
- "Server Package" on page 14
- "Service Location Package" on page 15
- "User Package" on page 15
- "Workstation Package" on page 15

Container Package

The Container Package holds only the Search policy. The Search policy is used to minimize tree walking. For more information, see "Container Package" on page 49.

Server Package

The Server Package has four policies:

- **Imaging Server:** Sets workstation imaging parameters.
- **Workstation Import:** Sets parameters to control automatic workstation importing. This policy must be enabled for Auto Workstation Import to function.
- **Workstation Removal:** Sets parameters to control automatic workstation removal. This policy must be enabled for Auto Workstation Removal to function.
- **zeninvRollUp:** Sets parameters for rolling up inventory data to a server.

For more information, see "Server Package" on page 49.

Service Location Package

The Service Location Package has three policies:

- **SMTP Host:** Sets the IP address of the relay host that processes outbound Internet e-mail. This policy must be enabled if the e-mail option for notifying or logging is selected in another policy.
- **SNMP Trap Targets:** Sets SNMP trap targets for associated NDS objects.
- **ZENworks Database:** Sets the DN for locating the ZENworks Database object.

For more information, see "Service Location Package" on page 50.

User Package

The User Package has nine policies found on various platform pages:

- **Desktop Preferences:** Sets defaults for a user's desktop. Use with Windows NT/2000 and Windows 95/98.
- **Dynamic Local User:** Lets you configure users created on Windows NT/2000 workstations after they have authenticated to NDS. Use with Windows NT/2000 only.
- **Help Desk:** Sets the choices viewed in the Help Desk user interface. This policy lets you collect help requests from users in a consistent manner. It also allows you to specify whether a help request can be sent through e-mail. This policy is found on each of the platform pages. Use with Windows NT/2000 and Windows 95/98.
- **NT User Printer:** Sets parameters for printing. Use with Windows NT/2000 only.
- **Remote Control:** Sets parameters for managing remote user functions, such as whether to prompt users for permission to remotely control their workstations. This policy is found on each of the platform pages. Use with Windows NT/2000 and Windows 95/98.
- **User Extensible:** Sets user-defined policies (from .ADM files) for user objects. Use with Windows NT/2000 and Windows 95/98.

  User System policies (ZfD 2) are now incorporated as extensible policies.
- **Windows 2000 Group:** Establishes membership in groups for Windows so that Desktop policies can be applied to them. Use with Windows NT/2000 only.
- **Windows Terminal Server:** Sets parameters for Citrix* users. Use with Windows NT/2000 and Windows 95/98.
- **Scheduled Action:** Sets up schedules for specific actions. This is a plural policy, meaning it can be added many times to the policy package for each of the platform pages. Use with Windows NT/2000 and Windows 95/98.

For more information, see "User Package" on page 51.

Workstation Package

The Workstation Package has ten policies found on various platform pages:

- **Computer Extensible:** Sets user-defined policies (from .ADM files) for workstation objects. Use with Windows NT/2000 and Windows 95/98.

  Computer System policies (ZfD 2) are now incorporated as extensible policies.
- **Client Configuration:** Sets configuration parameters for workstations. Use with Windows NT/2000 and Windows 95/98.

- **Computer Printer:** Sets workstation parameters for printing. Use with Windows NT/2000 and Windows 95/98.
- **RAS Configuration:** Sets dial-up networking parameters. Use with Windows NT/2000 and Windows 95/98.
- **Remote Control:** Sets parameters for managing remote user functions such as whether to prompt users for permission to remotely control their workstations. Use with Windows NT/2000 and Windows 95/98.
- **Workstation Imaging:** Sets the parameters for imaging workstations. Use with Windows NT/2000 and Windows 95/98.
- **Workstation Inventory:** Sets what hardware and software inventory data you want to view for each workstation. Use with Windows NT/2000 and Windows 95/98.
- **Restrict Login:** Sets parameters to restrict logging in by a workstation. Use with Windows NT/2000 and Windows 95/98.
- **Windows 2000 Group:** Establishes membership in groups so that Desktop policies can be applied to them. Use with Windows NT/2000 only.
- **Scheduled Action:** Sets up schedules for specific actions. This is a plural policy, meaning it can be added many times to the policy package for each of the platform pages. Use with Windows NT/2000 and Windows 95/98.

For more information, see "Workstation Package" on page 55.

Differences in the Application Management Component

As with ZfD 3, ZfD 3.2 includes Application Management features to make the management and use of software applications easier than in ZfD 2. The different features include:

- "Caching Applications and Running in Disconnected Mode" on page 16
- "Uninstalling Applications" on page 17
- "Managing Microsoft Windows Installer (.MSI) Applications" on page 17
- "Distributing Applications During the Imaging of a Workstation" on page 17
- "Reporting on Application Management Events" on page 17

For more information about any of these features, see Application Management in *Administration*.

Caching Applications and Running in Disconnected Mode

Application caching enables users to install, run, and verify (repair) applications while they are disconnected from NDS.

ZfD 3.2 Application Management creates a hidden cache directory (NALCACHE) on the root of each user's workstation. This cache directory contains the NDS information required to run an application when the workstation is disconnected from NDS. If the application has already been installed to the workstation and the user disconnects from NDS, the application will continue to run just as if the user were still connected.

The cache directory can also contain the application source files and other information required to install the application or verify (repair) problems that may occur with the application while in disconnected mode. For example, if a user does not install the application before disconnecting from NDS, he or she can still install it, provided the application has been cached to the workstation's cache directory.

To ensure that users will always have mission-critical applications when disconnected, you can configure Application objects to be cached automatically when you associate the Application objects with users. In addition, you can configure Novell Application Launcher™/Explorer to display the Application Management dialog box. This dialog box, which is turned off by default, enables users to select which applications they want to cache to their workstations' local drives.

To save disk space, application files are compressed before being stored in the cache direct.

Uninstalling Applications

Any application that was distributed through ZfD 2, ZfD 3, or ZfD 3.2 Application Management can be uninstalled. All files, INI entries, and registry entries associated with the application are deleted. Shared DLL references are observed.

Managing Microsoft Windows Installer (.MSI) Applications

In addition to being able to manage applications that use snAppShot (.AOT) installation packages, Application Management can now manage applications that use Microsoft* Windows Installer (.MSI) packages. When creating an Application object, you simply choose what type of installation package (.AOT or .MSI) will be used. All ZfD 3.2 functionality, including application distribution, application uninstall, caching, imaging, and disconnected mode, is supported for .MSI applications.

Distributing Applications During the Imaging of a Workstation

Workstation Imaging lets you create base images to apply to workstations. Using Application Management, you can take any Application object and create an add-on image. Once you associate the add-on image with one or more base images, any time the base image is applied to a workstation, the add-on image will be used to automatically distribute the application to the workstation during the imaging process.

Reporting on Application Management Events

Application Management reporting has been improved to provide information about a variety of events, including the success or failure of the following events:

- Distributing an application
- Launching an application
- Uninstalling an application
- Caching an application's source files to the local cache directory

In addition to still being able to report events through SNMP traps or a log file, you can now save events to any ODBC-compatible database.

The Workstation Imaging Component

ZfD 3.2 includes a workstation imaging component that lets you take images of workstation hard disks and then use the network to put them on other workstations. You can perform imaging tasks manually (by physically visiting workstations) or automatically through NDS or the new ZENworks Preboot Services 3.2.

For more information about Workstation Imaging and ZENworks Preboot Services, see Workstation Imaging in *Administration*.

Differences in the Remote Management Component

ZfD 3.2 includes several Remote Management features, including:

- "Remote Wake Up" on page 18
- "Screen Blanking" on page 18
- "User Control Locking" on page 18
- "Wallpaper Suppression" on page 18
- "Time-Out Configuration" on page 18

For more information about these Remote Control features, see Managing a Remote Control Session in Understanding Remote Management Components in *Administration*.

Remote Wake Up

You can remotely power up a powered-down node in your network if the network card on the node is Wake On LAN enabled. This feature lets the administrator manage nodes during off-hours to minimize the downtime that end users may otherwise experience for system maintenance and upgrades. It also facilitates power savings while keeping systems available for maintenance.

Screen Blanking

This option lets the administrator blank the managed workstation screen, making it possible to perform remote management operations unobserved by the end user.

User Control Locking

This feature lets the administrator lock the keyboard and mouse at the managed workstation, making it impossible for the end user to use these controls.

Wallpaper Suppression

When a Remote Control or Remote View session is initiated, this feature lets the administrator suppress the wallpaper displayed on the desktop of the managed workstation.

Time-Out Configuration

This feature lets the administrator set waiting time for connecting with the managed workstation prior to starting a Remote Control or a Remote View session.

Differences in the Workstation Inventory Component

The ZfD 3.2 Workstation Inventory component offers the following features:

- "Sybase/Oracle Database Support" on page 18
- "Inventory Data Roll-Up Support" on page 19
- "Inventory Tools" on page 19

For more information, see "What's in ZfD Inventory Management" on page 139.

Sybase/Oracle Database Support

In ZfD 3.2, the database is an RDMS that can be maintained either in Sybase* Adaptive Server Anywhere* version 7.0, which ships with ZfD 3.2, or the Oracle* 8i, 8.0.4, or 8.i.x databases, which are native on many servers.

Inventory Data Roll-Up Support

ZfD 3.2 supports roll-up of inventory information across servers, so you can choose the inventory deployment configuration that best suits your requirements, whether your network environment is large or small.

In large networks, ZfD 3.2 inventory data is rolled up or accumulated, and sent to a centralized database. Beginning at the leaf server level, changes in inventory data are first sent to intermediate servers (if deployed) and finally to the highest level server, which also holds the Inventory database. The roll-up of scan data in ZfD 3.2 can handle problems such as the WAN link being down.

Inventory Tools

ZfD 3.2 has a Backup tool to help you back up the Inventory database, a Synchronization tool to help you maintain the database in a consistent state with NDS, a Map Server tool to provide a unified view of all the servers and database servers deployed on your network, and a DataExport Tool to store the inventory data from the Inventory database in a comma separated value (.CSV) file format (a format that is usable by most third-party reporting programs).

Preparing Your System for the Upgrade to ZfD 3.2

To prepare for the upgrade to ZfD 3.2, you must first prepare your systems with the following items:

- "Making a Backup of the Existing ZfD 2 Installation" on page 19
- "Upgrading to ConsoleOne" on page 19
- "Editing the AUTOEXEC.NCF File" on page 20
- "Restarting the Server" on page 20
- "Unloading Java" on page 20

Making a Backup of the Existing ZfD 2 Installation

Before you install ZfD 3.2, you should make sure that you have made at least two backups of the existing ZfD 2 installation. For backing up a NetWare server, use Novell Storage Management Services™ (SMS™) or another backup utility to make sure that the server has an archived backup for you to restore later should there be problems with the migration.

For more information about SMS, see the Backup and Restore documentation at the NetWare 5.1 documentation Web site (http://www.novell.com/documentation).

Upgrading to ConsoleOne

Before you upgrade, you must install ConsoleOne version 1.3 or later. ZfD 3.2 components and policies snap in to this java-based network administration tool. Version 1.3 of ConsoleOne is included on the *Companion* CD that ships with ZfD 3.2. If you try to install ZfD 3.2 on a network server that has an older installation of ConsoleOne, you will receive the following message:

```
IMPORTANT: ZENworks for Desktops 3 requires ConsoleOne version 1.3 or later
to display all of its snap-ins. The version of CONSOLEONE.EXE currently
installed on server NAME is dated 03/01/2000 1.2c, which is older than the
required version. Do you want to proceed with the ZfD 3.2 snap-in
installation?
```

```
[Yes] Install ZfD 3.2 snap-ins into the older version of ConsoleOne. I will
install the required (or newer) version of ConsoleOne when this install is
complete.[No] Do not install ZfD 3.2 snap-ins. I will use the older version
of ConsoleOne.
```

If you click Yes, you will need to install the latest ConsoleOne version to SYS:\PUBLIC\MGMT\CONSOLEONE\1.2 on a network server. It is important to note that ConsoleOne 1.3 is also installed to the 1.2 directory.

For more information, see Obtaining and Installing ConsoleOne in *ZENworks for Desktops Getting Started*, or see the ConsoleOne documentation Web site (http://www.novell.com/documentation/lg/consol12c/docui/index.html).

IMPORTANT: If you use ConsoleOne to change the properties of existing ZfD objects, then save your changes, and subsequently open the ZfD objects using NetWare Administrator (NWADMN32.EXE), some of the attributes of the ZfD object will be lost. The best practice is: if you start to administer any ZfD object with ConsoleOne, do not revert to NetWare Administrator to manage that object.

Editing the AUTOEXEC.NCF File

Upgrading from ZfD 2 will make certain commands in the AUTOEXEC.NCF configuration file obsolete. Before you upgrade to ZfD 3.2, you should edit this file and remove or comment the following lines:

```
SEARCH ADD SYS:\PUBLIC\ZENWORKS\JAVALOAD JAVA.NLM

SYS:\SYSTEM\JVORBCFG.NCFLOAD ORBCMD.NLMLOAD OSAGENT.NLM

SYS:\PUBLIC\ZENWORKS\JAVA\ALARMMGR.NCF

SYS:\SYSTEM\MGMTDBS.NCF

SYS:\SYSTEM\GATHERER.NCF

SYS:\PUBLIC\ZENWORKS\JAVA\MASTER.NCF

SYS:\PUBLIC\ZENWORKS\JAVA\STORER.NCF
```

IMPORTANT: The preceding lines appear in the AUTOEXEC.NCF file after a test installation of the ZfD 2 International release. Your AUTOEXEC.NCF file may or may not contain any of the lines shown, depending on the version of ZfD 2 and the components installed.

Restarting the Server

When the latest version of ConsoleOne is installed and the AUTOEXEC.NCF file is edited, type the following command at the server console where you will be installing ZfD 3.2:

```
restart server
```

Restarting the server after the configuration file is properly altered for migration will keep it from loading old ZfD 2 NLM files and configuration files.

Unloading Java

You must unload Java before you begin the ZfD 3.2 installation program. Use the following command at the server console:

```
unload java
```

If Java is running when you run the installation program, the program will display the following message:

```
Java is running on server Name Install may not run properly if Java is running.

Please unload Java on this server then press OK to continue.
```

You can still safely unload Java when this message is displayed.

Installing ZfD 3.2

After you install ConsoleOne, edit the configuration file, and restart the server, you can install ZfD 3.2. We recommend that you use a Custom Install if you are migrating from an older version of ZfD, making sure you choose the option to extend the schema for each of the components you choose to install. For more details about the Custom Install for each ZfD 3.2 component, see *ZENworks for Desktops Getting Started* or the appropriate sections of this *Deployment* documentation.

The ZfD 2 Workstation Inventory component requires more attention to upgrade to ZfD 3.2 than other components. The following sections include information that will help with that migration:

- "Installing ZfD 3.2 Workstation Inventory" on page 21
- "After the Inventory Installation" on page 21
- "Restarting the Server" on page 22

Installing ZfD 3.2 Workstation Inventory

If you have previously been using a ZfD 2 Inventory database, it will be necessary to migrate its data to a ZfD 3.2 database. You will have the option of installing Sybase version 7 to the server during the ZfD 3.2 install. If you choose to install this database, the installation program will display the following message:

```
838:Sybase 6 files at \\Server\Volume\zenworks\database will be deleted.
Sybase 7 files will be copied.
```

This message indicates that support files for Sybase 6 will be replaced by support files for Sybase 7. Your ZfD 2 database is not deleted. You will have to migrate the ZfD 2 data to ZfD 3.2 using a special Database Migration tool. To learn more about this utility, see Migrating the Inventory Information from the ZENworks 2 Database in Understanding Workstation Inventory in *Administration*.

After the Inventory Installation

If you commented some of the lines in the AUTOEXEC.NCF configuration file rather than remove them, you will notice that the ZfD 3.2 installation program removes the following lines from the file:

```
SYS:\SYSTEM\GATHERER.NCFSYS:\PUBLIC\ZENWORKS\JAVA\MASTER.NCFSYS:\PUBLIC\ZEN
WORKS\JAVA\STORER.NCF
```

The installation program adds the following lines to the configuration file:

```
SEARCH ADD SYS:\JAVA\NJCLV2\BINZFDSTART.NCF
```

After you install ZfD 3.2 and restart the server, you may see the following message at the System console prompt:

```
Java: Class com.novell.zenworks.desktop.inventory.servercommon.

ZENWorksInventoryServiceManager exited with status -1.
```

This message is normal and is the result of running the STARTINV.NCF batch command from within ZFDSTART.NCF.

If you have installed a ZfD 3.2 Standalone Server Inventory component on a server, you can create a Service Location Package to correct this condition.

To create a Service Location Package:

1. In ConsoleOne, click the OU where the ZfD 3.2 Inventory Database object is located (this object would normally be found at the same level as the server).
2. Right-click New > Policy Package.
3. Select the Service Location Package > click Next.
4. Name the package > select the container to associate to > click Next.
5. Check Define Additional Properties > click Finish.
6. In the Policies/General tab, enable the ZENworks Database policy and open its properties.
7. In the Database Location tab, browse for the ZENworks Database DN. The ZENworks Database DN would normally be found at the same level of the database server. Look for the ZfD3.2 InventoryDatabase object. Click OK > OK.
8. From the Associations/Associations tab, select the objects to which you want to associate this Service Location Package > click OK.

When you have a Service Location Package, go to the System console and reload the STARTINV.NCF batch command. You should see the following message:

```
Successfully obtained site information from database. Starting Selector
Service. Obtaining dbdir from service object: DATA\Zenworks\Scandir\DbDir.
Trying to connect to the database.Connected to Database.
```

In this message, DATA\ZENWORKS\SCANDIR\DBDIR indicates the location of your database directory (\DBDIR).

Restarting the Server

After you have installed the ZfD 3.2 components that you want, type the following command at the server console where you have installed ZfD 3.2:

```
restart server
```

Restarting the server after the ZfD 3.2 installation will initialize new processes needed for further migration.

Upgrading the Novell Client

Many customers want to install the Novell Client before they install or upgrade to other new Novell products. This section covers two scenarios with the Client:

- “Upgrading to the ZfD 3.2 Client without Upgrading to ZfD 3.2” on page 23
- “Upgrading to the ZfD 3.2 Client Before Migrating ZfD 2 Policy Packages and Data” on page 23

Upgrading to the ZfD 3.2 Client without Upgrading to ZfD 3.2

If you want to, you can upgrade the Novell Client without upgrading to ZfD 3.2; the new client will continue to be compatible with ZfD 2 functionality. You should remember, however, that the client installation can also include various ZfD components to be installed on the workstation, not merely the NetWare connectivity portion of the client.

IMPORTANT: If you choose only to upgrade the ZfD 2 client to the ZfD 3.2 client without further migration, you should continue to administer ZfD 2 using NetWare Administrator rather than ConsoleOne.

If you installed Remote Management to your workstations when you installed the Novell Client that shipped with ZfD 2, the same option will be checked by default in the ZfD 3.2 Client Custom Install. If you uncheck this option during a Client upgrade, the ZfD 2 Remote Management functionality will not be upgraded to the ZfD 3.2 level. If the item is checked, the ZfD 3.2 functionality will be installed.

ZfD 2 will continue to function normally with the ZfD 3.2 clients; ZfD 2 workstations will not need to be re-registered unless a ZfD 3.2 Search policy is installed in the tree.

Upgrading to the ZfD 3.2 Client Before Migrating ZfD 2 Policy Packages and Data

If you install the ZfD 3.2 client after you run the ZfD 3.2 installation program (including extending the schema and installing the Auto Workstation Import component) and restarting the server, the workstations can be further enabled for Automatic Workstation Import. For more information about installing the Novell Client and Client Support Pack used with ZfD 3.2, see Obtaining and Installing the Novell Client in *Getting Started*.

Setting Up Automatic Workstation Import

Even though you install the Automatic Workstation Import/Removal component during the ZfD 3.2 installation program, it must be further configured before it will function and workstations can be imported. For details about how to set up Automatic Workstation Import and Automatic Workstation Removal, see "Automatic Workstation Import and Removal" on page 27.

Migrating ZfD 2 Policy Packages to ZfD 3.2

If you have a large number of workstations already associated with ZfD 2 policies, you can continue to use these same policies in ZfD 3.2. The majority of ZfD 2 policies are unchanged for ZfD 3.2, but the Policy packages have changed (see "Differences in Workstation/Policy Management" on page 14), so the Policy packages must be migrated.

You can migrate the legacy policies by using the ZfD 3.2 Migrate Legacy Policy Packages tool.

To use the tool:

1. From ConsoleOne, click the container where the ZfD 2 legacy policies reside.
2. Click Tools > ZENworks Utilities > Migrate Legacy Policy Packages.
3. From the Migrate Policy Packages dialog box, confirm the context of the container you have selected > click OK.

   HINT: You can preview what the migration utility will do to your legacy policy package without affecting your legacy policies by checking the Preview Only check box.

For more information about the Policy Package Migration tool, see "Migrating ZENworks 2 Policies" on page 90.

After you migrate a Policy package, it will be necessary to migrate the inventory policies. Migrating ZfD 2 inventory policies imports ZfD 2 policy settings for associated workstations to ZfD 3.2.

To migrate ZfD 2 inventory policies:

1. In ConsoleOne, click the Inventory Service object to which the workstations are attached.

   You must select an Inventory Service object that supports the role of an inventory server.

2. Click Tools > Inventory Policy Migration.

3. Specify the following options:

   Server Address IP/DNS: If your ZfD 2 inventory server is a NetWare 4.*x* server, specify the Server Address.

   NDS Search Context: Specify the context for searching the Workstation Inventory object. By default, this tool will search the Workstation object in the current root context.

4. Click Find.

   If any ZfD 2 inventory policies are found, these policies are listed in the Reports window.

5. Click Migrate.

   All the listed inventory policies will be migrated. From the Report window, you can see the list of the inventory policies that were migrated.

   To ensure that the migration is successful, open the inventory policy in ZfD 3.2.

   In ConsoleOne, double-click the Inventory Service object for which you have migrated the policies > click the Workstation Inventory Policy tab. You will see the same inventory settings as specified in ZfD 2.

Migrating ZfD 2 Inventory Data to a ZfD 3.2 Database

The ZfD 3.2 Database Migration tool migrates the existing inventory information from a ZfD 2 database to a ZfD 3.2 database.

IMPORTANT: ZfD 2 application reports are not migrated to ZfD 3.2. The data and formatting required for ZfD 3.2 application reports has changed completely.

To configure the inventory data migration:

1. Open the DBMIGRATE.NCF file in the NetWare server's SYS:\SYSTEM directory or the DBMIGRATE.BAT file in the Windows NT/2000 PUBLIC\ZENWORKS\WMINV\BIN directory. The following text shows the contents of the file:

```
#*************************************************************************
#             Running the DBMigrate Utility
# To run the DBMigrate Utility do the following:
#    1.    Check if the environment variable JDBC_DRIVER points to the
#          path where JDBCDRV.ZIP and CLASSES111.ZIP is present.
#    2.    Check if the environment variable WORKING_PATH points to
#          the path where ZENINVSERVER.JAR, STATUSLOG.JAR and
#          DESKTOPCOMMONUTILITY.JAR are present.
#    3.    Enter the IP address of ZENworks 5 Inventory
```

```
#          database server after the switch '-dbloc'.
#          For example,
#            .... $CLASSPATH -dbloc 164.99.156.134 .....
#    4.    Enter the IP address of ZENworks 2 Inventory database
#          server after the switch '-zen2dbloc'.
#          For example,
#            .... $CLASSPATH -dbloc 164.99.156.134 -zen2dbloc 164.99.156.135 ....
#*************************************************************************
# FOR ORACLE
# If the Zenworks for Desktops 3 inventory database is running on Oracle, then uncomment the
line below and comment the Sybase line.
# Also give the correct Oracle database SID for -sid switch.
#java -ns com.novell.zenworks.desktop.inventory.migration.database.Loader -#classpath
$classpath;$tmppath -nds -dbloc 164.99.149.246 -zen2dbloc #164.99.145.53 -oracle -sid orcl -
Logfilename sys:\etc\dbmigrate.log
# FOR SYBASE
# If the Zenworks for Desktops 3 inventory database is running on Sybase, then #uncomment the
line below and comment out the Oracle line above.
#java -ns com.novell.zenworks.desktop.inventory.migration.database.Loader
#-classpath $classpath;$tmppath -nds -dbloc 164.99.149.196 -zen2dbloc #164.99.145.53  -
Logfilename sys:\etc\dbmigrate.log
```

2. Follow the instructions in the file header and edit the file to add the correct IP addresses of the ZfD 2 server you are migrating from and of the ZfD 3.2 server you are migrating to.

   Be sure to use the command line that matches with the type of database you are running for ZfD 3.2.

3. Run the appropriate file (whether DBMIGRATE.BAT or DBMIGRATE.NCF) from the server console.

After you migrate the database, you can use the inventory policies to choose when you want to rescan the workstations. For more details on how to migrate the ZfD 2 inventory data to ZfD 3.2, see Migrating the Inventory Information from the ZENworks 2 Database in Understanding Workstation Inventory in *Administration*. This documentation also provides several scenarios that may help you in the migration process.

ZfD 3.2 Support Pack 1

The following sections provide references with more information about upgrading to ZfD 3.2 SP1:

- “Issues Resolved in ZfD 3.2 SP1” on page 26
- “ZfD 3.2 SP1 Installation and Issues” on page 26

Issues Resolved in ZfD 3.2 SP1

Many issues occurring in the original shipping version of ZfD 3.2 have been corrected in the ZfD 3.2 Support Pack 1 (SP1). For information on the ZfD 3.2 issues addressed by fixes in the Support Pack, see TID 10071863 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10071863.htm) at the Novell Support (http://support.novell.com) Web site.

ZfD 3.2 SP1 Installation and Issues

Procedures for downloading, installing, and using ZfD 3.2 SP1 are documented in the Server Update Readme file, which can be found at the ZENworks for Desktops 3.2 documentation Web site (http://www.novell.com/documentation/lg/zdfs/index.html).

2 Automatic Workstation Import and Removal

ZENworks® for Desktops (ZfD) Automatic Workstation Import provides simplified, hands-off management of users' workstations. Workstation objects provide you with a way to push software and computer settings down to the client by using the Novell® Application Launcher™ (NAL).

ZfD can be installed on any NetWare® 4.*x*, 5.*x,* or 6.*x* server, or an NDS® for NT server.

The following will help you to understand and deploy Automatic Workstation Import and Removal:

- "Understanding Automatic Workstation Import and Removal" on page 27
- "Deploying Automatic Workstation Import and Removal" on page 31

Understanding Automatic Workstation Import and Removal

Automatic Workstation Import includes Automatic Workstation Removal and provides management of the entire life cycle of a workstation, from the creation of its object to its removal.

The following sections will help you to understand Automatic Workstation Import and Removal:

- "Understanding Workstation Import and Registration" on page 27
- "Client/Server Considerations" on page 28

Understanding Workstation Import and Registration

After you have installed Automatic Workstation Import, importing workstations is a one-step process. The Workstation Registration program in the Novell Client™ accesses the Automatic Workstation Import service, which creates the Workstation object and registers the workstation.

The following sections provide information on importing and registration:

- "Using the Import Service" on page 27
- "Registering Imported Workstations" on page 28
- "Removing Workstation Objects" on page 28

Using the Import Service

The Automatic Workstation Import service creates network traffic; however, the import service is used only when one of the following occurs:

- A workstation is logged in to the tree and a corresponding Workstation object does not exist.

  This would normally be the first time the workstation is registered. The Automatic Workstation Import service initially creates the Workstation object in the tree, populates the

object with default values, and updates the properties with the current registration information.

The Workstation Import policy is used to determine where the Workstation object is created and how it is named.

- A workstation is logged in to the tree and its Workstation object was either moved or renamed.

  The registration program calls the import service to synchronize the workstation with its Workstation object.

At all other times when a workstation is logged in to the network, the Workstation Registration program in the client registers the workstation and updates the Workstation object. The import service is not contacted for these operations, so network traffic to and from the Workstation Import service is not an issue. (Workstations that authenticate and update Workstation objects will still generate some network traffic.)

Registering Imported Workstations

After a workstation has been imported, it only needs to be registered each time it logs in to the tree. The registration program updates the Workstation object when one of the following occurs:

- The Workstation Manager program starts
- A user logs in to the tree
- A Windows* 2000 or Windows NT* user logs out

After the workstation has been imported, the client's registration program updates the workstation's registration time, network address, last server, and last user information.

Network traffic is minimized because the Workstation Registration program doesn't need to access the import service.

Removing Workstation Objects

You should periodically remove unused Workstation objects so that inventory reporting is more accurate.

Automatic Workstation Removal uses the Workstation Removal policy to determine when Workstation objects are considered to be unused so that they can automatically be removed from NDS.

Workstation objects can be automatically removed when a workstation has not been registered within the time frame specified by the effective Workstation Removal policy.

You can specify any number of days for how long a workstation can go without registering before it is considered unused.

Client/Server Considerations

You should consider the following information before setting up Automatic Workstation Import and Removal:

- "Server Considerations" on page 29
- "Client Considerations" on page 29

Server Considerations

Consider the following when setting up the server portion of Automatic Workstation Import and Removal:

- “Selecting Servers for Deployment” on page 29
- “Using DNS Names or HOSTS Files” on page 29
- “Scheduling Workstation Removal” on page 29

Selecting Servers for Deployment

Generally, more workstations will be imported than are removed. Therefore, you will want to have more servers set up with the Automatic Workstation Import service than with the Automatic Workstation Removal service.

To minimize network traffic, you should install the Automatic Workstation Import service on at least one server per WAN. Automatic Workstation Removal does not generally produce a lot of network traffic, so it can be used across WAN links.

Using DNS Names or HOSTS Files

In setting up Automatic Workstation Import, you should use DHCP for TCP/IP addresses so that DNS names can be found automatically, instead of setting up and maintaining a HOSTS file on every workstation.

Using DHCP and DNS names in your network provides you with automated management of workstation importing. You should coordinate with your DNS administrator to set up IP addresses for your workstation import services according to physical location in order to allow workstations to contact the import service locally, rather than across WAN links.

You can differentiate IP addresses according to domain or zone by using multiple domains or by using primary and secondary zones. For example, you could have a DNS entry for Automatic Workstation Import using the following syntax:

```
zenwsimport.context_string.com
```

HOSTS files can be used to handle exceptions, such as when you want a specific client to resolve to a specific workstation import service. A HOSTS file is useful for manually importing a workstation, such as in a test environment.

Scheduling Workstation Removal

You should schedule workstation removal so that it is performed periodically when the network is least busy, such as during non-work hours.

Client Considerations

Consider the following when setting up the client portion of Automatic Workstation Import and Removal:

- “Different Registration Methods” on page 30
- “Backwards Compatibility and the Search Policy” on page 30
- “Upgrading Client Software” on page 30

Different Registration Methods

The registration method for ZfD is not backwards compatible with previous versions of ZENworks. Workstation importing is server-centric in ZfD; it was user-centric in ZENworks 2.

Much of the work that was done manually in ZENworks 2 is now automated. Workstation registration has become a one-step automatic process.

For example, to import a workstation in ZENworks 2:

1. The workstation is registered upon login to the network.
2. The workstation is imported.

   Result: The object is created the first time it is registered.
3. The workstation is re-registered.

   Result: If the object was created, the workstation is placed into the registry.

To import a workstation in ZfD:

1. The workstation is registered upon login to the network.

   Result: The object is created the first time it is registered and the workstation is placed into the registry each time it is registered.

Backwards Compatibility and the Search Policy

ZfD is backwards compatible with the policies in previous versions of ZENworks. Therefore, the old and new policies can co-exist. This allows you to continue using ZENworks 2 policies after you have installed ZfD policies, which is useful for performing an incremental transition to the newer policies.

Because of the new ZfD registration method, the Search policy becomes very important. After you have installed ZfD and updated workstations with the newer Novell Client, the ZENworks 2 Search policy must be used for ZENworks 2 policies to be found. By using ZENworks 2 Search policies, you can have backwards compatibility between the ZfD Novell Client and the ZENworks 2 policies.

For example, if you want a container and its objects to recognize existing ZENworks 2 policies, you must create a ZENworks 2 Search policy in ConsoleOne® and associate it with that container. Then the newer Novell Client will find the older policies. However, when both a ZENworks 2 Search policy and a ZfD Search policy are associated with the same container, ZfD policies take precedence.

If you have no Search policy associated with an object, ZfD will search the tree for ZfD policies. In this case, ZENworks 2 policies are ignored by the ZfD Novell Client.

Upgrading Client Software

You can upgrade the Novell Client, then install Automatic Workstation Import, or you can install the import service then upgrade the client. Either way, once both have been done, Automatic Workstation Import can become functional.

Deploying Automatic Workstation Import and Removal

When installing ZfD, you will be able to specify import and removal roles for selected servers. Therefore, before running the ZfD installation program, you should determine which servers you want to run the import service, the removal service, or both.

To deploy Automatic Workstation Import and Removal, we recommend the following sequence:

1. Install the Automatic Workstation Import and Removal service software.
2. Set up the Automatic Workstation Import and Removal policies.
3. Set up DHCP and DNS names and customize logging.

   Using NDS names is preferable to using HOSTS files for registering workstations because HOSTS files must be managed manually at each workstation.
4. Update the Novell Client on the workstations using ACU.

   ACU is the preferred method. For information on other methods, see "Upgrading Specific Files with Policy Packages" on page 37 or "Distributing Client Updates with an Application Object" on page 38.

After you have completed this sequence, Automatic Workstation Import and Removal will be functional.

The following sections contain steps to help you deploy Automatic Workstation Import and/or Removal:

Installing Automatic Workstation Import and Removal

To install Automatic Workstation Import and Removal on NetWare or Windows NT/2000 servers:

1. Select a workstation where you can run the ZfD installation program and later run ConsoleOne to administer ZfD.

   IMPORTANT: Make sure that this workstation and all other administrative workstations are not running ConsoleOne while the ZfD installation is running.
2. At the workstation, insert the *ZENworks for Desktops* product CD.

   The WINSETUP.EXE program will auto run. If it does not auto run, run it from the root of the CD.
3. To launch the NIS setup program, click English > Install ZENworks.
4. To display the User License Agreement for the ZfD software, click Next > read the agreement > click Accept if you agree with the terms of the agreement.

   If you do not agree with the terms of the software agreement, do not install the software.
5. In the ZENworks Install Types dialog box, select Custom > click Next.
6. Deselect all options except for Automatic Workstation Import > click Next.

Selecting this option allows you to set up the import and removal roles for your servers in a later dialog box.

7. If you have already extended the schema on the current tree for ZfD, deselect Schema Extensions > click Next.

   Keep the other two options selected, because both files and application objects need to be installed for Automatic Workstation Import and Removal.

8. In the ZENworks List of Trees dialog box, click the name of the NDS tree where you want to install Automatic Workstation Import and Removal.

9. In the ZENworks List of Servers dialog box, click the names of the servers where you want to install Automatic Workstation Import and/or Removal.

10. In the Languages dialog box, click the language of the files that you have chosen to be installed to the server > click Next.

    English is chosen by default and must be installed in addition to any other language you choose.

11. In the Automatic Workstation Import Management dialog box, select one of the following roles for each server:

    None: You will generally use this option when you are installing other components in addition to Automatic Workstation Import or Removal and do not want a server to run the import or removal service.

    Import: Select this option for each server where you want to run only the import service.

    Removal: Select this option for each server where you want to run only the removal service.

    Import/Removal: Select this option for each server where you want to run both the import and removal services.

12. In the Summary dialog box, review the list of the products to be installed and how much disk space each product will consume when installed > click Finish to begin the installation process.

Setting Up the Automatic Workstation Import and Removal Policies

The following sections will help you to configure and associate the necessary policies:

- "Configuring the Automatic Workstation Import Policy" on page 32
- "Configuring the Automatic Workstation Removal Policy" on page 34
- "Associating the Server Package" on page 35

Configuring the Automatic Workstation Import Policy

For Automatic Workstation Import to work, you must configure the Workstation Import policy. This policy determines how the workstation objects will be named and placed in NDS.

To configure the Workstation Import Policy for ZfD:

1. If you have not created a Server Package, in ConsoleOne, right-click the server container where your server object is found > click New > click Policy Package > select Server Package > click Next > name the package > click Next > click Finish.

2. Right-click the Server Package > click Properties.

The Policies tab with the General page is displayed. We recommend you use the General policies for your test system. General policies will apply to all valid platforms (NetWare and Windows NT/2000).

3. On the General page, check the box under the Enabled column for the Workstation Import policy.

   This both selects and enables the policy.

4. Click Properties.

5. On the Containers tab, click Add.

6. Select valid workstation containers where rights are needed to create workstations > click OK.

   These are containers where you plan to import Workstation objects. This establishes the rights that make importing possible.

   These rights are inherited by all subcontainers.

7. Click the Platforms tab.

   The General page with its Location tab is displayed.

8. To select where to create workstation objects, click the Create Workstation Objects In drop-down list > select one of the following:

   Selected Container: The selected path is displayed (recommended). You may need to create the container before you can select it here.

   Server Container: Uses a server container, or enter a relative DS path.

   User Container: Uses a user container, or enter a relative DS path.

   Associated Object Container: Uses an associated object container, or enter a relative DS path.

9. Click the Naming tab.

10. To change the default workstation naming syntax, do one or more of the following:

    - Click Add to add name field items (Computer+MAC Address defaults). You can select from the following: User, Container, DNS, Server, OS, CPU, IP Address, or user-defined.
    - Click an item, then click either the up-arrow or down-arrow to change the item's position in the syntax.

11. Click the Groups tab > select the groups where the workstations will automatically be imported.

    You may need to create the Workstation Group objects.

    IMPORTANT: If workstations are to be imported to a workstation group, the container for that group object must be in the container list of the Workstation Import policy (see Step 6). Otherwise, newly imported workstations will not be added to the group.

12. To set login limits, click the Limits page > do any of the following:

    - Select the user login number if relative to a user container, or if "user" is part of the workstation's name. This number represents how many times you will allow a user to log in before importing the workstation.
    - To limit the number of workstations that can be imported per hour, check the box.

- Specify the upper limit for the number of Workstation objects that can be created in an hour.

13 Click OK to save your changes.

14 To configure Workstation object removal, continue with "Configuring the Automatic Workstation Removal Policy" on page 34; otherwise, skip to "Associating the Server Package" on page 35.

Configuring the Automatic Workstation Removal Policy

For Automatic Workstation Removal to work, you must configure the Workstation Removal policy. This policy determines when unused Workstation objects will be removed from NDS.

To configure the Workstation Removal policy for ZfD:

1 In ConsoleOne, right-click the Server Package > click Properties.

2 Click the Policies tab > click one of the following pages:

General
NetWare
WinNT-2000

The following steps are the same for all platforms. If this policy is set for a specific platform, it will override the policy set for General.

3 Check the check box under the Enabled column for Workstation Removal policy.

This both selects and enables the policy.

4 Click Properties > Add.

The Containers page is displayed.

5 Select a valid workstation container where rights are needed to delete workstations.

6 Click the Limits page > specify the number of days for removing a Workstation object.

This is a consecutive number of days that the workstation has not registered.

7 Click the Schedule page.

8 Select the year > select the date (month and day) > select when to start the policy (start and duration times).

This establishes when this policy can first be in effect.

9 To set how often this policy should be repeated (how frequently to remove Workstation objects), specify the frequency in days.

10 To limit the number of Workstation objects that can be removed in one session, specify the number.

This option is provided to help in load-balancing the server that is doing the Workstation object removal work.

Each session is started when the policy is started again (see Step 9).

11 Click OK > continue with "Associating the Server Package" on page 35.

Associating the Server Package

The import and removal policies you configured and enabled cannot be in effect until you associate their Server Package with a Container object.

To associate the Server Package containing the import and removal policies you have configured:

1. In ConsoleOne, right-click the Server Package > click Properties.
2. Click the Associations tab > Add.
3. Browse for the container for associating the package > click OK.

Setting Up Automatic Workstation Import and Removal to Run on the Servers

The steps in the following sections assume that you selected the Import, Removal, or Import/Removal option as part of Automatic Workstation Import installation:

- "Setting Up Automatic Workstation Import" on page 35
- "Customizing Logging for the Import and Removal Services" on page 36

Setting Up Automatic Workstation Import

The most important item to remember when deploying Automatic Workstation Import is to use DHCP for TCP/IP addresses so that DNS names can be found automatically for simplified workstation importing. This is preferable to setting up and maintaining HOSTS files on every workstation.

To set up Automatic Workstation Import, do the following for each import service server:

1. Set up a DNS name for Automatic Workstation Import to use.

   This can be either a DNS entry or an entry in a local HOSTS file. An example of a DNS name is www.novell.com.

   The following is an example of the text you would add in a HOSTS file for Automatic Workstation Import:

   ```
   151.155.155.55 zenwsimport
   ```

   In this example, the TCP/IP address is for the server where you are running the Automatic Workstation Import service. "zenwsimport" is not the name of a server, but a DNS name that resolves to this TCP/IP address. In other words, zenwsimport is a label to identify the server as the one running the Automatic Workstation Import service.

   For Windows 95/98, the HOSTS file's location should be:

   Win95-98_drive:*Win95-98_directory*\HOSTS

   IMPORTANT: The default host file in Windows is named HOSTS.SAM. Do not use the .SAM extension with your host filename. Rename HOSTS.SAM to HOSTS, or make a copy and rename the copy. Remember that by default, Windows 95/98 hides filename extensions that are of a known type. Therefore, make sure filename extensions are being displayed so that you can correctly rename the HOSTS.SAM file to HOSTS.

   For Windows NT/2000, the HOSTS file's location should be:

   WinNT-2K_drive:*WinNT-2K_directory*\SYSTEM32\DRIVERS\ETC\HOSTS

   HOSTS as shown above is a filename, not a folder name. By default, Windows 95/98 will hide a filename extension (such as .SAM) because it is a known file type.

2 To verify the DNS name or TCP/IP address, type the following at the workstation command prompt:

```
ping zenwsimport
```

Customizing Logging for the Import and Removal Services

To customize logging for the import and removal services, do the following for each import and removal service server:

- **NetWare Servers:** To change logging to a higher level, modify the following line in ZENWSIMP.NCF or ZENWSREM.NCF:

  ```
  -Dlogfile=sys:\zenworks\zenwsimp.log -Dlogfilelevel=1
  ```

  by changing the logging level from 1 (brief) to 2 (medium) or 3 (verbose).

  For the removal service, the log file is named ZENWSREM.LOG.

- **NetWare Servers:** If you want logging to also display on screen, do the following:
  - In ZENWSIMP.NCF or ZENWSREM.NCF, add the following line before the class names:

    ```
    Java -ns
    ```

  - In ZENWSIMP.NCF or ZENWSREM.NCF, locate the -Dloglevel=0 line and change the number to 1 (brief), 2 (medium) or 3 (verbose).
- **NDS for NT/2000 Servers:** To change logging to a higher level, run ZENWSIMP.REG on the server.

  ZENWSIMP.REG is located on the *ZENworks for Desktops* product CD.

  This will modify the workstation's registry for both services. The following registry key will be added:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZENworks\AutoWSImport
  ```

  The added strings are:

  ```
  zenwsimportCmdLine
  ```

  ```
  zenwsremovalCmdLine
  ```

  The log files will be located and named according to the following entries:

  ```
  -Dlogfile=c:\zenwsimp.log -Dlogfilelevel=1
  ```

  ```
  -Dlogfile=c:\zenwsrem.log -Dlogfilelevel=1
  ```

  You can edit both the filename and location and the logging level. The available logging levels are:

  0 = None
  1 = Brief
  2 = Medium
  3 = Verbose

Upgrading the Novell Client

You must update each workstation that you want to import with the latest Novell Client (shipped on the *ZENworks for Desktops Companion* CD). This is required to place Workstation Manager on the workstations.

Make sure Workstation Manager is enabled on each workstation.

You can update or upgrade the Novell Client using three different methods. We recommend that you use ACU to upgrade the client. Review the following sections for detailed information on each method:

- "Upgrading the Client with ACU" on page 37
- "Upgrading Specific Files with Policy Packages" on page 37
- "Distributing Client Updates with an Application Object" on page 38

Upgrading the Client with ACU

Novell Automatic Client Upgrade (ACU) provides a way to upgrade from earlier Novell Client software to the latest Novell Client software. On Windows NT workstations, you can also upgrade the operating system. This upgrade happens when users log in.

HINT: Novell recommends using this method to upgrade the Novell Client software.

The ACU process requires the following tasks:

1. Create an ACU folder on the NetWare server.
2. Copy the Novell Client files to the ACU folder.

   Workstations read these files during login.
3. Grant rights to all users to the ACU folder.
4. Update the appropriate .CFG, .INI, or unattended file for each platform-specific client.
5. Modify the appropriate login script.

Extensive documentation about the ACU process is available at the Novell Client Documentation Web site (http://www.novell.com/documentation) for each platform, including specific requirements and examples to assist you. Read this documentation before establishing an ACU process for your network.

The client documentation is also available on the *ZENworks for Desktop* product CD. See the following documents:

- Novell Client for Windows 95 (see ACU Install)
- Novell Client for Windows NT (see Automatic Client Upgrade)

You can also create a script that upgrades the clients on four different operating systems.

Upgrading Specific Files with Policy Packages

You can use ZfD features to routinely update files you specify. You can create a policy package and then add an action to the policy package that updates a certain file each morning, for example. Then when you associate that policy package with a Workstation object, Workstation Group, or Container object where the Workstation object resides, the file will be updated each morning on that workstation.

Distributing Client Updates with an Application Object

You can distribute client updates to workstations by using NAL. For more information, see Chapter 4, “Application Management,” on page 91.

Verifying that Automatic Workstation Import and Removal are Working

At this point, if the scheduler is working, registration should happen automatically when any of these events occur:

- Scheduler service startup (95/98 and NT/2000)
- User login (95/98 and NT/2000)
- User logout (NT/2000 only)
- System shutdown (95/98 and NT/2000)

To verify that Automatic Workstation Import and Removal are working:

- For each NetWare import or removal service server, type the following at the server console:

  `java -show`

  and look for:

  `com.novell.application.zenworks.autowsmanagement...`

- For each Windows NT/2000 import or removal service server, check services for:

  `ZENworks Workstation Import`

  or

  `ZENworks Workstation Removal`

If Automatic Workstation Import or Removal is not running, restart the server.

If WSREG32.LOG shows problems or no activity, registration can be forced to run (without event logging) by running WSREG32.EXE, which is located on the workstation at:

`windows_drive``:\`*`windows_directory`*`\`*`windows_system_directory`*

To stop an import or removal service, you can use the following commands in place of using the process IDs displayed by the java -show command. Type the following at the server console:

```
java -killzenwsimp
java -killzenwsrem
```

These commands are also contained in the following .NCF file:

SYS:\SYSTEM\ZFDSTOP.NCF

3 Workstation Management

Much of the functionality of ZENworks® for Desktops (ZfD) Workstation Management depends on the preliminary administrative work you do in ConsoleOne® as you import user workstations into the tree and set up the policies that can be associated with User and Workstation objects.

Before you can manage your network's workstations, you must understand Workstation Management, plan how you want it set up, then deploy your configuration.

The following sections provide planning and deployment information:

Planning Workstation Management

The following sections will help you to understand and plan a full deployment of Workstation Management on your network:

Understanding Workstation Management Components and Features

Workstation Management features are designed to help you reduce the overall cost and complexity of configuring and maintaining workstation desktops in the network. Such inventory information as hard disk space, machine memory, and processes running can be pushed up to NDS® Workstation objects from the ZfD components pushed down to each network workstation.

The following sections provide information on components and features:

Components

Workstation Management has the following components:

- “ConsoleOne Snap-ins” on page 40

Workstation Resident Modules

The workstation resident modules authenticate the user to the workstation (Windows* NT* only) and network, and transfer configuration information to and from NDS. Under Windows NT, Workstation Management runs with administrative privileges that allow it to dynamically create and delete NT user accounts, provided it can communicate with NDS.

ConsoleOne Snap-ins

The snap-ins are Java* files that are used to create, view, and configure the various Workstation Management NDS objects through ConsoleOne.

Features

Workstation Management features let you store and configure Windows 95/98 and Windows NT/2000 desktop policies in NDS and push them down to the client. You can also push printer drivers to the client. The client workstation can be thought of as an extension of the user.

Workstation Management has the following features:

- “Multiple Platform Support” on page 40
- “Windows NT/2000 Support” on page 40
- “Novell Client Configuration” on page 41
- “Workstation Profile Management” on page 41
- “Scheduled Updates” on page 41
- “Server and Client Policies” on page 41
- “NDS Storage for Policies” on page 41
- “Dynamic Printer Configurations” on page 41
- “ZfD Reports” on page 41

Multiple Platform Support

Workstation Management software allows all user account and desktop information for Windows 95/98 and Windows NT/2000 to be centrally managed within NDS using a single administrative utility: ConsoleOne.

Configuration information is stored in policy package objects that are particular to a platform. For example, there are policy package objects containing policies for NetWare®, Windows 95/98, and Windows NT/2000 that can be downloaded to the workstations.

Windows NT/2000 Support

For Windows NT environments, Workstation Management also eliminates the need for NT domains or for a large number of NT user accounts to reside in the local Security Access Manager (SAM) of each workstation.

The Windows 2000 Group policy is an extension of extensible policies for Windows 2000 and Active Directory*.

Workstation Management stores user information, desktop configuration, OS configuration, and workstation information in NDS. For NT users, this means that when a user's NDS user account is

associated with this configuration information, the user can access the network using any NT workstation configured with Workstation Management.

If the user does not have an account on the workstation at the time of login, Workstation Management can automatically create one according to the associated user information. Once the user is attached to the network, associated policies are downloaded to the workstation to provide a consistent desktop on each workstation used.

Novell Client Configuration

You can configure settings specific to the Novell® Client™, such as the name context and preferred tree in NDS, then have that configuration rolled out to multiple workstations on the network.

Workstation Profile Management

You can create and manage mandatory user profiles, and you can control user interface options, such as the command console, display control, keyboard control, mouse control, and sound control attributes. Once you have set these attributes, users cannot modify these settings unless they are given the appropriate NDS rights.

Scheduled Updates

This feature lets you schedule software upgrades to occur for workstations at a specific time, such as during the evening when the workstation is not in use. These updates can be done without requiring users to be logged in to the network from the workstation. As long as the workstation is powered on, Workstation Management can authenticate the workstation to NDS and perform the update.

Server and Client Policies

ZfD uses policies for hands-off management of server and client processes. Policies can be set for automating workstation import and removal, managing users and workstations, and providing workstation inventory information.

NDS Storage for Policies

Workstation Management lets you create policies using ConsoleOne instead of the Microsoft* POLEDIT utility. This approach to creating policies provides three specific benefits:

- It eliminates the requirement that you copy the policy file to the SYS:\PUBLIC directory of each NetWare server on the network, thus reducing your initial setup workload.
- Because the policy is stored in NDS, you only have to make changes once.
- Any change you make to a policy is automatically replicated across the network in a multiple-partition NDS network, thus providing automatic fault tolerance.

Dynamic Printer Configurations

Using ConsoleOne, you can configure printing for users without ever leaving your office. You can associate a print queue and its associated print driver with Workstation or User objects. Then, when the user authenticates to NDS, the printer configuration is dynamically created on the user's workstation and the printer driver is automatically downloaded and installed.

ZfD Reports

ZfD provides predefined reports for effective policies and policy package associations. The scope of both reports is for a selected container and, optionally, its subcontainers.

The effective policies report provides the following information:

Version
Tree
Container
Object DN
Platform
Effective Policy DN

The policy package report provides the following information:

Tree
Container
Package DN
Association

The report results are displayed in Notepad and are automatically saved as text files in the \WINDOWS\TEMP directory of the workstation where you are running ConsoleOne.

Understanding the ZENworks Database

The ZENworks database is used for logging report information for ZfD. Therefore, to run reports on Workstation Management, you will need a configured Database object with an associated ZENworks Database policy.

If you selected to install the ZENworks database during installation of ZfD, you should configure and enable the ZENworks Database policy to identify the location of the ZENworks Database object, which knows the location of the database file (MGMTDB.DB).

If you are using a Sybase* database, the Database object will be created during installation if you selected the Inventory option. The Database object will then contain default values. If you did not select the Inventory option, you will need to create the Database object and configure the properties to populate it with default values. In either case, you will still need to edit the Database object properties to fill in the User Name and Password fields to secure the database file because this information cannot be automatically populated.

If you are using an Oracle* database, you will need to create and configure the Database object. Although the database files may have been installed, the Database object will not have been created.

Understanding ZfD Policies and Policy Packages

To fully deploy ZfD Workstation Management, you must configure, enable, and associate the necessary policies and policy packages in ConsoleOne.

Review the following sections for an understanding of ZfD policies and policy packages:

- “Understanding Policy Packages” on page 43
- “Understanding ZfD Policies” on page 43
- “Understanding Plural Policies” on page 44
- “Understanding Enabling of Policies” on page 44
- “Understanding Policy Scheduling” on page 44

Understanding Policy Packages

A policy package is an NDS object that contains policies, which are properties in the package object. ZfD policies are grouped into policy packages for ease of administration. You create and manage policy packages using ConsoleOne.

Each policy package contains one or more platform-specific tabs that contain one or more policies specific to that platform and package. One of the platform pages can be labeled General.

A policy package has a Policies tab that contains several pages. These pages each identify an operating platform, such as General, NetWare, or Windows (95-98 or NT-2000). Any policy that you enable on a General page applies generally to all platforms indicated by the other pages. However, any policy configurations you set on a specific platform page will override similar settings on the General page.

The ZfD policy packages are:

Container Package
Server Package
Service Location Package
User Package
Workstation Package

The Container Package and Service Location Package are identical to the policy packages used in ZENworks for Servers (ZfS). The Server Package also exists in ZfS; however, in ZfD it contains different polices. The User Package and Workstation Package are unique to ZfD.

Understanding ZfD Policies

ZfD policies provide you with automated management of server, user, and workstation configurations, processes, and behaviors. For example, policies can define the following:

- Parameters for importing workstation objects to the tree
- Locations to search for effective policies
- Login restrictions
- Desktop preferences for users
- Help desk parameters for users
- Dynamic printer definitions
- Dial-up networking parameters
- Parameters for remotely controlling a workstation
- Event and action scheduling

Each policy's properties contains one or more tabs where you can specify settings or configurations related to User, Workstation, Group, or container objects, depending on the type of policy.

For a list of ZfD policies, see “Determining the Necessary Policies” on page 48.

Understanding Plural Policies

ZfD has one plural policy with the default name of Scheduled Action. Plural policies allow you to have multiple instances of the same policy type within the same policy package.

Because you can have several different actions that you might want to run on different schedules, when you add a Scheduled Action policy to the policy package you should name it to reflect the action being scheduled.

For ZfD, the Scheduled Action plural policy is available for all platforms in the User Package and Workstation Package.

Understanding Enabling of Policies

As your Workstation Management needs change, you can enable, disable, or modify a policy using any of the three states for policy settings:

Check Box	State	Description
☑	Enabled	Activates the policy’s settings; however, they are not enforced unless the policy package is also associated with an object.
☐	Disabled	Clears a policy. However, disabling a policy in ConsoleOne does not immediately clear its effect at the workstation. The workstation will run the policy with the cleared settings because the settings for each policy are saved in the workstation's registry.
☑ or ☐	Ignored	Does not guarantee the clearing or enabling of a policy, because it will allow the workstation to continue with whichever policy setting it previously had.

When you create a policy package, its policies are disabled by default. Once you enable a policy, some default settings will be in place.

A policy can be enabled when you:

- Create a policy package
- Modify a policy package

A policy can also be enabled anytime from within most of the lists where the policy is displayed.

Understanding Policy Scheduling

Some policies can be scheduled to run at a certain time. During creation, all policy packages are given a default run schedule. This means that all applicable policies in this package will run according to the default schedule. However, you can change the entire policy package schedule, or you can set a policy within the package to run at a different time from the rest of the package.

If you should enable a policy but fail to schedule it, it will run according to the schedule currently defined in the Default Package Schedule.

Understanding Policy Package Associations

Once you have enabled a policy, you must then associate it to make it effective. Configuring, enabling, and scheduling a policy only sets it up. A policy is enforced through its association with an NDS object, such as a Server, User, Group, or Workstation object.

Because policy package associations flow down a tree like Inherited Rights do in NDS, you can associate a policy package directly with an object. You can also associate a policy package indirectly, such as with the object's parent container.

When you view the associated policy packages for an object, ZfD starts at the object and searches up the tree in the following order for the associated policy packages to be displayed:

1. The object
2. Any Group where the object has membership
3. Any container above the object up to [Root]

Similar to assigning different rights for different users in NDS, you can set a general policy for most users and unique policies for unique users.

You must have the Write right to both the policy package and the object in order to associate one with the another.

You can associate a policy package with Server, User, Group, or Workstation objects when you:

- Create or modify the policy package
- Create or modify the Server, User, or Workstation objects
- Associate a policy package with a group or container where the User or Workstation objects have membership

Understanding the Search Policy

The Search policy is used to prevent tree-walking. Unless specified differently in a Search policy, when ZfD starts searching for an object's associated policy packages, it starts at the object and works its way up the tree. If ZfD does not have any Search policies defined, it will walk the tree until if finds an effective policy for the object. This can cause unnecessary network traffic. Therefore, plan to use Search policies wherever needed.

All enabled policies in a policy package that is associated directly with an object have precedence over contradicting policies in policy packages higher in the tree.

Search policies can be defined for both ZfD and ZENworks 2 policy packages. For ZENworks 2 policies to be usable in a ZfD environment, ZENworks 2 Search policies must be defined and correctly associated. For more information, see "How Effective Policies Work When ZfD and ZENworks 2 Policies Coexist in the Tree" on page 46.

Understanding Effective Policies

Effective policies for an NDS object are those that have been configured, enabled, and associated with the object. Just as the effective rights in NDS flow down the tree, policy package associations also flow down the tree.

ZfD and ZENworks 2 policies can both be associated with the same object. However, which policy is effective depends on the version of the Novell Client that is being used by the workstation and if the proper Search policies have been set up.

The following sections provide more information on effective policies:

- "How Effective Policies Are Determined" on page 46
- "How Package Associations Are Resolved to Determine Effective Policies" on page 46
- "How Effective Policies Work When ZfD and ZENworks 2 Policies Coexist in the Tree" on page 46

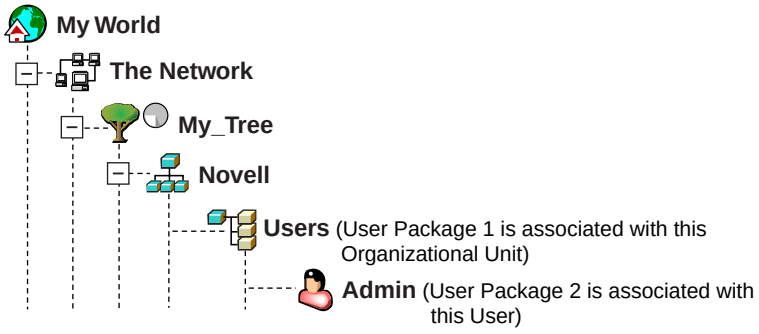
How Effective Policies Are Determined

When ZfD calculates the effective policies for an object, it starts with all policy packages assigned to that object. It then looks up the tree (assuming that the search order starts at the leaf object and goes up towards the root of the tree) for associations made to parent containers. The first enabled policy it finds is the one it uses, just as the system looks up the tree for effective rights.

How Package Associations Are Resolved to Determine Effective Policies

Because ZfD policies provide management-by-exception through policy package associations, a lower package association overrides an upper package association. In other words, a package associated to a User object overrides any similar settings in a package associated to the user's container object.

The following illustrates policy package associations:



Suppose that in this illustration, User Package 1 contains three enabled policies: Desktop Preferences, Help Desk, and Remote Control. User Package 2 contains one enabled policy: Desktop Preferences. For the User object, the Desktop Preferences policy settings in User Package 2 will override the similar policy settings in User Package 1.

The effective policies for the user are the Desktop Preferences policy in Policy Package 2 and the Help Desk and Remote Control policies in Policy Package 1. The Associations tab for this User object will list the one policy in User Package 2 that has been enabled. The two enabled policies in User Package 1 will also be listed on the User object's Associations tab. In other words, effective policies are the sum of all enabled policies in all policy packages associated directly or indirectly to an object.

How Effective Policies Work When ZfD and ZENworks 2 Policies Coexist in the Tree

If an object is associated with policies from both ZfD and ZENworks 2, the policy that is effective for the object depends on the schema extension version, the associated Search policy version, and the version of the Novell Client that is used by the workstation. The ZfD version of the client must be used to recognize ZfD policies. The following discussion is concerned with the possibilities from various combinations of the schema and Search policy versions.

ConsoleOne will display only the effective policies in an object's properties for ZfD policies. To view the effective policies for ZENworks 2 policies, you must use NetWare Administrator. However, in some instances ZfD reporting can show effective policies for an object for both versions.

The following table lists the policy version that is effective for the item listed in the first column according to the combination of the schema and Search policy versions listed in the column headings.

Item	Schema=v2, Search Policy=v2	Schema=v3, Search Policy=v2	Schema=v3, Search Policy=v3
Policies Actually Effective for ZfD Workstations	ZENworks 2	ZENworks 2	ZfD
ConsoleOne Snap-in for ZfD	N/A	ZfD	ZfD
Effective Policies Report for ZfD	ZENworks 2	ZENworks 2 and ZfD	ZENworks 2 and ZfD
Policies Actually Effective for ZENworks 2 Workstations	ZENworks 2	ZENworks 2	ZENworks 2
NetWare Administrator Snap-in for ZEnworks 2	ZENworks 2	ZENworks 2	ZENworks 2

Note the following from this table:

- The two Policies Actually Effective rows mean that the workstations are running their respective versions of the client. In other words, a ZENworks 2 workstation is not running the ZfD version of the client.
- The Policies Actually Effective For ZfD Workstations row indicates that until a ZfD Search policy has been associated with the object, any associated ZfD policies will not be in effect, although they could be displayed in some ConsoleOne object's properties as if they were.
- The ConsoleOne Snap-ins for ZfD row indicates that for the ZfD version of the client there are no effective policies for an object when the schema and associated Search policy are both ZENworks 2.
- The Effective Policies Report for ZfD row indicates that there are two instances when the effective policies report for ZfD can show the effective policies for an object for both versions. In all cases for the report, any policies that could be effective or have been associated are displayed. However, because ZfD is combing NDS and not pinging each client to build the report, it cannot indicate which policies are actually in effect.
- In the NetWare Administrator Snap-in for ZENworks 2 row, ZENworks 2 in the last column assumes that it existed when ZfD was installed. Otherwise, that entry would be N/A.

Understanding Extensible Policies

For any software program, an extensible policy allows you to control any application function that is configured in the Windows registry. Extensible policies are user-defined. ZfD lets you easily customize and deploy extensible policies across your network to accommodate your specific business practices.

ZfD leverages Microsoft desktop enhancements by doing the following to provide extensible policies that are enabled in NDS:

- Moving the policy editor functionality into NDS
- Moving Windows registry information for applications into NDS
- Enabling NDS to point to extensible policy files

How Extensible Policies Work

When you install a software application that is Windows 95/98 compatible, that application's installation program uses the Microsoft policy editor (POLEDIT.EXE) to read the application's .ADM file and create a .POL file that updates the workstation's Windows registry. However, when you install an application on a workstation under the umbrella of ZfD, the Novell ZENworks policy editor (WMPOLSNP.EXE) is used instead to read the .ADM file and make the necessary changes to the workstation's Windows registry.

The Microsoft policy editor lets you make changes to the policies .ADM files create, but only per workstation. The ZENworks policy editor, when an application is installed under ZfD, ensures that the application's DNS-enabled policies are automatically applied across the network, rather than manually to one workstation at a time.

When you create an extensible policy, you must schedule it to run before it can take effect. Note that some hard-coded policies are run explicitly at login. Such policies are not scheduled.

ADM Files

The .ADM files are static templates for creating policies in the ZfD database. When you edit a policy in ZfD, the changes are made in the database rather than the .ADM file. Even so, you should not delete an .ADM file from a directory once it has been used in ZfD because it will be needed to undo registry changes if you should remove the policy from ZfD.

When you have .ADM files that you want to use, you should place them in a location where you will be able to easily browse for them. You can save them on a workstation or on a server, because once the .ADM file has been used to create a policy, it will not be needed again until you remove the policy.

Because ZfD automatically displays any policies listed in the following location when you view an Extensible Policies tab, we recommend that you use it:

SYS:\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\ZEN\ADM Files

This is the default location where .ADM files shipped with ZfD are placed.

Determining the Necessary Policies

To use the ZfD features, you must create policy packages and configure and enable the needed policies. ZfD provides policies in the following five policy packages. Review these sections and determine which policies are needed.

- “Container Package” on page 49
- “Server Package” on page 49
- “Service Location Package” on page 50
- “User Package” on page 51
- “Workstation Package” on page 55

Container Package

The Container Package has only one policy: Search. It is used to limit how far up the tree ZfD will search for the effective policies.

The Search policy provides the following benefits:

- Improved security
- The ability to reorder a search
- Better search performance by limiting the search levels traversed in NDS and by avoiding unnecessary LAN traffic

The Search policy locates policy packages that are associated with containers. To make a Search policy effective you can associate it only with a container. The container you associated it with provides the location from where the search begins.

You can specify the number of levels above or below the location where to begin the search:

Number	Description
0	Limits the search to the selected level.
1	Limits the search to one level above the selected level. For example, if you selected the server's parent container, this would limit the search to one level above the parent level.
-1	Limits the search to one level below the selected level. For example, if you selected [Root], -1 would limit the search to one level *below* [Root].

Without a Search policy in effect, the default is to search from the parent container clear to [Root] hourly. The search checks each container up the tree towards [Root] for policy packages associated with those containers.

The default Search policy will recognize the policy package associated with the User or Workstation object before it will look in any group or container where such an object resides.

The default search order, Object > Group > Container > Root, can be reordered and can include as few as one of the locations. For instance, you can exclude Group objects by setting the search order to Object > Container > Root.

You can avoid unnecessary LAN traffic by searching to the partition instead of [Root].

When you view the associated policy packages for an object, by default ZfD starts at the object and searches up the tree to [Root] for all policy packages associated with:

- The object
- Any Group where the object has membership
- Any of the object's parent containers

The first enabled policy package found is used.

Server Package

The Server Package has four policies that are used for ZfD server functions. These policies are duplicated on each of the platform pages of the Policies tab:

- "Imaging Server" on page 50
- "Inventory Roll-Up" on page 50
- "Workstation Import" on page 50
- "Workstation Removal" on page 50

Imaging Server

This policy sets rules that determine which images to put on workstations that are imaged by this policy. For more information, see Chapter 5, "Workstation Imaging," on page 109. For more information on setting up this policy, see "Setting Up the Imaging Server Policy" on page 62.

Inventory Roll-Up

This policy sets parameters for rolling up inventory data to a server. For more information, see Chapter 7, "Workstation Inventory," on page 137. For more information on setting up this policy, see "Setting Up the Inventory Roll-Up Policy" on page 65.

Workstation Import

This policy sets parameters to control automatic workstation importing. It must be enabled for Automatic Workstation Import to function.

You can set rules on how Workstation objects are named and where they are created. You should decide if you want to create Workstation objects in their own containers or in the container where the User objects reside.

You may find it easiest to manage Workstation objects in a common container if your User objects are scattered among various containers in the tree.

You may also find it easiest to keep User and Workstation objects in the same container. This will minimize the number of policies you must create and associate for using all of the ZfD features.

For more information, see Chapter 2, "Automatic Workstation Import and Removal," on page 27. For more information on setting up this policy, see "Setting Up the Workstation Import Policy" on page 62.

Workstation Removal

This policy sets parameters to control automatic workstation removal. This policy must be enabled for Auto Workstation Removal to function.

For more information, see Chapter 2, "Automatic Workstation Import and Removal," on page 27. For more information on setting up this policy, see "Setting Up the Workstation Removal Policy" on page 64.

Service Location Package

The Service Location Package has three policies:

- "SMTP Host" on page 51
- "SNMP Trap Targets" on page 51
- "ZENworks Database" on page 51

SMTP Host

This policy sets the IP address of the relay host that processes outbound Internet e-mail. It must be enabled if the e-mail option for notifying or logging is selected in another policy. For more information on setting up this policy, see "Setting Up the SMTP Host Policy" on page 66.

SNMP Trap Targets

This policy sets SNMP trap targets for associated NDS objects.

Part of setting SNMP trap targets is to create trouble tickets. When users open a Help Requester trouble ticket, they select a subject from a drop-down list. You can use the Trouble Ticket Subject Lines dialog box to create a list of subject lines from which users can choose.

When users create a trouble ticket, it is sent to the help contact (as selected in the Help Desk policy) as an e-mail message. Carefully chosen subject lines can aid the help contact in organizing trouble tickets.

For more information on setting up this policy, see "Setting Up the SNMP Trap Targets Policy" on page 66.

ZENworks Database

This policy sets the DN for locating the ZENworks Database object. This allows ZfD to log information in the database file for ZfD reporting. For more information on setting up this policy, see "Setting Up the ZENworks Database Policy" on page 66.

User Package

The User Package has a Policies tab that has three pages (General, WinNT-2000, and Win95-98). User policies are listed under each of the pages. The policies found on the various pages are:

- "Desktop Preferences" on page 51
- "Dynamic Local User" on page 51
- "Help Desk" on page 52
- "User Printer" on page 53
- "Remote Control" on page 53
- "Scheduled Action" on page 53
- "User Extensible" on page 53
- "User System" on page 53
- "Windows 2000 Group" on page 54
- "Windows Terminal Server" on page 54

Desktop Preferences

For the Windows 95/98 and Windows NT/2000 platforms, this policy sets defaults for users' desktops. For more information on setting up this policy, see "Setting Up the Desktop Preferences Policy" on page 69.

Dynamic Local User

For Windows NT/2000, this policy lets you configure users created on a Windows NT/2000 workstation after they have authenticated to NDS.

A Dynamic Local User (DLU) is a User object that the Novell Client temporarily or permanently creates in the workstation's Security Access Manager (SAM) database.

A temporary user or account is known as a volatile user, and the duration is determined by the administrator. This type of account prevents the SAM from becoming too large.

If a user is not defined as a DLU and does not have an account on the workstation, the Novell Client cannot create the user's account. Therefore, the user cannot log in to the workstation, unless there is a previous account, or the administrator manually creates the user's account on the workstation. If the user is not defined as a DLU, the Novell Client uses the user's credentials from the Windows NT tab of the login dialog box to authenticate to the workstation.

If the user is defined as a DLU, the Novell Client uses the user's credentials from NDS or from the WinNT User Package, depending on how the administrator sets it up.

If you configure a DLU in an NT User Policy Package to administer user access to NT workstations, and if you use a credential set other than the NetWare credential set, the NT workstation user accounts created have a random, unknown password and are created as volatile user accounts. If volatile user caching is also enabled, the NT user accounts will persist on the workstation for the duration of the cache life. However, these accounts are inaccessible because they have an unknown password.

If you use volatile user caching for users with non-NetWare credential sets, those NT user accounts will not be accessible unless the users log in to NDS concurrently and have the Manage Existing Accounts option set.

You can allow or restrict DLU login access to certain workstations by using the Login Restrictions page. Workstations and containers listed in the Excluded Workstation list cannot use DLU access; workstations listed or workstations that are part of containers listed in the Included Workstations list can use DLU access.

To properly manage group priorities, do not allow users associated with DLUs to be members of multiple groups.

For more information on setting up this policy, see "Setting Up the Dynamic Local User Policy" on page 70.

Help Desk

This policy sets the choices viewed in the Help Desk user interface. It lets you collect help requests from users in a consistent manner. It also allows you to specify whether a help request can be sent through e-mail. This policy is found on each of the platform pages.

Setting up a Help Desk policy for your users provides you with pertinent user information, such as user context or network address, with little effort required from the user. This policy can be associated with a User, Group, or container object.

When users or members of the group or container associated with that policy run the Help Requester on the workstation, they can send a request for help through e-mail. By selecting a problem category to display in the e-mail subject line and then entering a message, they will access support contact information, such as an e-mail address or phone number, and will be able to view information specific to their workstations.

For example, Kim is a network administrator who set up a Help Desk Policy for Joe and other users in Joe's group. Kim added three items to the Subject drop-down list: Server problem, Application problem, and Hardware problem. Kim also decided that she wanted the group's help requests to be e-mailed to her, so she placed her e-mail address in the Contact information.

Joe can't access a spreadsheet program, so he contacts the help desk by using the following steps:

1. Runs Help Requester on his workstation.
2. Selects "Application problem" as the subject of his help request.
3. Enters the message "My spreadsheet program won't open."
4. Clicks Send.

The next time Kim checks her e-mail she has a message from Joe with "Application problem" in the subject line. When Kim opens the e-mail, she sees all the pertinent information about the workstation, the user, and the problem.

For more information on setting up this policy, see "Setting Up the Help Desk Policy" on page 71.

User Printer

For Windows NT/2000, this policy displays a list of the currently installed printers. It lets you add printers to the list, remove printers from the list, select a printer as the default, and assign a print driver to each printer. In addition, you can identify the settings for network printers.

For more information on setting up this policy, see "Setting Up the NT User Printer Policy" on page 72.

Remote Control

This policy sets parameters for managing remote user functions, such as whether to prompt users for permission to remotely control their workstations. This policy is found on each of the platform pages.

For more information, see *Chapter 6, "Remote Management," on page 125*. For more information on setting up this policy, see "Setting Up the Remote Control Policy" on page 73.

Scheduled Action

This policy sets schedules for specific actions. This is a plural policy, meaning it can be added many times to the policy package. It is available for each of the platform pages.

For more information on setting up this policy, see "Setting Up the Scheduled Action Policy" on page 74.

User Extensible

This policy sets user-defined policies (from .ADM files) for user objects. It is found only on the WinNT-2000 and Win95-98 pages.

For more information, see "Understanding Extensible Policies" on page 47. For more information on setting up this policy, see "Setting Up the User Extensible Policy" on page 75.

User System

This ZENworks 2 policy is now incorporated in extensible policies. If you migrate your ZENworks 2 policies, the User System policy will exist in the User Package; however, it cannot be edited—it can only be enabled or disabled. To change its settings you would need to use an extensible policy.

For more information, see "User Extensible" on page 53. For more information on setting up this policy, see "Setting Up the User Extensible Policy" on page 75.

Windows 2000 Group

Only for Windows 2000, this policy is an extension of extensible policies for Windows 2000 and Active Directory.

For the following reasons, you will need to use UNC paths rather than mapped drives for importing this policy to ZfD:

- Users could change their login scripts, altering drive mappings
- Workstation objects are often logged in before users are; therefore, there are no drive mappings available

With UNC paths, as long as the server is available, the policy will be found.

Group policies have changed significantly since the ZfD version 3 initial release. Group policies are now additive, they check for revisions, they cache already-processed policies, and they use persistent or volatile settings. Review the following sections for more information:

Additive Group Policies: Group policies are now additive. This means that settings from multiple Group policies are cumulatively effective, rather than individually. Settings from multiple Group policies can affect users and workstations. Policies start with the local Group policy settings and are applied in reverse of the policy search order. This means that a setting in a policy applied first has lowest priority and its value is overwritten by any other policy with the same setting.

Security settings are not additive; they are set by the last effective policy.

Revision Checking: Group policies now track the revision of the policies in effect. As long as the list of effective policies and their revisions remains the same, Group policies are not processed, but use the cached Group policy.

NOTE: Each time the Edit Policies button is clicked, the revision of a Group policy changes, causing the policies to be reprocessed.

Group Policy Caching: The last-processed Group policy is cached locally. This helps reduce network traffic by processing Group policies only if necessary. If UserA logs in on a new machine, his or her effective Group policies are processed and then cached.

If UserA logs out and UserB logs in, and if UserB has the same effective Group policies as UserA, the locally-cached Group policy is restored instead of reprocessing Group policies. If the list of effective policies is different or if the revision is changed on any policy, the Group policies are reprocessed.

Persistent and Volatile Settings The administrator determines if Group policies are persistent or volatile. The persistent setting indicates that when the Group Polices are set, they remain set—even if a user happens to log in only to a workstation and not to the network.

The volatile setting indicates that the original local Group policy settings will be restored when:

- The user logs out (user settings are restored)
- The system shuts down (workstation settings are restored)

For more information on setting up this policy, see "Setting Up the Windows 2000 Group Policy" on page 77.

Windows Terminal Server

Only for Windows 2000, this policy sets parameters for Citrix* and Microsoft Terminal Server users.

For more information on setting up this policy, see "Setting Up the Windows Terminal Server Policy" on page 78.

Workstation Package

The Workstation package has a Policies tab that has three pages (General, WinNT-2000, and Win95-98). Workstation policies are listed under each of the pages. The policies found on the various pages are:

Client Configuration

This policy sets configuration parameters for workstations. It is found only on the WinNT-2000 and Win95-98 pages.

For more information on setting up this policy, see "Setting Up the Client Configuration Policy" on page 80.

Computer Extensible

This policy sets user-defined policies (from .ADM files) for workstation objects. It is found only on the WinNT-2000 and Win95-98 pages.

For more information, see "Understanding Extensible Policies" on page 47. For more information on setting up this policy, see "Setting Up the Computer Extensible Policy" on page 81.

Computer Printer

This policy sets workstation parameters for printing. It is found only on the WinNT-2000 and Win95-98 pages.

The printer feature lets you dynamically create printer access when a user logs in to the network or at any other time you determine it necessary. Once you configure and assign printer access, the printer icon is displayed on the workstation's desktop.

Only printers that are QMS-compatible can take advantage of this Workstation Management feature.

You can assign printers to users or workstations.

You make printer assignments to users from the Printer Policy Details page of the User Package associated with the User object. When assigned to users, printers follow the user. Regardless of which workstation the user accesses to log in to the network, the printer icon is displayed on the desktop of the workstation from which the user logs in.

You make printer assignments to workstations from the Printer Policy Details page of the Workstation Package associated with the Workstation object. When they are assigned to the workstation, printers remain with the workstation, and the printer icon is displayed on that workstation desktop regardless of which user logs in to the network from that workstation.

To enable this feature you must:

1. Enable the Printer Policy in the appropriate User or Workstation Package.
2. Set up and configure the printer.
3. Associate the User or Workstation Packages with User or Workstation objects.

For more information on setting up this policy, see "Setting Up the Computer Printer Policy" on page 82.

Computer System

This ZENworks 2 policy is now incorporated in extensible policies. If you migrate your ZENworks 2 policies, the migrated Computer System policy will exist in the Workstation Package; however, it cannot be edited—it can only be enabled or disabled. To change its settings you would need to use an extensible policy.

For more information, see "Computer Extensible" on page 55. For more information on setting up this policy, see "Setting Up the Computer System Policy" on page 82.

RAS Configuration

This policy sets dial-up networking parameters.It is found only on the WinNT-2000 and Win95-98 pages.

The Dial-Up Networking page lets you dial into a network and establish a connection before any action item is executed.

The number to dial or phone book entry to be applied to the workstations represented by the Workstation object are defined via ConsoleOne.

If a connection is not successful, the action will be rescheduled according to the options selected in the Options page of the Scheduled Action's properties. That is, the action will be considered as unsuccessful.

After they are downloaded to the workstation, the dial-up entries can be seen via the Dial-Up tab of the workstation Scheduler. The entries are downloaded when the workstation is used to log in to the network or when the administrator schedules a download.

The Dial-Up Networking page lets you:

- Select a dial-up number
- Create a new dial-up entry
- Edit a dial-up entry
- Delete a dial-up entry
- Import dial-up entries defined at the workstation

The workstation itself may have dial-up numbers that are defined via the Windows Dial-Up Networking utility. These numbers are not administered by the Dial-Up Networking page.

For more information, use either Windows Help under the Start Menu in Windows or the What's This help on the individual pages associated with dial-up networking.

Dial-up networking and remotely controlling workstations are not the same. For more information on setting up this policy, see "Setting Up the RAS Configuration Policy" on page 83.

Remote Control

This policy sets parameters for managing remote user functions. For example, whether to prompt users for permission to remotely control their workstations. This policy is found on each of the platform pages.

For more information, see *Chapter 6, "Remote Management," on page 125*. For more information on setting up this policy, see "Setting Up the Remote Control Policy" on page 83.

Restrict Login

This policy sets parameters to restrict logging in by specified users. It is found only on the WinNT-2000 and Win95-98 pages.

For more information on setting up this policy, see "Setting Up the WS Restrict Login Policy" on page 89.

Scheduled Action

This policy sets schedules for specific actions. This plural policy can be added multiple times to each of the platform pages.

For more information on setting up this policy, see "Setting Up the Scheduled Action Policy" on page 85.

Windows 2000 Group

Only for Windows 2000, this policy is an extension of extensible policies for Windows 2000 and Active Directory.

For the following reasons, you will need to use UNC paths rather than mapped drives for importing this policy to ZfD:

- Users could change their login scripts, altering drive mappings
- Workstation objects are often logged in before users are; therefore, there are no drive mappings available

With UNC paths, as long as the server is available, the policy will be found.

Group policies have changed significantly since the ZfD version 3 initial release. Group policies are now additive, they check for revisions, they cache already-processed policies, and they use persistent or volatile settings. Review the following sections for more information:

Additive Group Policies: Group policies are now additive. This means that settings from multiple Group policies are cumulatively effective, rather than individually. Settings from multiple Group policies can affect users and workstations. Policies start with the local Group policy settings and are applied in reverse of the policy search order. This means that a setting in a policy applied first has lowest priority and its value is overwritten by any other policy with the same setting.

Security settings are not additive; they are set by the last effective policy.

Revision Checking: Group policies now track the revision of the policies in effect. As long as the list of effective policies and their revisions remains the same, Group policies are not processed, but use the cached Group policy.

NOTE: Each time the Edit Policies button is clicked, the revision of a Group policy changes, causing the policies to be reprocessed.

Group Policy Caching: The last-processed Group policy is cached locally. This helps reduce network traffic by processing Group policies only if necessary. If UserA logs in on a new machine, his or her effective Group policies are processed and then cached.

If UserA logs out and UserB logs in, and if UserB has the same effective Group policies as UserA, the locally-cached Group policy is restored instead of reprocessing Group policies. If the list of effective policies is different or if the revision is changed on any policy, the Group policies are reprocessed.

Persistent and Volatile Settings The administrator determines if Group policies are persistent or volatile. The persistent setting indicates that when the Group Polices are set, they remain set—even if a user happens to log in only to a workstation and not to the network.

The volatile setting indicates that the original local Group policy settings will be restored when:

- The user logs out (user settings are restored)
- The system shuts down (workstation settings are restored)

For more information on setting up this policy, see "Setting Up the Windows 2000 Group Policy" on page 86.

Workstation Imaging

This policy sets the parameters for imaging workstations. It is found on each of the platform pages.

For more information, see *Chapter 5, "Workstation Imaging," on page 109*. For more information on setting up this policy, see "Setting Up the Workstation Imaging Policy" on page 87

Workstation Inventory

This policy sets what hardware and software inventory data you want to view for each workstation. It also identifies an inventory server for each workstation in the network. This policy is found only on the WinNT-2000 and Win95-98 pages.

For more information, see Chapter 7, "Workstation Inventory," on page 137. For more information on setting up this policy, see "Setting Up the Workstation Inventory Policy" on page 88.

Determining Whether to Migrate Older Policies

You should eventually migrate all ZENworks 2 policies to obtain the better performance and ease of management that ZfD offers. When you install ZfD, you are not required to migrate older policies because ZENworks 2 policy objects are not removed when extending the schema. This allows you to migrate the older policies in phases, such as by context.

If you do not migrate ZENworks 2 policies to ZfD, you must continue using NetWare Administrator for management purposes. ZfD uses ConsoleOne for management purposes. ConsoleOne will display only the effective policies in an object's properties for ZfD policies. To view the effective policies for ZENworks 2 policies, you must use NetWare Administrator. If you

have a mixed environment of ZENworks 2 policies and ZfD policies, you must use both NetWare Administrator and ConsoleOne.

When you migrate the older policies, they are placed into the newer policy packages. You cannot choose their placement. Most ZENworks 2 policies are placed in either the User Package or Workstation Package.

Default Package schedules are not migrated, so you will need to redefine these schedules for the migrated policies.

The individual User System and Computer System policies in ZENworks 2 have been incorporated as extensible policies in ZfD. They are migrated as individual policies that cannot be edited in ZfD. By default, they are automatically enabled when migrated. To override them, you must disable them, make changes that correspond to the ZENworks 2 settings in a ZfD extensible policy, then enable the ZfD extensible policy. For more information, see "Understanding Extensible Policies" on page 47.

You can continue to use the older versions of the User/Computer System policies until you have duplicated the settings for these older policies in the newer extensible policies.

IMPORTANT: The User/Computer System policy settings cannot be viewed after they have been migrated. You will need to know how these policies were configured in ZENworks 2 to configure the similar settings in a ZfD extensible policy. Therefore, you should note the settings for the individual ZENworks 2 policies before you migrate them.

Deploying Workstation Management

For ZfD to function properly, you must create the policy packages so that you can configure, enable, schedule, and associate your planned policies.

To implement your planned deployment of Workstation Management on your network, proceed with the following:

- "Installing Workstation Management" on page 59
- "Creating the Policy Packages" on page 59
- "Setting Up a Search Policy" on page 60
- "Setting Up the Server Package Policies" on page 61
- "Setting Up the Service Location Package Policies" on page 65
- "Setting Up the User Package Policies" on page 69
- "Setting Up the Workstation Package Policies" on page 80

Installing Workstation Management

Many of the ZfD policies are available only if you select the Workstation Management installation option. For installation steps, see Workstation Management in *Getting Started*.

Creating the Policy Packages

You should create an Organizational Unit (OU) for holding the policy packages. Consider the following when determining where to place this OU:

- If you have partitions in your tree

- The 256-character limit in NDS for the full distinguished name
- The Search policy is used to locate the policy package

To minimize tree walking, it is best to create this policy package OU at the root of the partition that contains the objects with which the policy package will be associated. In doing so, the following benefits are realized:

- Tree walking is minimized with the root of the partition and the Search policy being used
- Placing the OU at the partition's root maximizes the number of characters that will be available for naming plural policies

To create a policy package:

1. In ConsoleOne, right-click the container where you want the container for the policy packages placed > click New > click Object > click Organizational Unit > click OK.
2. Give the container a short name.

   HINT: Because you can have both ZfD and ZfS policies in the same tree, make sure you distinguish your ZfD policies container. For example, ZfD Policies.
3. Right-click the policy package's container > click New > click Policy Packages.
4. Select one of the following policy packages:

   Container Package
   Server Package
   Service Location Package
   User Package
   Workstation Package
5. Click Next > give the package a short name > click Next > click Create Another Policy Package (unless this is the last one being created) > click Finish.

   Short package name suggestions include:

   Container
   Server
   Location
   User
   Workstation
6. Repeat Step 4 through Step 5 for each policy package to be created.

Setting Up a Search Policy

The Search policy is required for finding other policies. You set up Search policies at a container level. Create as many Search policies as you will need to help minimize network traffic.

To create a Search policy:

1. In ConsoleOne, right-click the Container Package > click Properties.
2. Check the check box under the Enabled column for the Search policy.

   This both selects and enables the policy.
3. Click Properties.

   The Search Level tab is displayed.

4. Select the level to search up to:

   [Root]: Search to the root of the tree.

   Object Container: Search to the parent container.

   Partition: Search to the partition root.

   Selected Container: Search to the selected container.

5. If you chose Selected Container, browse to select the container.

6. To determine the searching limits in either direction, specify a number:

Number	Description
0	Limits the search to the selected level.
1	Limits the search to one level above the selected level. For example, if you selected the server's parent container, this would limit the search to one level above the parent level.
-1	Limits the search to one level below the selected level. For example, if you selected [Root], -1 would limit the search up to one level *below* [Root].

   You can specify any number between -25 and 25.

7. Click the Search Order tab > specify the policy searching order.

   Use the arrow keys, the Add button, and the Remove button as necessary to create your search order.

8. Click the Refresh Interval tab > specify the frequency for how often the policy should be refreshed.

   The default is hourly. If you set both time increments to zero (0), policies will never be refreshed.

9. Click OK.

10. Click the Associations tab > Add.

11. Browse to select the container object for association to the Search policy.

12. Click OK when finished.

Setting Up the Server Package Policies

Review the following sections to help you set up the Server Package policies:

- "Setting Up the Imaging Server Policy" on page 62
- "Setting Up the Workstation Import Policy" on page 62
- "Setting Up the Workstation Removal Policy" on page 64
- "Setting Up the Inventory Roll-Up Policy" on page 65
- "Associating the Server Package" on page 65

Setting Up the Imaging Server Policy

If you will be imaging workstations, configure and enable this policy. This section contains step-by-step information to set up the Imaging Server policy. For more detailed information on imaging, see Chapter 5, "Workstation Imaging," on page 109. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Imaging Server policy:

1. In ConsoleOne, right-click the Server Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.

2. Check the check box under the Enabled column for the Imaging Server policy.

   This both selects and enables the policy.

3. Click Properties.

4. Click the Image Selection tab > Rules.

5. Click Add > define the conditions under which the imaging server should lay down a particular image > click OK.

   For details on how to perform this task, click Help in the New Image Selection Rule dialog box.

6. Repeat the previous step as needed to provide rules that will cover all the target workstations.

7. Click OK to save the policy.

8. Repeat Step 1 through Step 7 for each platform where you want to set an Imaging Server policy.

9. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Server Package" on page 65 to associate the policy package.

Setting Up the Workstation Import Policy

You must configure and enable this policy to use the Automatic Workstation Import service. This section contains step-by-step information to set up the Workstation Import policy. For more detailed information, see Chapter 2, "Automatic Workstation Import and Removal," on page 27. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Workstation Import policy:

1. In ConsoleOne, right-click the Server Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.

2. Check the check box under the Enabled column for the Workstation Import policy.

   This both selects and enables the policy.

3. Click Properties.

   The Containers tab is displayed.

4. Click Add > select the NDS containers where rights are needed for creating Workstation objects > click OK.

5. Click the Limits tab > fill in the fields:

User Login Number: If the Workstation Import policy requires user information, this number represents the number of times the user can log in before the user's Workstation object is created.

Limit Number of Workstations Imported: To help balance server workload, enable this option to limit how many workstations are imported.

Workstations Created Per Hour: Specify the limit for how many Workstation objects can be created per hour.

6 Click the Platforms tab > click General, Win9x, or WinNT/2000, as applicable.

The Location page is displayed.

7 Fill in the fields:

Allow Importing of Workstations: Enable this option to allow registered workstations to be imported.

Create Workstation Objects In: Select an option from the drop-down list:

- **Selected Container:** The Workstation object will be created in the container specified in the Path field. This is an absolute NDS path.
- **Server Container:** The Workstation object will be created in the same container as the server running the import service. You can specify a relative path from the server container.
- **User Container:** The Workstation object will be created in the container where the User object resides for the logged-in user. You can specify a relative path from the user container.
- **Associated Object's Container:** The Workstation object will be created in the container that is associated with the Workstation Import policy. You can specify a relative path from the associated container.

Path: If you are using a relative path, enter a string. The number of periods you end the path with determines the number of relative levels. If you are using an absolute path, select the container.

8 Click the Naming page > fill in the fields:

Workstation Name: Displays the workstation naming convention currently defined in the Add Name Fields and Place Them in Order field. Whenever there is a potential name conflict (such as two Workstation objects in the same container named after the User object), the system will append a 3-digit number on the end of the name that you enter here.

Add Name Fields and Place Them in Order: You must have at least one option in this list. By default, there is one of two option pairs in the list, either Computer + Network Address or User + Network Address. Click Add to select from the following list of name fields:

<User Defined>	CPU	OS
Computer	DNS	Server
Container	Network Address	User

9 Click the Groups page > click Add > browse for the workstation groups you want this Workstation object to belong to when it is imported.

10 Click OK to save the policy.

11 Repeat Step 1 through Step 10 for each platform where you want to set a Workstation Import policy.

12 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Server Package" on page 65 to associate the policy package.

Setting Up the Workstation Removal Policy

If you want Workstation objects to be automatically removed after they have not been used for a specified period of time, configure and enable this policy. This section contains step-by-step information to set up the Workstation Removal policy. For more detailed information on workstation removal, see Chapter 2, "Automatic Workstation Import and Removal," on page 27. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Workstation Removal policy:

1 In ConsoleOne, right-click the Server Package > click Properties > click the appropriate platform page.

Policies set on a specific platform will override policies set on the General tab.

2 Check the check box under the Enabled column for the Workstation Removal policy.

This both selects and enables the policy.

3 Click Properties.

The Containers tab is displayed.

4 Click Add > select the containers where workstations to be removed reside.

5 To specify how long a Workstation object should remain in the tree without registering, click the Limits tab > specify the number of days.

6 To schedule when Workstation objects should be removed, click the Schedule tab > fill in the fields:

Year: Year to begin schedule.

Date: Day of month to begin schedule.

Start Time: Beginning time for the window when policy can run.

Duration: Length of the time window.

Repeat Interval In Days: Beginning from the starting date, Workstation object removal is performed at this interval.

Limit Number of Workstations Removed: To help balance server workload, enable this option to limit how many workstations are removed in a session.

Workstations Removed Per Session: A number to set the limit for how many Workstation objects can be removed per hour.

7 Click OK to save the policy.

8 Repeat Step 1 through Step 7 for each platform where you want to set a Workstation Removal policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Server Package" on page 65 to associate the policy package.

Setting Up the Inventory Roll-Up Policy

If you want to track workstation inventory information, configure and enable this policy. This section contains step-by-step information to set up the Inventory Roll-Up policy. For more detailed information on Inventory, see Chapter 7, "Workstation Inventory," on page 137. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Inventory Roll-Up policy:

1. In ConsoleOne, right-click the Server Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.

2. Check the check box under the Enabled column for the Inventory Roll-Up policy.

   This both selects and enables the policy.

3. Click Properties.

   The Roll-Up Policy tab is displayed.

4. Browse for the destination server object.

5. Click Roll-Up Policy > click Roll-Up Schedule > select the schedule:

   Daily
   Monthly
   Yearly
   Never

6. Click OK to save the policy.

7. Repeat Step 1 through Step 6 for each platform where you want to set an Inventory Roll-Up policy.

8. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Server Package" on page 65 to associate the policy package.

Associating the Server Package

The policies you configured and enabled will not be in effect until you associate their policy package with a container object.

To associate the Server Package:

1. In ConsoleOne, right-click the Server Package > click Properties.
2. Click the Associations tab > Add.
3. Browse for the container for associating the package > click OK.

Setting Up the Service Location Package Policies

Do the following to set up the Service Location Package policies:

- "Setting Up the SMTP Host Policy" on page 66
- "Setting Up the SNMP Trap Targets Policy" on page 66
- "Setting Up the ZENworks Database Policy" on page 66
- "Associating the Service Location Package" on page 69

Setting Up the SMTP Host Policy

If you want e-mail notifications, you should configure and enable this policy. For more information, see "SMTP Host" on page 51. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the SMTP Host policy:

1. In ConsoleOne, right-click the Service Location Package > click Properties.

   The General tab is displayed.

2. Check the check box under the Enabled column for the SMTP Host policy.

   This both selects and enables the policy.

3. Click Properties > enter the SMTP Host name > click OK.

4. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Service Location Package" on page 69 to associate the policy package.

Setting Up the SNMP Trap Targets Policy

If you are using SNMP, you should configure and enable this policy. For more information, see "SNMP Trap Targets" on page 51. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the SNMP Trap Targets policy:

1. In ConsoleOne, right-click the Service Location Package > click Properties.

   The General tab is displayed.

2. Check the check box under the Enabled column for the SNMP Trap Targets policy.

   This both selects and enables the policy.

3. Click Properties.

   The SNMP Trap Policy tab is displayed.

4. Click Add > enter a new target > click OK.

5. Repeat Step 4 for each trap target you need.

6. Click OK to save the policy.

7. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Service Location Package" on page 69 to associate the policy package.

Setting Up the ZENworks Database Policy

This policy identifies the location of the ZENworks Database object. If you selected to install the ZENworks database, you should configure and enable this policy.

If you are using a Sybase database, the Database object may have been installed with default property values, depending on whether you selected to install ZfD Inventory. In either case, follow the applicable steps under "Configuring the ZENworks Database Object for Sybase" on page 67, then continue with "Creating the ZENworks Database Policy" on page 68.

If you are using an Oracle database, you need to create the Database object and enter the required property values. In this case, follow the steps under "Configuring the ZENworks Database Object for Oracle" on page 67, then continue with "Creating the ZENworks Database Policy" on page 68.

Configuring the ZENworks Database Object for Sybase

To configure the ZENworks Database object:

1. In ConsoleOne, right-click the Database object > click Properties.

   The ZENworks Database tab should be displayed.

   HINT: While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

2. Fill in the applicable fields, keeping the user name and password pairs together:

   Database (Read-Write) User Name: Secures read and write access to the database file.

   Database (Read-Write) Password: Secures read and write access to the database file.

   Database (Read Only) User Name: Secures only read access to the database file.

   Database (Read Only) Password: Secures only read access to the database file.

   Database (Write Only) User Name: Secures only write access to the database file.

   Database (Write Only) Password: Secures only write access to the database file.

3. To change any default JDBC driver type information, click the JDBC Driver Information tab > edit the fields:

   Driver
   Protocol
   SubProtocol
   SubName
   Port
   SID Server Name

4. If you will use an ODBC driver for the database file, click the ODBC Driver Information tab > fill in the fields:

   Driver Filename
   Data Source Name
   Connection Parameters

5. Click OK to save the database property changes.

Continue with "Creating the ZENworks Database Policy" on page 68.

Configuring the ZENworks Database Object for Oracle

To create and configure the ZENworks Database object:

1. In ConsoleOne, right-click the container where the Database object is to be created > click New > click Object > click ZENworks Database > click OK.

   HINT: While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

2. Enter a name for the Database object > click Define Additional Properties > click OK.

   The ZENworks Database tab should be displayed.

3. Select the DN of the server where the database files will be stored.
4. (Optional) Enter the IP address of the server.
5. Fill in the applicable fields, keeping the user name and password pairs together:

   Database (Read-Write) User Name: Secures read and write access to the database file.

   Database (Read-Write) Password: Secures read and write access to the database file.

   Database (Read Only) User Name: Secures only read access to the database file.

   Database (Read Only) Password: Secures only read access to the database file.

   Database (Write Only) User Name: Secures only write access to the database file.

   Database (Write Only) Password: Secures only write access to the database file.
6. To specify the JDBC driver type, click the JDBC Driver Information tab > click the Populate Fields With Default Values For An Oracle Database radio button > click Populate Now.
7. To change any default JDBC driver type information, edit the fields:

   Driver
   Protocol
   SubProtocol
   SubName
   Port
8. If you will use an ODBC driver for the database file, click the ODBC Driver Information tab > fill in the fields:

   Driver Filename
   Data Source Name
   Connection Parameters
9. Click OK to save the database property changes.

Continue with "Creating the ZENworks Database Policy" on page 68.

Creating the ZENworks Database Policy

To create the ZENworks Database policy:

1. In ConsoleOne, right-click the Service Location Package > click Properties.

   The General tab is displayed.

   HINT: While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.
2. Check the check box under the Enabled column for the ZENworks Database policy.

   This both selects and enables the policy.
3. Click Properties.

   The ZfD Database tab is displayed.
4. Select the database DN > click OK.
5. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Service Location Package" on page 69 to associate the policy package.

Associating the Service Location Package

The policies you configured and enabled will not be in effect until you associate their policy package with a container object.

To associate the Service Location Package:

1. In ConsoleOne, right-click the Service Location Package > click Properties.
2. Click the Associations tab > Add.
3. Browse for the container for associating the package > click OK.

Setting Up the User Package Policies

Review the following sections for information to help you set up the User Package policies:

Setting Up the Desktop Preferences Policy

For the Windows 95/98 and Windows NT/2000 platforms, sets defaults for users' desktops. This section contains step-by-step information to set up the Desktop Preferences policy. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Desktop Preferences policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the Desktop Preferences policy.

   This both selects and enables the policy.
3. Click Properties.

   The Roaming Profiles tab is displayed.
4. To enable roaming profiles, check the Roaming Profiles box > set the desired parameters in the following fields:

   Override Terminal Server Profile: Stores the roaming profile on the network in the user's home directory.

Store User Profile in User's Home Directory: Stores the roaming profile on the network in the user's home directory. This allows the user to utilize the same desktop environment on all workstations throughout the network.

Find Profile in a NetWare File System Directory: The mandatory profile is found in a specific directory on a NetWare server. A mandatory profile requires all users to utilize the same desktop environment on all workstations throughout the network.

Path: Specify the user's home directory.

5. Click the Settings tab > click an icon to display a dialog box that shows the options available for each feature.

   This page displays icons matching the equivalent desktop features in Windows 95/98 or Windows NT/2000.

   See your Microsoft Windows documentation for help on these features and their options.

6. Click OK to save the policy.

7. Repeat Step 1 through Step 6 for each platform where you want to set desktop preferences.

8. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the Dynamic Local User Policy

For Windows NT/2000, lets you configure users created on Windows NT/2000 workstation after they have authenticated to NDS. This section contains step-by-step information to set up the Dynamic Local User policy. For more detailed information, see "Dynamic Local User" on page 51. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Dynamic Local User policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the Windows NT-2000 platform page.

2. Check the check box under the Enabled column for the Dynamic Local User policy.

   This both selects and enables the policy.

3. Click Properties.

   The Dynamic Local User tab is displayed.

4. Fill in the following fields:

   Enable Dynamic Local User: Enables creation of a User object that resides either temporarily or permanently in the workstation's Security Access Manager (SAM) database.

   Manage Existing NT Account (If Any): Allows management through the existing NT account.

   Use NetWare Credentials: Enables logging in through the user's NetWare credentials instead of NT credentials.

   Volatile User (Remove NT User After Logout): Specifies the use of a volatile user account for NT login.

   NT User Name: The NT user name. The NT user name (not including the context) must contain fewer than 20 characters for a dynamic local user to log in.

   A user that is manually created via User Manager can`t have a longer name.

Full Name: The user's full name.

Description: Enter any additional information that helps you to further identify this user account.

Member Of: Lists the groups where this user has membership.

Not Member Of: Lists available groups where this user has not been assigned as a member.

Custom: Opens the Custom Groups page, where you can add a new custom group, delete an existing custom group, and view or modify properties of an existing custom group.

5 Click OK to save the policy.

6 Repeat Step 1 through Step 5 for each platform where you want to set a Dynamic Local User policy.

7 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the Help Desk Policy

Sets the choices viewed in the Help Desk user interface. This policy is available on each of the platform pages. This section contains step-by-step information to set up the Help Desk policy. For more detailed information, see "Help Desk" on page 52. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Help Desk policy:

1 In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.

Policies set on a specific platform will override policies set on the General tab.

2 Check the check box under the Enabled column for the Help Desk policy.

This both selects and enables the policy.

3 Click Properties.

The Configuration tab is displayed.

4 To enable the Help Requester, fill in the fields:

Allow User to Launch the Help Requester: Users can run the Help Requester only if this option is checked.

Allow User to Send Trouble Tickets from the Help Requester: Disables the Mail For Help option in the user's Help Requester interface.

Trouble Ticket Delivery Mode: To specify e-mail delivery of help requests, select either GroupWise 5.0 or MAPI.

Trouble Ticket Subject Lines: Create a list of possible categories for help requests.

5 To configure what choices should be available to users, click the Configure Trouble Ticket tab > fill in the fields:

User Information: Check the box for each of the following user information items that you want to be available for sending with the trouble ticket:

User Context
User Tree
User Location

User Phone

Workstation Information: Check the box for each of the following workstation information items that you want to be available for sending with the trouble ticket:

Workstation ID
Workstation Tree
Workstation Inventory

6 Click the Information tab > fill in the fields:

Contact Name: The primary contact for help requests.

E-mail Address: The primary contact's e-mail address.

Telephone Number: The primary contact's telephone number.

7 Click OK to save the policy.

8 Repeat Step 1 through Step 7 for each platform where you want to set a Help Desk policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the NT User Printer Policy

For Windows NT/2000, sets parameters for printer drivers. This section contains step-by-step information to set up the NT User Printer policy. For more detailed information, see "User Printer" on page 53. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the NT User Printer policy:

1 In ConsoleOne, right-click the User Package > click Properties > click the Windows NT/2000 platform page.

2 Check the check box under the Enabled column for the NT User Printer policy.

This both selects and enables the policy.

3 Click Properties.

The Printer Entries tab is displayed.

4 To set printer configurations for users, fill in the fields:

Installed NetWare Printers: List of currently defined printers.

Toggle Default: Makes the selected printer the default.

New Driver: Opens the Driver dialog box, where you can assign a print driver.

NetWare Settings: Opens the Advanced Workstation Printer Options dialog box, where you can define various settings:

- **Output Settings:** Sets the following: number of copies, form feed, spaces for tabs, and number of spaces for tabs.
- **Banner Settings:** Sets the following: enable banners, first banner name, and second banner name.
- **Other Settings:** Sets the following: hold print jobs, keep print job in queue, and notify when print job is done.

5 Click OK to save the policy.

6 Repeat Step 1 through Step 5 for each platform where you want to set an NT User Printer policy.

7 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the Remote Control Policy

Sets parameters for remote management sessions. This policy is available on each of the platform pages. This section contains step-by-step information to set up the Remote Control policy. For more detailed information, see Chapter 6, "Remote Management," on page 125. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Remote Control policy:

1 In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.

Policies set on a specific platform will override policies set on the General tab.

2 Check the check box under the Enabled column for the Remote Control policy.

This both selects and enables the policy.

3 Click Properties.

The Remote Management tab is displayed.

4 On the General page, fill in the fields:

Enable Chat: Allows the administrator to chat with the user logged in to the managed workstation.

Enable Diagnostics: Allows the administrator to diagnose the managed workstation.

Remote Control/View Startup Timeout for Console User __ Minutes: The maximum duration of time to wait for connecting with the managed workstation to start a Remote Control or a Remote View session. The default timeout value is 5 minutes. The range is 1 to 30 minutes.

5 Click the Control page > fill in the fields:

Enable Remote Control: Allows the administrator to remotely control the managed workstation.

Prompt User for Permission to Remote Control: Click this option if you want the administrator to seek permission from the user at the managed workstation before initiating a remote control session.

Give User Audible Signal When Remote Controlled: Click this option if you want the management console to send an audible signal to the managed workstation every time the administrator remotely controls the managed workstation.

Every __ Seconds: The time interval for the management console to periodically send the audible signal to the managed workstation.

Give User Visible Signal When Remote Controlled: Click this option if you want the management console to send a visible signal to the managed workstation every time the administrator remotely controls the managed workstation.

Display Name of Initiator Every __ Seconds: The time interval for the management console to periodically send the visible signal to the managed workstation.

Allow Blanking User's Screen: Allows the administrator to blank the screen of the managed workstation during a remote control session.

Allow Locking User's Keyboard and Mouse: Allows the administrator to lock the keyboard and mouse controls of the managed workstation during a remote control session.

6 Click the View page > fill in the fields:

Enable Remote View: Allows the administrator to remotely view the desktop of the managed workstation.

Prompt User for Permission to Remote View: Click this option if you want the administrator to seek permission from the user at the managed workstation before initiating a remote view session with the managed workstation.

Give User Audible Signal When Remote Viewed: Click this option if you want the management console to send an audible signal to the managed workstation every time the administrator remotely views the managed workstation.

Every __ Seconds: Specify the time interval for the management console to periodically send the audible signal to the managed workstation.

Give User Visible Signal When Remote Viewed: Click this option if you want the management console to send a visible signal to the managed workstation every time the administrator remotely views the managed workstation.

Display Name of Initiator Every __ Seconds: Specify the time interval for the management console to periodically send the visible signal to the managed workstation.

7 Click the File Transfer page > fill in the fields:

Enable File Transfer: Choose to allow the administrator to transfer files between the management console and the managed workstation.

Prompt User for Permission to Transfer Files: Click this option if you want the administrator to seek permission from the user at the managed workstation before transferring files between the management console and the managed workstation.

8 Click the Remote Execute page > fill in the fields:

Enable Remote Execute: Choose to allow the administrator to execute applications or files on the managed workstation.

Prompt User for Permission to Remote Execute: Click this option if you want the administrator to seek permission from the user at the managed workstation before running applications or files at the managed workstation.

9 Click OK to save the policy.

10 Repeat Step 1 through Step 9 for each platform where you want to set a Remote Control policy.

11 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the Scheduled Action Policy

Sets up schedules for specific actions. This is a plural policy, meaning it can be added many times to the policy package. It is available for each of the platform pages. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Scheduled Action policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.

2. Check the check box under the Enabled column for the Scheduled Action policy.

   This both selects and enables the policy.

3. Click Properties.

   The Actions tab is displayed.

4. Fill in the fields:

   Name: The name that was entered in the Name field on the Item Properties tab when the action item was added.

   Working Directory: Generally, this is the path where the executable file for this action is located. It can be a different path if the program requires it.

   Parameters: The parameters to pass to the action item. For more information, see the documentation associated with the executable file specified in the Working Directory field.

   Priority: The importance assigned to this action in relation to the user's access to the workstation.

   Terminate Time: The length of time this action can run before the system stops it. The assumption is that if it takes longer than a specified time to run, there might be a problem associated with running this action and the action should be terminated. The length of time was specified under the Terminate Item If Still Running After check box on the Action Items tab when you added this action.

   Run Items in Order Listed: The items will run in the order they display in the list. You can reorder the list with the up/down arrows.

5. Click the Policy Schedule Tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly

6. Click OK to save the policy.

7. Repeat Step 1 through Step 6 for each platform where you want to set a Scheduled Action policy.

8. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the User Extensible Policy

Sets user-defined policies (from .ADM files) for user objects. This policy is found only on the WinNT-2000 and Win95-98 pages. This section contains step-by-step information to set up the User Extensible policy. For more detailed information, see "User Extensible" on page 53. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the User Extensible policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the User Extensible policy.

   This both selects and enables the policy.
3. Click Properties.

   The User Extensible Policies tab is displayed.
4. Click Add > browse for a .ADM file.
5. To edit the properties of a policy, click the policy in the ADM Files box > browse and edit the policy settings in the Policies box.

   Click the plus signs to expand the attributes.

   The check box states are as follows:

Check Box	State	Description
☑	Enabled	Attribute is enabled in the client. Any values you enter for it are applied.
☐	Disabled	Attribute is disabled in the client.
☑ or ☐	Ignored	Attribute is ignored (not changed in the client). If the attribute is already enabled in the client, it remains enabled. If it is already disabled in the client, it remains disabled.

6. Repeat Step 4 and Step 5 for each extensible policy to be added.
7. Click the Policy Schedule tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly
8. Click OK to save the policy.
9. Repeat Step 1 through Step 8 for each platform where you want to set a User Extensible policy.
10. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the User System Policy

This ZENworks 2 functionality is now a part of ZfD Extensible policies.

For Windows NT, use the COMMON.ADM, WINNT.ADM, and ZAKWINNT.ADM files in Extensible policies.

For Windows 95/98, use the ADMIN.ADM file in Extensible policies.

If this policy has been migrated from ZENworks 2, the functionality is enabled in ZfD but you cannot edit or modify the policy. If you want to change these settings, you must create a new User Package in ZfD and enable Extensible policies.

Setting Up the Windows 2000 Group Policy

Only for Windows 2000, this policy is an extension of extensible policies for Windows 2000 and Active Directory. This section contains step-by-step information to set up the Windows 2000 policy. For more detailed information, see "Windows 2000 Group" on page 54. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Windows 2000 Group policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the Windows NT/2000 platform page.
2. Check the check box under the Enabled column for the Windows 2000 Group policy.

   This both selects and enables the policy.
3. Click Properties.

   The Windows 2000 Group Policies tab is displayed.
4. Browse for an NDS policy directory > click Edit.

   This launches the Microsoft Management Console editor, where you can edit a User Package policy or a Workstation Package policy. For more information, click Help in the dialog boxes.
5. Click the Workstation Manager Policies tab > click Active Directory Group Policy Import > fill in the fields:

   Active Directory Policy Path: Specify the UNC path where group policies created by Active Directory exist that you want to migrate to NDS. You must know or browse for the Unique Name of the directory from where you will import the Active Directory group policy.

   NDS Policy Directory: Enter or browse for a target UNC path location on the NetWare server for migrating the Windows 2000 group policies into NDS from the location specified in the Active Directory Policy Path field. The User and Workstation objects must have Read and File Scan rights to this location.

   IMPORTANT: You should use UNC paths rather than mapped drives for Windows 2000 Group policies. For more information, see "Windows 2000 Group" on page 54.
6. If you enter information into the fields, click Import Files.

   This copies the Active Directory group policy to the directory specified in the NDS Policy Directory field. If the specified directory does not exist, it will be automatically created.

   WARNING: Make sure you have selected the correct directory path in the NDS Policy Directory field because you could destroy data. All of the files in the selected directory and any of its subdirectories will be deleted before the Active Directory group policy is copied to it.
7. Click the Policy Schedule tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly

You can click Advanced Settings to set additional settings such as Completion, Fault, Impersonation, Priority, and Time Limit. For detailed information on each of these settings, click the Help button on each tab.

IMPORTANT: The default Impersonation setting is Interactive User. If you change this setting the policy will not function properly.

8. Click OK to save the policy.
9. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Setting Up the Windows Terminal Server Policy

Only for Windows 2000, this policy sets parameters for Citrix and Microsoft Terminal Server users. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Windows Terminal Server policy:

1. In ConsoleOne, right-click the User Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the Windows Terminal Server policy.

   This both selects and enables the policy.
3. Click Properties.

   The Terminal Configuration Connection tab is displayed.
4. Fill in the fields:

   Allow Logon to Terminal Server: Lets the user log on to the Terminal Server.

   Broken or Timed-out Connections: Specifies settings for when a session limit is reached or connection is broken. Click Disconnect to disconnect the user from the session, allowing the session to be reconnected. Click End to end the session.

   Reconnect From: Reconnects disconnected sessions from any client (lets the user reconnect to a disconnected session from any computer) or from the previous client (lets the user reconnect to a disconnected session only from the client computer where the session originated).

   Timeout Settings (in minutes): Sets timeout options for disconnected, active, and idle sessions.

   - **Connection:** Specify the amount of time a user's session can remain active on the server. When the time limit is reached, the user is either disconnected from the session or the session ends.
   - **Disconnection:** Specify the amount of time that a disconnected session remains on the server. When the time limit is reached, the disconnected session ends.
   - **Idle:** Specify the amount of time that an idle session (a session without client activity) remains on the server. When the time limit is reached, the user is either disconnected from the session or the session ends.

   Shadowing: Session shadowing lets you monitor the display of another active session, see what users are doing, and interact with a user's session using the keyboard and mouse. You can shadow active sessions on the same server or on other Citrix servers.

   - **Enabled:** Specifies that sessions on the connection can be shadowed.

- **Allow Input:** Allows the shadower to input keyboard and mouse actions to the shadowed session.
- **Notify Client:** Specifies that the shadowed user gets a message asking if it is permissible for the shadowing to occur.

Modem Callback: Use this option to configure asynchronous ICS connections to hang up and dial a preset or user-specified number after a user logs on to the Citrix server.

- **Enabled:** Enables modem callback.
- **Phone Number:** Enter the callback phone number.
- **Roving Phone Number:** Prompts users to enter a callback number when they start an async session. You can use this option to centralize telephone charges.

5 Click the Terminal Configuration tab > click Login > fill in the fields:

Initial Program: Use the following settings to configure an initial program for the connection.

- **Command Line:** Enter the path and filename of the program that you want to start when the user logs on to the Terminal Server.
- **Working Directory:** Specifies the working directory path for the program.
- **Inherit Client Configuration:** If this option is checked, the client settings in User Manager are used.

Client Devices: Controls client device mappings. The Client Devices options control whether drives and printers are mapped to client drives and printers. If these options are cleared, the devices are still available but must be manually mapped to drive letters and port names.

- **Connect Client Drives at Logon:** Automatically maps the client computer's drives at logon.
- **Connect Client Printers at Logon:** Automatically maps the client computer's printers at logon. This applies only to Windows clients and maps only printers already configured in Print Manager on the client computer. DOS printers must be manually mapped.
- **Default to Main Client Printer:** Configures the user's default client printer as the default printer for the ICA session.

Terminal Server Home Directory: Specify the user's Terminal Server home directory.

- **Local Path:** Sets the Terminal Server home directory to the local path you specify.
- **Connect:** Sets the Terminal Server home directory to the drive you specify. Choose a driver from the drop-down list, then enter a path.

Terminal Server Profile Path: Specify the user's Terminal Server profile path.

6 Click OK to save the policy.

7 Repeat Step 1 through Step 6 for each platform where you want to set a Windows Terminal Server policy.

8 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the User Package" on page 79 to associate the policy package.

Associating the User Package

The policies you configured and enabled will not be in effect until you associate their policy package with a container object.

To associate the User Package:

1. In ConsoleOne, right-click the User Package > click Properties.
2. Click the Associations tab > Add.
3. Browse for the container for associating the package > click OK.

Setting Up the Workstation Package Policies

Review the following section for more information to help you set up the Workstation Package policies:

Setting Up the Client Configuration Policy

Sets configuration parameters for workstations. This policy is found only on the WinNT-2000 and Win95-98 pages. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Client Configuration policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the Client Configuration policy.

   This both selects and enables the policy.
3. Click Properties.

   The Novell Client Configuration Client tab is displayed.
4. Click Help in this dialog box for instructions on how to configure the policy.
5. When you have finished configuring the policy, click OK.
6. Repeat Step 1 through Step 5 for each platform where you want to set a Client Configuration policy.
7. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Computer Extensible Policy

Sets user-defined policies (from .ADM files) for Workstation objects. This policy is found only on the WinNT/2000 and Win95/98 pages.

To create the Computer Extensible policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the Computer Extensible policy.

   This both selects and enables the policy.
3. Click Properties.

   The Computer Extensible Policies tab is displayed.
4. Click Add > browse for a .ADM file.
5. To edit the properties of a policy, click the policy in the ADM Files box > browse and edit the policy settings in the Policies box.

   Click the plus signs to expand the attributes.

   The check box states are as follows:

Check Box	State	Description
☑	Enabled	Attribute is enabled in the client. Any values you enter for it are applied.
☐	Disabled	Attribute is disabled in the client.
☑ or ☐	Ignored	Attribute is ignored (not changed in the client). If the attribute is already enabled in the client, it remains enabled. If it is already disabled in the client, it remains disabled.

6. Repeat Step 4 and Step 5 for each extensible policy to be added.
7. Click the Policy Schedule tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly
8. Click OK to save the policy.
9. Repeat Step 1 through Step 8 for each platform where you want to set a Computer Extensible policy.
10. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Computer Printer Policy

Sets workstation parameters for printing. This policy is found only on the WinNT/2000 and Win95/98 pages. This section contains step-by-step information to set up the Computer Printer policy. For more detailed information, see "Computer Printer" on page 55. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Computer Printer policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the Computer Printer policy.

   This both selects and enables the policy.
3. Click Properties.

   The Printer Entries tab is displayed.
4. To set printer configurations for users, fill in the fields:

   Installed NetWare Printers: List of currently defined printers.

   Toggle Default: Makes the selected printer the default.

   New Driver: Opens the Driver dialog box, where you can assign a print driver.

   NetWare Settings: Opens the Advanced Workstation Printer Options dialog box, where you can define various settings:

   - **Output Settings:** Sets the following: number of copies, form feed, spaces for tabs, and number of spaces for tabs.
   - **Banner Settings:** Sets the following: enable banners, first banner name, and second banner name.
   - **Other Settings:** Sets the following: hold print jobs, keep print job in queue, and notify when print job is done.
5. Click OK to save the policy.
6. Repeat Step 1 through Step 8 for each platform where you want to set a Computer Printer policy.
7. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Computer System Policy

This ZENworks 2 functionality is now a part of ZfD Extensible policies.

For Windows NT, use the COMMON.ADM, WINNT.ADM, and ZAKWINNT.ADM files in Extensible policies.

For Windows 95/98, use the ADMIN.ADM file in Extensible policies.

If this policy has been migrated from ZENworks 2, the functionality is enabled in ZfD but you cannot edit or modify the policy. If you want to change these settings, you must create a new User Package in ZfD and enable Extensible policies.

Setting Up the RAS Configuration Policy

Sets dial-up networking parameters. This policy is found only on the WinNT-2000 and Win95-98 pages. This section contains step-by-step information to set up the RAS Configuration policy. For more detailed information, see "RAS Configuration" on page 56. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the RAS Configuration policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.
2. Check the check box under the Enabled column for the RAS Configuration policy.

   This both selects and enables the policy.
3. Click Properties.

   The RAS Phonebook Entries tab is displayed.
4. Click Help for information on filling in the fields for this tab.
5. Click the Policy Schedule Tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly
6. Click OK to save the policy.
7. Repeat Step 1 through Step 6 for each platform where you want to set a RAS Configuration policy.
8. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Remote Control Policy

Sets parameters for managing remote user functions. This policy is found on each of the pages. This section contains step-by-step information to set up the Remote Control policy. For more detailed information, see Chapter 6, "Remote Management," on page 125. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Remote Control policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.
2. Check the check box under the Enabled column for the Remote Control policy.

   This both selects and enables the policy.
3. Click Properties.

   The Remote Management tab is displayed.

4 On the General page, fill in the fields:

Enable Chat: Allows the administrator to chat with the user logged in to the managed workstation.

Enable Diagnostics: Allows the administrator to diagnose the managed workstation.

Display Remote Management Agent Icon to Users: Click this option if you want to display the Remote Management Agent icon in the task bar of the Windows 95, Windows 98, Windows NT, or Windows 2000 managed workstation on which the Remote Management Agent is installed and running.

Default protocol to use for Remote Control and Remote View: Select the preferred protocol to use for communication between the managed workstation and the management console during Remote Control and Remote View sessions.

5 Click the Control page > fill in the fields:

Enable Remote Control: Allows the administrator to remotely control the managed workstation.

Prompt User for Permission to Remote Control: Click this option if you want the administrator to seek permission from the user at the managed workstation before initiating a remote control session.

Give User Audible Signal When Remote Controlled: Click this option if you want the management console to send an audible signal to the managed workstation every time the administrator remotely controls the managed workstation.

Every __ Seconds: The time interval for the management console to periodically send the audible signal to the managed workstation.

Give User Visible Signal When Remote Controlled: Click this option if you want the management console to send a visible signal to the managed workstation every time the administrator remotely controls the managed workstation.

Display Name of Initiator Every __ Seconds: The time interval for the management console to periodically send the visible signal to the managed workstation.

Allow Blanking User's Screen: Allows the administrator to blank the screen of the managed workstation during a remote control session.

Allow Locking User's Keyboard and Mouse: Allows the administrator to lock the keyboard and mouse controls of the managed workstation during a remote control session.

6 Click the View page > fill in the fields:

Enable Remote View: Allows the administrator to remotely view the desktop of the managed workstation.

Prompt User for Permission to Remote View: Click this option if you want the administrator to seek permission from the user at the managed workstation before initiating a remote view session with the managed workstation.

Give User Audible Signal When Remote Viewed: Click this option if you want the management console to send an audible signal to the managed workstation every time the administrator remotely views the managed workstation.

Every __ Seconds: Specify the time interval for the management console to periodically send the audible signal to the managed workstation.

Give User Visible Signal When Remote Viewed: Click this option if you want the management console to send a visible signal to the managed workstation every time the administrator remotely views the managed workstation.

Display Name of Initiator Every __ Seconds: Specify the time interval for the management console to periodically send the visible signal to the managed workstation.

7. Click the File Transfer page > fill in the fields:

   Enable File Transfer: Choose to allow the administrator to transfer files between the management console and the managed workstation.

   Prompt User for Permission to Transfer Files: Click this option if you want the administrator to seek permission from the user at the managed workstation before transferring files between the management console and the managed workstation.

8. Click the Remote Execute page > fill in the fields:

   Enable Remote Execute: Choose to allow the administrator to execute applications or files on the managed workstation.

   Prompt User for Permission to Remote Execute: Click this option if you want the administrator to seek permission from the user at the managed workstation before running applications or files at the managed workstation.

9. Click OK to save the policy.

10. Repeat Step 1 through Step 9 for each platform where you want to set a Remote Control policy.

11. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Scheduled Action Policy

Sets up schedules for specific actions. This plural policy can be added multiple times to each of the platform pages. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Scheduled Action policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.

   Policies set on a specific platform will override policies set on the General tab.

2. Check the check box under the Enabled column for the Scheduled Action policy.

   This both selects and enables the policy.

3. Click Properties.

   The Actions tab is displayed.

4. Fill in the fields:

   Name: The name that was entered in the Name field on the Item Properties tab when the action item was added.

   Working Directory: Generally, this is the path where the executable file for this action is located. It can be a different path if the program requires it.

Parameters: The parameters to pass to the action item. For more information, see the documentation associated with the executable file specified in the Working Directory field.

Priority: The importance assigned to this action in relation to the user's access to the workstation.

Terminate Time: The length of time this action can run before the system stops it. The assumption is that if it takes longer than a specified time to run, there might be a problem associated with running this action and the action should be terminated. The length of time was specified under the Terminate Item If Still Running After check box on the Action Items tab when you added this action.

Run Items in Order Listed: The items will run in the order they display in the list. You can reorder the list with the up/down arrows.

5. Click the Policy Schedule Tab > select a schedule type:

   Package Schedule
   Event
   Daily
   Weekly
   Monthly
   Yearly

6. Click OK to save the policy.

7. Repeat Step 1 through Step 6 for each platform where you want to set a Scheduled Action policy.

8. When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Windows 2000 Group Policy

Only for Windows 2000, this policy is an extension of extensible policies for Windows 2000 and Active Directory. This section contains step-by-step information to set up the Windows 2000 Group policy. For more detailed information, see "Windows 2000 Group" on page 57. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Windows 2000 Group policy:

1. In ConsoleOne, right-click the Workstation Package > click Properties > click the Windows NT/2000 platform page.

2. Check the check box under the Enabled column for the Windows 2000 Group policy.

   This both selects and enables the policy.

3. Click Properties.

   The Windows 2000 Group Policies tab is displayed.

4. Browse for an NDS Policy Directory > click Edit.

   This launches the Microsoft Management Console editor, where you can edit a User Package policy or a Workstation Package policy. For more information, click Help in the dialog boxes.

5. Click the Workstation Manager Policies tab > click Active Directory Group Policy Import > fill in the fields:

Active Directory Policy Path: Specify the UNC path where group policies created by Active Directory exist that you want to migrate to NDS. You must know or browse for the Unique Name of the directory from where you will import the Active Directory group policy.

NDS Policy Directory: Enter or browse for a target UNC path location on the NetWare server for migrating the Windows 2000 group policies into NDS from the location specified in the Active Directory Policy Path field. The User and Workstation objects must have Read and File Scan rights to this location.

IMPORTANT: You should use UNC paths rather than mapped drives for Windows 2000 Group policies. For more information, see "Windows 2000 Group" on page 57.

6 If you enter information into the fields, click Import Files.

This copies the Active Directory group policy to the directory specified in the NDS Policy Directory field. If the specified directory does not exist, it will be automatically created.

WARNING: Make sure you have selected the correct directory path in the NDS Policy Directory field because you could destroy data. All of the files in the selected directory and any of its subdirectories will be deleted before the Active Directory group policy is copied to it.

7 Click the Policy Schedule tab > select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

You can click Advanced Settings to set additional settings such as Completion, Fault, Impersonation, Priority, and Time Limit. For detailed information on each of these settings, click the Help button on each tab.

IMPORTANT: The default Impersonation setting is System. If you change this setting the policy will not function properly.

8 Click OK to save the policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Workstation Imaging Policy

Sets the parameters for imaging workstations. This policy is found on each of the platform pages. This section contains step-by-step information to set up the Workstation Imaging policy. For more detailed information, see Chapter 5, "Workstation Imaging," on page 109. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Workstation Imaging policy:

1 In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.

Policies set on a specific platform will override policies set on the General tab.

2 Check the check box under the Enabled column for the Workstation Imaging policy.

This both selects and enables the policy.

3 Click Properties.

The Image Selection Rules tab is displayed.

4 Click Add > define the conditions under which the imaging server should lay down a particular image > click OK.

For details on how to perform this task, click Help in the New Image Selection Rule dialog box.

5 Repeat the previous step as needed to provide rules that will cover all the target workstations.

6 Click OK to save the policy.

7 Repeat Step 1 through Step 6 for each platform where you want to set a Workstation Imaging policy.

8 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the Workstation Inventory Policy

Sets what hardware and software inventory data you want to view for each workstation.This policy is found only on the WinNT-2000 and Win95-98 pages. This section contains step-by-step information to set up the Workstation Inventory policy. For more detailed information, see Chapter 7, "Workstation Inventory," on page 137. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the Workstation Inventory policy:

1 In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.

2 Check the check box under the Enabled column for the Workstation Inventory policy.

This both selects and enables the policy.

3 Click Properties.

The Workstation Inventory Policy tab is displayed. Use this tab to:

- Specify the DN name of the Inventory server
- Enable or disable software scanning of workstations associated with this Inventory Policy

4 Fill in the fields:

Inventory Service: Specify the DN of the Inventory server. An Inventory server has a list of workstations attached to it.

Software Scanning:

- **Enable Software Scan:** Click this option to specify software scanning for the workstations associated with the Inventory Policy. The Scan programs collect software information for the workstation only if this option is enabled.
- **Custom Scan Editor:** Click this option to customize the list of software applications to scan for at the workstations associated with the Inventory Policy. Use the Custom Scan Editor to maintain the list of software applications that you want to scan for at the workstations.

5 Click the Policy Schedule tab > select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

6 Click OK to save the policy.

7 Repeat Step 1 through Step 6 for each platform where you want to set a Workstation Inventory policy.

8 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Setting Up the WS Restrict Login Policy

Sets parameters to restrict logging in by a workstation. This policy is found only on the WinNT-2000 and Win95-98 pages. While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

To create the WS Restrict Login policy:

1 In ConsoleOne, right-click the Workstation Package > click Properties > click the appropriate platform page.

2 Check the check box under the Enabled column for the WS Restrict Login policy.

This both selects and enables the policy.

3 Click Properties.

The Restrict Login tab is displayed.

4 Use the Add and Delete buttons to add users to either list.

The Excluded Users list contains the users that you want to exclude Dynamic Local User (DLU) access to. Users listed in this box cannot use DLU access. You can make exceptions for individual users by listing them in the Included Users list. This will allow DLU access to those users only, while excluding DLU access to the remaining users in the container.

The Included Users lists contains the users that you want to allow DLU access to. Users listed in this box can use DLU access. You can make exceptions for individual users by listing them in the Excluded User list. This will exclude DLU access to those users only, while allowing DLU access to the remaining users in the container.

5 Click the Restrict Login tab > click Inclusions > click Add > browse for NDS objects for which you want to specifically allow login.

6 Click OK to save the policy.

7 Repeat Step 1 through Step 6 for each platform where you want to set a WS Restrict Login policy.

8 When you have finished configuring all of the policies for this package, continue with the steps under "Associating the Workstation Package" on page 90 to associate the policy package.

Associating the Workstation Package

The policies you configured and enabled will not be in effect until you associate their policy package with a container object.

To associate the Workstation Package:

1. In ConsoleOne, right-click the Workstation Package > click Properties.
2. Click the Associations tab > Add.
3. Browse for the container for associating the package > click OK.

Migrating ZENworks 2 Policies

When you migrate ZENworks 2 policies to ZfD, they are migrated into the new policy packages. You cannot choose which packages the policies are migrated to. However, you can select the context so that you can migrate your policies in phases.

For more information, see "Determining Whether to Migrate Older Policies" on page 58.

To migrate ZENworks 2 policies:

1. In ConsoleOne, click Tools > ZENworks Utilities > Migrate Legacy Policy Packages.
2. In the Migrate From field, browse for a context that contains policy packages.

   The policy packages contained directly within this context will be migrated.
3. To include all policies in subcontainers for the selected context, click Include Subcontainers.

   The policy packages contained in all of the subcontainers under the context you selected in Step 2 will be migrated.
4. To preview the migration results, click Preview Only.

   IMPORTANT: We highly recommend using this option. It allows you to see exactly which policies are being migrated and how they are being migrated.
5. Click OK to begin the migration process.

4 Application Management

Using ZENworks® for Desktops (ZfD) Application Management and NDS®, you can easily distribute applications to workstations and then manage those applications. The following sections provide information to help you plan and deploy Application Management.

If you have not already completed the instructions in Application Management in *ZENworks for Desktops Getting Started*, you should do so before beginning deployment. *Getting Started* provides basic information about Application Management as well as instructions for setting up and testing Application Management in a single-server environment. The experience you gain by completing the tasks in *Getting Started* will help you successfully deploy Application Management in your more complex production environment.

Planning Application Management Deployment

Before you begin deploying Application Management, you should review the sections listed below. These sections provide information regarding issues such as where you should install the Application Management software, how you should organize Application objects in NDS, where you should store application installation files, and whether you should use Novell® Application Launcher™ or Application Explorer.

Selecting NDS Trees and Network Servers

Application Management requires schema extensions to NDS to support new NDS objects and properties. If you have more than one NDS tree, you should extend the schema of all trees where you want to implement Application Management. The installation program lets you extend the schema of one tree at a time. To extend a tree's schema, you must 1) be authenticated to the tree and 2) have Admin equivalent rights to the root.

You also need to decide which servers to install the Application Management software to. The Application Management software consists of three main components: the Application

Management snap-in for ConsoleOne®, the snAppShot™ utility, and the Application Launcher and Application Explorer applications.

When you install the Application Management software to a server, all three components are installed. You cannot install specific components only. Because of this, you will want to install the software to any server where:

- You plan to run ConsoleOne to administer Application Management
- You want to run snAppshot to create installation packages
- You want users to be able to run Application Launcher/Explorer

The Application Management software requires approximately 28 MB of free space on the server.

The installation program lets you install to any servers located in the NDS tree you've selected.

Organizing Application Objects in NDS

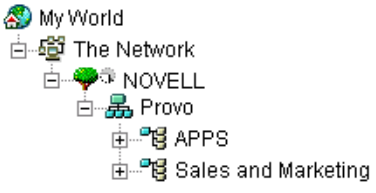
Every application you distribute to users must have a corresponding Application object in NDS. The Application object lets you determine the characteristics and behaviors associated with distributing, caching, and uninstalling the application.

When deploying Application Management, you need to consider where to place Application objects in NDS. The primary principle to follow is that an Application object should be placed in a container at the same site as the application's users. The following two sections provide examples:

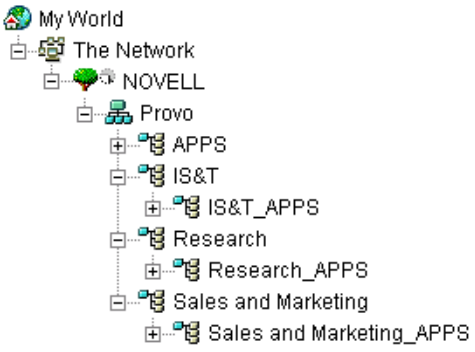
- "Single Site" on page 92
- "Multiple Sites" on page 93

Single Site

If your NDS tree encompasses one site only, you can place Application objects in any container. For example, if you have a small site consisting of one or two organizations, you may want to create a common APPS container.

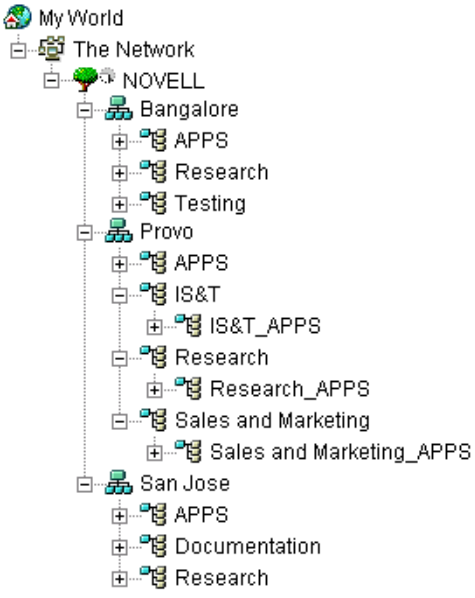


If your site is divided into many organizations, you may want to create a general APPS container for your corporate-wide Application objects and then create APPS containers within each organization container for the organization-specific applications.



Multiple Sites

If your NDS tree encompasses several sites, we recommend that you place your Application objects in the NDS tree at the same site as the users who will be using them. Typically, this will mean that you have APPS containers at multiple sites, as shown below.



In the above example, the NDS tree has been established geographically, with each Organization container comprising a different site. Ideally, this is the most efficient way to organize your NDS tree. If you have not organized your NDS tree by geographical location, you can still place Application objects in the same location as the users who will access them, but you will need to discover these locations.

Undoubtedly, you will have an application that you need to distribute to users at all your sites. In this case, you should create multiple Application objects (at least one at each site) for the application.

When giving users access to the application, you would associate the users with the Application object located at their site. Ensuring that users are accessing applications at their own site speeds user access to the applications and reduces cross-site network traffic.

If you have users who travel from site to site, you can set up site lists for any applications you want them to have access to at all sites. An application site list ensures that the user is accessing the

application from the site where he or she is located, regardless of which Application object the user has been associated with. For more information about site lists, see Application Object Settings in *ZENworks for Desktops 3.2 Administration Guide*.

Storing Application Installation Packages

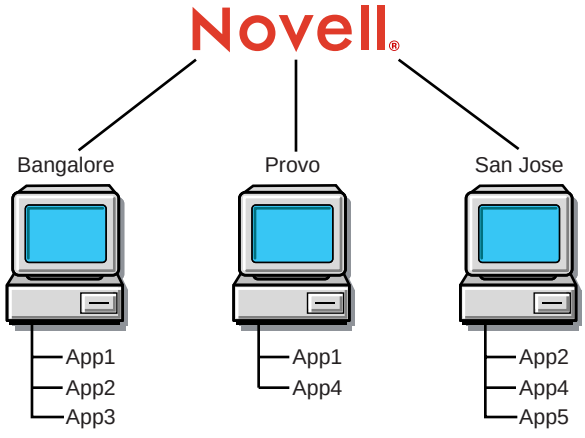
An NDS Application object contains the information required to distribute the application to users. Most applications you distribute will also require either a snAppShot installation package (.AOT, .AXT, .FIL, and .TXT files) or a Microsoft* Windows* Installer package (.MSI and associated files). An installation package contains the actual files that Application Launcher/Explorer will use to install the application to users' workstations. For Application Launcher/Explorer to access an installation package, the package must be located on a network server.

When deciding where to store installation packages, consider the following:

- "Location of the Application's Users" on page 94
- "Application Disk Space Requirements" on page 94
- "Fault Tolerance and Load Balancing Requirements" on page 95

Location of the Application's Users

The same principle that applies to Application objects applies to application installation packages. A package should be located at the same site as the application's users. This reduces cross-site network traffic and decreases the amount of time required to access the application.



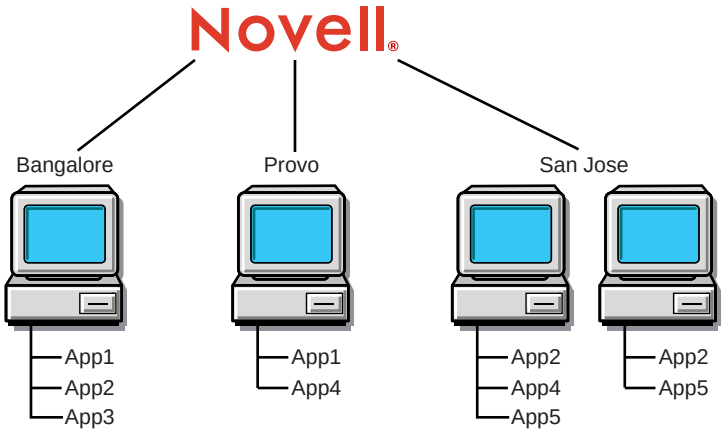
In the above example, App1 is used at both the Bangalore and Provo sites, so App1's application installation package is stored at each site. The same is true of App2 (Provo and San Jose) and App4 (Bangalore and San Jose).

Application Disk Space Requirements

Disk space requirements for installation packages vary. However, many packages can require substantial amounts of disk space. For example, a package for Microsoft Word requires approximately 400 MB on a server. You need to ensure that the server where you want to place your installation packages has sufficient disk space.

Fault Tolerance and Load Balancing Requirements

If you want to use Application Management's fault tolerance and load balancing features, you will need to store an application's installation package on multiple servers. In the following example, App2 and App5 are stored on two different servers at the San Jose site.



You should ensure that each server has sufficient disk space for the applications. For more information about fault tolerance and load balancing, see Application Object Settings in *ZENworks for Desktops 3.2 Administration Guide*.

Using Application Launcher or Application Explorer

To receive distributed applications, users must have either Application Launcher or Application Explorer running on their workstations.

Both Application Launcher and Application Explorer can be used on Windows 95/98 and Windows NT*/2000 workstations. The main difference is that Application Launcher can replace the Windows desktop, providing greater administrative control of users' workstations, while Application Explorer extends the Windows desktop and allows users to access Application objects from multiple locations (Quick Launch toolbar, system tray, desktop, and so forth).

Depending on your needs or your users' needs, you may want some users to run Application Launcher and some users to run Application Explorer. You can accomplish this by configuring users' login scripts to launch the appropriate application executable. See "Starting Application Launcher and Application Explorer" on page 101 for more information.

IMPORTANT: Users who plan to run in disconnected mode (disconnected from NDS) must connect to NDS and the network at least one time to have Application Launcher/Explorer copied to their computers.

Users should not run both Application Launcher and Application Explorer on the same workstation at the same time, unless you run Application Launcher as the Windows shell and then start Application Explorer using the I/ startup switch (NAL.EXE /I) through the login script.

For information about using Application Launcher as the Windows shell, see Using Application Launcher as the Windows Shell in Setting Up Application Launcher/Explorer in Application Management in the *ZENworks for Desktops 3.2 Administration Guide* guide.

For information about Application Explorer startup switches, see Application Launcher/Explorer Command Line Switches in Setting Up Application Launcher/Explorer in Application Management in the *ZENworks for Desktops 3.2 Administration Guide* guide.

Associating Applications with Users or Workstations

To give users access to applications, you associate the applications with the users or with the users' workstations. When you associate an application with a user, the application is available to the user regardless of the workstation from which the user logs in to NDS. When you associate an application with a workstation, the application is available on that workstation only.

Associating applications with users is the most common way to distribute applications. If you choose to associate applications with workstations, you should be aware of the following:

- Each workstation that will be associated with applications must first be imported into NDS as a Workstation object. For details about importing workstations, see Chapter 2, "Automatic Workstation Import and Removal," on page 27.
- Users must be trustees of the Application object. Trustee rights are not granted automatically; you must use ConsoleOne to manually give default trustee rights to each user who will run the application on the workstation.
- Users must run Application Launcher/Explorer to see applications that have been associated with the workstation, but they do not need to be logged in to NDS. The Workstation Manager, which is installed when the workstation is imported into NDS, retrieves workstation-associated applications from NDS but has no way to display them. Instead, Workstation Manager passes the list of workstation-associated applications to Application Launcher/Explorer, which can then display the applications.
- Application Launcher/Explorer will display applications that are associated with the workstation and applications that are associated with the user logged in to NDS at the workstation. This enables you to configure applications you want on the workstation regardless of the user who logs in, while still providing individual users with access to their specific applications.

For more information about associating applications with users or workstations, see Distributing Applications in *ZENworks for Desktops 3.2 Administration Guide*.

Distributing Applications in a Terminal Server Environment

Application Management supports application distribution to users running in a Microsoft Windows Terminal Server or Citrix* MetaFrame environment. When using a terminal server, you should consider the following:

- **Novell Client and Application Launcher/Explorer:** The Novell® Client™ must be installed on the terminal server so that users can log in to NDS when they access the terminal server. Application Launcher/Explorer should be included in each user's login script so that it is started when a user logs in to NDS. For additional information about starting Application Launcher/Explorer, see "Starting Application Launcher and Application Explorer" on page 101.
- **Software Distribution:** You can configure an Application object so that the application will be installed to the terminal server one time (in a standard location) or once for each user (in a non-standard location such as a user directory). The method you choose depends on the application requirements and how you want to utilize the terminal server's resources.

  To install a Microsoft Windows Installer package (.MSI and associated files) on the terminal server, the user must be a member of the Administrators group. Microsoft Windows Installer does not allow non-administrator users to do installations from a terminal client session.

- **User Associations:** An application must be associated with terminal server users through their User objects and the Application object in NDS. This process is identical to associating the application to non-terminal server users.
- **Multiple Users with the Same NDS Username:** If you have multiple users on the same terminal server who log in to NDS via the same User object, you need to make sure to configure Application Launcher/Explorer to not remove the icons from a user's desktop when he or she exits Application Launcher/Explorer. Otherwise, the icons will disappear from the desktops of all users who are logged in through the same User object. This is configured through the Application Launcher/Explorer's Enable Automatic Icon Cleanup option (ConsoleOne > User object > Application Launcher tab > Launcher Configuration page > Edit > User page). For additional information, see Configuring Application Launcher/Explorer in Setting Up Application Launcher/Explorer in Application Management in the *ZENworks for Desktops 3.2 Administration Guide* guide.

Metering Software Licenses

Application Management integrates with Novell Licensing Services (NLS) to enable you to track an application's usage and comply with the application's license agreement. When a user launches an application that has been configured as part of NLS, Application Launcher/Explorer checks to make sure that a license is available before running the application.

To use Application Management's software metering, you need to:

- Install Novell Licensing Services (NLS). NLS is included with NetWare® 4.*x*, 5.*x*, and 6, and with Novell Cluster Services™. For more information about NLS, see the Novell Documentation Web site (http://www.novell.com/documentation).
- Create a License container and a Metered Certificate for each application you want to track.
- Configure the Application object in NDS to use NLS and software metering. For details, see Metering Software Licenses in *ZENworks for Desktops 3.2 Administration Guide*.

Because NLS administration is performed through NetWare Administrator, software metering is not available in a pure Windows 2000 environment.

As you install NLS, you should follow the installation and deployment guidelines provided in the NLS documentation (http://www.novell.com/documentation). NLS does not need to be installed before you deploy Application Management. You can, at any time, start using NLS in combination with Application Management to meter software licenses.

Reporting Application Management Events

Application Management supports reporting on the success or failure of the following events:

- Launching of an application
- Distribution of an application
- Filtering of an application when the workstation does not meet the application's system requirements
- Removal of an application (uninstall)
- Caching of an application's installation source files

The above events can be recorded using one or any combination of the following reporting methods:

Sending Events to a Database

Application Launcher/Explorer can record events to most ODBC-compatible databases, provided:

- Each user's workstation has the correct database driver installed.
- The connection is configured correctly in NDS.

ZfD includes a Sybase* database that you can install. Sybase is also used for the Workstation Inventory database. If you plan to use a database for Application Management reports and you also plan to use Workstation Inventory, you can use the same database installation for both purposes.

NOTE: While the same database installation can be used for both Application Management and Workstation Inventory, each component still uses its own database file. Application Management creates a NAL.DB database file and Workstation Inventory creates a MGMTDB.DB database file.

Because the main requirement for Application Management reporting is that the database be at the same site as the users, you should follow the instructions provided for Workstation Inventory to deploy your databases, and then choose one or more database to use for Application Management reporting. For information about Workstation Inventory deployment, see Chapter 7, "Workstation Inventory," on page 137.

The Sybase database installation requires approximately 19 MB on a network server. However, as with all reporting databases, the database can expand rapidly to consume large amounts of disk space.

Detailed instructions for setting up database reporting are included in "Setting Up Database Reporting" on page 103.

Sending Events as SNMP Traps

If you use a management console to collect SNMP traps, you can have Application Launcher/Explorer send SNMP traps to the console. The use of SNMP traps requires the following:

- A Service Location Package in NDS to be associated with the containers where Application objects reside
- An SNMP Trap Targets policy to be defined in the Service Location Package
- The SNMP Trap Targets policy to include the SNMP trap targets (IP addresses) for the locations you want the traps sent

Detailed instructions for setting up SNMP traps reporting are included in "Setting Up SNMP Trap Reporting" on page 106.

Sending Events to a Log File

You can have Application Launcher/Explorer record events to a log file. This can be an individual log file located on the user's workstation or a common log file on a network server. When using a common log file, users must be given Read and Write rights to the log file, but Application Launcher/Explorer will automatically authenticate them to the log file location.

Detailed instructions for setting up log file reporting are included in "Setting Up Log File Reporting" on page 107.

Deploying Application Management

The following sections provide information to help you deploy Application Management:

Rolling Out the Novell Client

Application Management requires users to have the Novell Client installed on their workstations. The client version must meet the following requirements:

- Windows 95/98: Novell Client for Windows 95/98, version 3.3 with the SP4 patch. The basic version of the client is available from the Novell Software Downloads page (http://www.novell.com/download). The SP4 patch is available from the \CLIENT directory of the *Companion* CD shipping with ZENworks for Desktops.
- Windows NT/2000: Novell Client for Windows NT/2000, version 4.8 with the SP4 patch. The basic version of the client is available from the Novell Software Downloads page (http://www.novell.com/download). The SP4 patch is available from the \CLIENT directory of the *Companion* CD shipping with ZENworks for Desktops.

You can roll out the Novell Client to users before you begin installing Application Management. Both Novell Clients listed above are compatible with ZENworks for Desktops 2.

For information about installing the Novell Client, see the Novell Client documentation at the Novell Documentation Web site (http://www.novell.com/documentation).

Installing Application Management

To extend the schema of an NDS tree to support the Application Management objects and properties or to install the Application Management software to one or more servers, complete the tasks in the following sections:

Completing the Installation Prerequisites

Before you can install Application Management, you must perform the following tasks:

- Make sure that all of the recommended hardware and software requirements are met. For details, see Overall Hardware Requirements and Overall Software Requirements in Installation and Setup in *ZENworks for Desktops Getting Started*.
- Make sure that you have Admin equivalent rights to the servers where you will install Application Management.
- Make sure that you have Admin equivalent rights to extend the NDS schema.
- Make sure that the workstation where you will run the installation program is authenticated to the servers where you are installing the software.

- If you will be installing on a NetWare server, it will be necessary to unload JAVA.NLM (at the Server Console, type **`java -exit`**). Make sure you do this when Java* is not being used by another process and the proper Java components have already been installed.
- Exit any program that uses files in the SYS:PUBLIC directory on the server where you will be installing Application Management.
- Exit any Windows programs on the network workstation where you will be running the installation program.

Running the Installation Program

To install Application Management:

1. Select a network workstation where you can later run ConsoleOne to administer Application Management. This is the workstation where you will run the installation program.

   IMPORTANT: Make sure that this workstation and all other administrative workstations are not running ConsoleOne while the installation program is running.

2. At the workstation, insert the ZENworks for Desktops *Program* CD.

   The WINSETUP.EXE program will autorun. If it does not autorun, run it from the root of the CD.

3. Click English > Install ZENworks to launch the NIS setup program.
4. Follow the prompts until you reach the ZENworks Install Types dialog box.
5. In the ZENworks Install Types dialog box, select Custom > click Next.
6. In the Components dialog box, deselect all components except Application Management > click Next.

   IMPORTANT: If you want to install the Sybase database to enable storing of Application Management events in the database, select Sybase in addition to Application Management. For more information about Sybase and Application Management reporting, see "Sending Events to a Database" on page 98.

7. In the ZENworks Part Selection dialog box, select the parts (Files, Schema Extensions, and NDS Objects) you want to install > click Next.

   IMPORTANT: If you have not previously installed ZfD 3 Application Management, you should select all three parts. If you have already installed to the tree and are simply installing the software files to another server in the tree, select the Files option only.

8. In the ZENworks List of Trees dialog box, select the NDS tree where you want to install Application Management > click Next.
9. In the ZENworks List of Servers dialog box, select the servers where you want to install Application Management > click Next.

   For information about where you should install Application Management, see "Selecting NDS Trees and Network Servers" on page 91.

10. If you are installing the Sybase database, the Database Server Selection dialog box is displayed. Click the name of the server where you want to install the database > click Next > select the server volume > click Next.
11. In the Languages dialog box, select the language to install > click Next.
12. If you are installing the Sybase database, the Site ID for Database dialog box is displayed. Enter a site ID (a number between 0 and 255) and site name (cannot include underscore (_) characters) > click Next.

13 In the Summary dialog box, review the products to be installed > click Finish > follow the prompts to complete the installation.

Starting Application Launcher and Application Explorer

Once you've installed Application Management, you can start Application Launcher or Application Explorer on users' workstations. The following sections explain the rights required by Windows NT/2000 users, how to manually start the applications, and how to automate the starting of the applications:

- "Rights for Windows NT/2000 Users" on page 101
- "Manually Starting Application Launcher or Application Explorer" on page 101
- "Automating Application Launcher or Application Explorer Startup" on page 101

Rights for Windows NT/2000 Users

Application Launcher/Explorer needs to be able to copy files to the workstation, write to the Windows registry, and so forth.

On Windows NT, users need to be members of the Users group to receive all the required rights

On Windows 2000, users need to be members of the Power Users group.

Manually Starting Application Launcher or Application Explorer

You can run either Application Launcher or Application Explorer on a workstation. Do not run both on the same workstation.

To manually start Application Launcher or Application Explorer on a workstation:

1 Make sure that the Novell Client for Windows 95/98 (version 3.3 with SP4 or later) or the Novell Client for Windows NT/2000 (version 4.8 with SP4 or later) is installed on the workstation. For information, see "Rolling Out the Novell Client" on page 99.

2 To start Application Launcher, run NAL.EXE from the SYS:\PUBLIC directory on a server where you installed Application Management.

NAL.EXE copies Application Launcher files to the workstation and starts Application Launcher. For details about Application Launcher files, see Setting Up Application Launcher/Explorer in *ZENworks for Desktops 3.2 Administration Guide*.

3 To start Application Explorer, Run NALEXPLD.EXE from the SYS:\PUBLIC directory on a server where you installed Application Management.

NALEXPLD.EXE copies Application Explorer files to the workstation and starts Application Explorer. For details about Application Explorer files, see Setting Up Application Launcher/Explorer in *ZENworks for Desktops 3.2 Administration Guide*.

Automating Application Launcher or Application Explorer Startup

You can run either Application Launcher or Application Explorer on a workstation. Do not run both on the same workstation.

To automatically start Application Launcher each time a user logs in to NDS:

1. Make sure that the Novell Client for Windows 95/98 (version 3.3 with SP4 or later) or the Novell Client for Windows NT/2000 (version 4.8 with SP4 or later) is installed on the workstation. For information, see "Rolling Out the Novell Client" on page 99.
2. To use Application Launcher, enter the following line in the user's login script:

   @*servername*\sys\public\nal.exe

   where *servername* is the actual name of your network server.

   You can enter this line in a container, profile, or user login script. If the login script also contains an entry for the Automatic Client Upgrade (ACU), make sure the NAL.EXE entry is listed before the ACU entry.
3. To use Application Explorer, enter the following line in the user's login script:

   @*servername*\sys\public\nalexpld.exe

   where *servername* is the actual name of your network server.

   You can enter this line in a container, profile, or user login script. If the login script also contains an entry for the Automatic Client Upgrade (ACU), make sure the NALEXPLD.EXE entry is listed before the ACU entry.

You can also add Application Launcher or Application Explorer to the Windows Startup folder. This enables Application Launcher/Explorer to start when the workstation is disconnected from NDS. You configure this option in ConsoleOne and can have it apply to a single user, a group of users, or all users in a container. To do so, right-click a User, Group, or container object > click Properties > click the Application Launcher tab. On the Application Launcher page, click Edit > click the User tab > scroll to select the Auto-Start NAL When Disconnected option > set the option to Yes.

Setting Up Software Metering

You can set up software metering as part of Application Management deployment or you can implement it at a later time. If you want to set up software metering at this time, complete the following tasks:

- Install Novell Licensing Services (NLS). NLS is included with NetWare 4.*x*, 5.*x*, and 6, and with Novell Cluster Services. For more information about NLS, see the Novell Documentation Web site (http://www.novell.com/documentation).
- Create a separate License container and one or more Metered Certificates for each application you want to track. For instructions, see the NLS documentation at the Novell Documentation Web site (http://www.novell.com/documentation).
- Configure the Application object in NDS to use NLS and software metering. You won't be able to complete this step until after you've created an Application object for the application. For details about creating an Application object, see Distributing Applications in *ZENworks for Desktops 3.2 Administration Guide*. For details about configuring the Application object to use software metering, see Metering Software Licenses in *ZENworks for Desktops 3.2 Administration Guide*.

Setting Up Event Reporting

As with software metering, you can set up event reporting as part of Application Management deployment or you can implement it at a later time.

See the following sections for information about setting up the type of event reporting you want:

Setting Up Database Reporting

To set up database reporting, you need to complete the following tasks:

Creating a ZENworks Database Object

If you are using the Sybase database that comes with ZfD and have already installed it, the installation program creates the database object in NDS. You can skip to the next section, "Configuring the Database's JDBC and ODBC Information" on page 103.

If you are using another database, such as the Oracle* database that comes with NetWare 5.1, you will need to create a ZENworks Database object in NDS to represent the database.

To create a ZENworks Database object:

1. Right-click the container in which you want to create the object > click New > click Object to display the New Object dialog box.
2. Select ZENworks Database > click OK to display the New ZENworks Database dialog box.
3. In the Name box, type a name for the database, such as ZfDAppManReports.
4. Select the Define Additional Properties box > click OK.
5. In the Server DN field, browse for and select the Server object for the server where the database is physically installed and running.
6. If you want to set up Read-Write, Read-Only, or Write-Only users, enter information in the appropriate username and password fields.
7. Click OK to save the information.

Configuring the Database's JDBC and ODBC Information

ConsoleOne uses a JDBC driver to pull information from the database for a set of predefined Application Management reports. If you want to use these predefined reports, you need to configure the ZENworks Database object with the correct JDBC driver information.

Application Launcher/Explorer uses an ODBC driver to write event information to the database. You need to configure the ZENworks Database object with the ODBC driver information that Application Launcher/Explorer will need.

To provide the JDBC and ODBC information:

1. Right-click the ZENworks Database object > click Properties.

2. Click the JDBC Driver Information tab.
3. If you are using a Sybase or Oracle database, click the appropriate Populate option > click Populate Now to automatically populate the fields with the default information for a Sybase or Oracle database.

   or

   If you are using a different type of database, fill in the fields with the appropriate information for your database. Click the Help button for a description of each field.
4. Click the ODBC Driver Information tab. Fill in the following fields:

   Driver File Name: Enter the name of the ODBC driver file that resides on the workstation to enable Application Launcher/Explorer to access the database. For Sybase, the driver file name is DBODBC6.DLL.

   Data Source Name: Enter **`NAL Reporting`**.

   Connection Parameters: Enter the appropriate commands to connect to the database. For Sybase, these commands are:

   ```
   CommLinks=TCPIP{Host=IPAddress:2638};AutoStop=Yes;Integrated=No;DBN=NAL;
   ENG=IPAddress
   ```

   where *IPAddress* is the actual IP address of the server where the database resides.
5. Click OK to save the JDBC and ODBC driver information.

Granting ODBC Property Rights to Users

You need to grant users Read and Compare rights to the ODBC properties you defined for the ZENworks Database object in the previous section. This allows Application Launcher/Explorer to retrieve the ODBC information it needs to access the database.

To grant rights:

1. Right-click the ZENworks Database object > click Trustees of This Object.
2. Click Add Trustee.
3. Select [PUBLIC] > click OK to add [PUBLIC] to the list of trustees.

   Adding [PUBLIC] as a trustee gives every user Read and Compare rights to all of the database object's properties, including the various usernames and passwords that can be used to access the database. To avoid this, you need to limit the [PUBLIC] access to the three ODBC properties.
4. In the Property list, select [All Attribute Rights] > click Delete Property to remove it from the list.
5. Click Add Property to display the Add Property dialog box > select zendbODBCConnectionParameters > click OK to add it to the Property list.

   The default rights, Read and Compare, are sufficient. You do not need to change these rights.
6. Repeat Step 5 to add the following two properties: zendbODBCDataSourceName and zendbODBCDriverFileName. Keep the default rights (Read and Compare).
7. Click OK > OK to save the changes.

Enabling the ZENworks Database Policy

Before Application Management can use the database, you need to:

- Activate a Database policy in an NDS Service Location Package. The Database policy simply points to the location of the ZENworks database you are using. If you haven't created a Service Location Package, instructions are provided in the steps below.
- Associate the Service Location Package with the containers where Application objects reside. This association is how Application Launcher/Explorer knows which database to use when reporting events for the applications.

To enable the ZENworks Database policy:

1. In ConsoleOne, right-click the Service Location Package you want to use > click Properties.

   or

   If you do not have a Service Location Package, right-click the container where you want to create one > click New > click Policy Package. Follow the instructions provided in the Policy Package Wizard to create a Service Location Package.
2. On the General page, check the box in the Enabled column to enable the ZENworks Database policy.
3. Select the ZENworks Database policy in the list > click Properties.
4. Click the Application Management tab.
5. In the Database DN field, browse for and select the ZENworks Database object you want to use for Application Management reporting. This should be the same object you configured in "Configuring the Database's JDBC and ODBC Information" on page 103.
6. Click OK to return to the General page.
7. Click Associations to display the Associations page.

   You use this page to associate the Service Location Package with the containers where Application objects reside. If you have Application objects in multiple containers, make sure to add all containers to the list (unless you don't want events reported for applications in those containers, or want to use another database for those applications' events). If a parent container includes several containers where Application objects reside, you can select the parent container rather than each individual container.
8. Click Add > browse for and select the container you want to add > click OK to add it to the list.
9. Repeat Step 8 to add additional containers.
10. When you've finished adding containers, click OK to save the information.

Configuring Application Objects to Use Database Reporting

Event reporting is configured on a per-application basis. You can choose which objects you want to collect event reports for and which ones you don't.

You use an Application object's Reporting page (Common tab) to configure which events are reported and to instruct Application Launcher/Explorer to save them to the database. For detailed instructions, see Reporting on Application Management Events in *ZENworks for Desktops 3.2 Administration Guide*.

Generating the Predefined Reports

Application Management includes a set of predefined reports for you to use. There are six basic reports that let you report on the success or failure of an event either by application, by user, or by workstation. For example, you could use the Failure by App report to view a list of all application

distributions, sorted by user, that failed. Or you could use the Failure by User to view a list of all application launches, sorted by user, that failed.

IMPORTANT: Before you can generate an Application Management report from the ZENworks database, the database needs to include at least one Application Management event. To generate an event, configure an Application object to use database reporting (see "Configuring Application Objects to Use Database Reporting" on page 105) and then perform a task with the application (distribute, uninstall, cache, or so forth) that will create an event report.

To access the predefined reports:

1. Right-click the ZENworks Database object > click Reporting.
2. In the Available Reports list, expand the ZENworks NAL Reports category > select the report you want.
3. In the Event Type list, select the event you want to include in the report.
4. Click Run Selected Report.

Setting Up SNMP Trap Reporting

To set up SNMP trap reporting, you need to complete the following tasks:

- "Enabling the SNMP Trap Targets Policy" on page 106
- "Configuring Application Objects to Use SNMP Trap Reporting" on page 107

Enabling the SNMP Trap Targets Policy

Before Application Management can use SNMP traps for event reporting, you need to:

- Activate an SNMP Trap Targets policy in an NDS Service Location Package. The SNMP Trap Targets policy simply points to the IP address (or addresses) of the management console that will display the traps. A Service Location Package can have one SNMP Trap Targets policy only. If you haven't created a Service Location Package, or if your current packages' SNMP Trap Targets policies are being used for other databases, you will need to create a new Service Location Package. Instructions are provided in the steps below.
- Associate the Service Location Package with the containers where Application objects reside. This association is how Application Launcher/Explorer knows which database to use when reporting events for the applications.

To do so, complete the following steps:

1. In ConsoleOne, right-click the Service Location Package you want to use > click Properties.

   or

   If you do not have a Service Location Package, right-click the container where you want to create one > click New > click Policy Package. Follow the instructions provided in the Policy Package Wizard to create a Service Location Package.
2. On the General page, check the box in the Enabled column to enable the SNMP Trap Targets policy.
3. Select the policy in the list > click Properties to display the SNMP Trap Targets list.
4. Click Add to display the SNMP Target dialog box > enter the IP address of the workstation or server where the management console is running > click OK to add the IP address to the list.
5. Repeat Step 4 to add additional targets.
6. When you've finished adding targets, click OK to return to the General page.

7 Click Associations to display the Associations page.

You use this page to associate the Service Location Package with the containers where Application objects reside. If you have Application objects in multiple containers, make sure to add all containers to the list (unless you don't want events reported for applications in those containers, or want to use another management console for those applications' events). If a parent container includes several containers where Application objects reside, you can select the parent container rather than each individual container.

8 Click Add > browse for and select the container you want to add > click OK to add it to the list.

9 Repeat Step 8 to add additional containers.

10 When you've finished adding containers, click OK to save the information.

Configuring Application Objects to Use SNMP Trap Reporting

Event reporting is configured on a per-application basis. You can choose which objects you want to collect event reports for and which ones you don't.

You use an Application object's Reporting page (Common tab) to configure which events are reported and to instruct Application Launcher/Explorer to send them as SNMP traps. For detailed instructions, see Reporting on Application Management Events in *ZENworks for Desktops 3.2 Administration Guide*.

Setting Up Log File Reporting

To set up log file reporting, you need to complete the following tasks:

- "Setting Up a Common Log File Location" on page 107
- "Configuring Application Objects to Use Log File Reporting" on page 107

Setting Up a Common Log File Location

With log file reporting, you have two options. You can have Application Launcher/Explorer log events for each individual user to a file on the user's local driver, or you can have Application Launcher/Explorer log events for all users to a file in a common network location.

If you want Application Launcher/Application Explorer to log events to a file in a common network location, you need to establish the network directory and provide users with Read and Write rights to files in the directory.

Because log file names are established on a per-application basis, you can have individual log files for each application (by specifying a different log file name for each Application object) or one log file for all applications (by specifying the same log file name for all Application objects). You cannot have log files on a per-user basis, unless you have Application Explorer/Launcher save the files to the users' local drives.

Configuring Application Objects to Use Log File Reporting

Event reporting is configured on a per-application basis. You can choose which applications you want to collect event reports for and which ones you don't.

You use an Application object's Reporting page (Common tab) to configure which events are reported and to instruct Application Launcher/Explorer to log them to a text file. For detailed instructions, see Reporting on Application Management Events in *ZENworks for Desktops 3.2 Administration Guide*.

As you configure the location for the log file that will be used for an application's events (using the Application object's Reporting page), make sure you enter a network location for the log file if you want events for all users logged to the same file, and that all users have Read and Write rights to the network location. If you want each user to have an individual log file for the application, enter a path on the users' local drives (for example, C:\TEMP).

5 Workstation Imaging

The following sections provide information on deploying ZENworks® for Desktops (ZfD) Workstation Imaging services in a production environment. We assume that you have tested and are familiar with the basic workstation imaging operations covered in *ZENworks for Desktops Getting Started*.

The following sections contain detailed information to help you deploy Workstation Imaging:

Imaging Deployment Strategies

The table below indicates possible approaches to deploying ZfD imaging services for a few common enterprise scenarios. Use it to determine which procedures (documented in subsequent sections) to perform and in what order.

Scenario	Description	Possible Approach
New workstations	As new computers are purchased, before deploying them you install a standard software platform and enable the computer for future unattended reimaging.	1. Create a model workstation of each type that you'll deploy, and create an image of each on a ZfD imaging server. These images should include the Novell® Client™ and imaging agent. 2. Create imaging diskettes or CDs that point to the ZfD imaging server where the model images are stored (not required if you are using PXE). 3. Create a policy for unregistered workstations that specifies which image to put on a new machine, depending on its hardware. As each new computer comes in, do the following: 1. If you are using PXE, check to see if the workstation is PXE capable. Enable PXE if it isn't enabled by default. Make sure Preboot Services (PXE Support) has been installed on your imaging server. 2. Physically connect the workstation to the network. If using PXE, boot it from the PXE server. If not using PXE, boot it with the imaging diskettes or CD and install the imaging partition. 3. Reboot from the imaging partition (not required if you are using PXE). 4. Let the computer be auto-imaged by the policy. 5. After deploying the machine, have the user register it as a Workstation object in NDS®.

Scenario	Description	Possible Approach
Existing workstations	With minimal disruption to users, you enable existing workstations for possible future reimaging.	This might need to be phased in by local administrators. Each administrator could: 1. Upgrade each workstation to the latest Novell Client, using Automatic Client Update. 2. Install the ZfD imaging agent on each workstation by distributing an Application object. 3. Register each workstation as a Workstation object in NDS. 4. If the workstations are PXE capable, make sure PXE is enabled and make sure Preboot Services (PXE Support) has been installed on your imaging server. Or, prepare a few sets of imaging boot diskettes or CDs that users can use when they run into trouble. These devices could point to an imaging server that contains the same clean images used for new computers. 5. If a user runs into trouble, use the following strategy for corrupted workstations:
Corrupted workstations	Without data loss or undue disruption to users, you fix workstations that have become misconfigured or corrupted.	1. Create a policy for registered workstations. Use the same image-selection logic as the policy for new (unregistered) workstations. 2. When a computer needs to be fixed, have the user back up (to the network) any files that he or she wants to keep. 3. Flag the Workstation object in NDS to receive an image the next time it boots. 4. Have the user reboot. If it's an older workstation (without a ZfD partition), the user should boot with the imaging diskettes or CD. If it's a newer workstation (with a ZfD partition or PXE-enabled), the user should boot from the ZfD partition or PXE server. (If you are using PXE, make sure Preboot Services (PXE Support) has been installed on your imaging server.) 5. Restore any user files that were backed up in Step 2.
Lab or classroom	After each lab session, you restore every workstation to a clean state, removing any changes or additions made during the session.	1. Create an image of a clean model workstation and store it on a ZfD imaging server. The image should include the Novell Client and imaging agent. 2. Create imaging diskettes or CDs that point to the ZfD imaging server where the clean image is stored. If the workstations are PXE capable, make sure PXE is enabled and make sure Preboot Services (PXE Support) has been installed on your imaging server. 3. Create a policy for unregistered workstations that specifies the clean image to restore. Choose the option to always force down the same base image. Deploy each lab computer as follows: 1. Physically connect the workstation to the lab network. If using PXE, boot it from the PXE server. If not using PXE, boot it with the imaging diskettes or CD and install the imaging partition. 2. Reboot from the imaging partition (not required if you are using PXE). 3. Let the computer be auto-imaged by the policy. 4. At the end of each lab session, reboot each computer and let it be auto-imaged by the policy.

Setting Up Workstations for Imaging

The following sections cover procedures to prepare workstations for imaging. The procedures that are applicable to you depend on your imaging deployment strategy. (See "Imaging Deployment Strategies" on page 109.)

- "Preparing an Imaging Boot Device or Method" on page 111
- "Installing the Imaging Agent to Safeguard Workstation Identity Data" on page 116
- "Registering Workstations for Auto-Imaging" on page 117

Preparing an Imaging Boot Device or Method

Because the ZfD imaging engine is a Linux* application, in order to image a computer you must boot it to Linux temporarily while the imaging engine runs. The bootable device or method you use can be any of the following:

- Preboot Services (PXE)

  PXE (Preboot Execution Environment) is an industry-standard protocol that allows a workstation to boot up and execute a program from the network before the workstation operating system starts. PXE uses DHCP and TFTP protocols. The PXE environment is loaded from either the NIC (Network Interface Card) in flash or ROM, or in the same memory as the system BIOS.

  Before you can use PXE, you need to install the ZfD 3.2 Imaging and Preboot Services (PXE Support) components on your imaging server and enable PXE on the workstation. A standard DHCP server must already be installed—either on the same server where you are installing ZfD Preboot Services or on another server in the network—before you install the ZfD Preboot Services Proxy DHCP server. If the standard DHCP server is on the same server where you are installing the Proxy DHCP, you must set option tag 60 in DHCP services. For more information, see the ZfD 3.2 Preboot Services *Administration* guide at the ZfD 3.2 Preboot Services documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html). See Workstation Imaging in *Getting Started* for PXE system requirements.

  When a PXE-enabled workstation is booted, it looks for the server where PXE is installed. Using a DHCP request, it checks the server to see if there is any imaging work to do. If there is imaging work to do, it downloads the Linux imaging environment from the server so that the workstation can be booted to Linux. Then the image is downloaded to the workstation. If there is no imaging work to do, these three files are not downloaded and the workstation proceeds to boot to its operating system.

  Finding Out If a Workstation Is PXE Capable: To image a workstation using PXE, you need to find out if the workstation is PXE capable, and then make sure that PXE is enabled. (When PXE is enabled, it can lengthen the time of the boot process slightly, so most NICs have PXE turned off by default.) To do so, enter the computer system BIOS and look at the boot up options. These typically include Floppy Disk, Hard Disk, and CD-ROM. If PXE is not listed and the NIC is embedded in the motherboard, refer to the integrated devices section of the BIOS. In the integrated devices section, you may have an option to activate PXE. It may be called by another name, such as MBA (Managed Boot Agent) or Pre-Boot Service. Once you have activated it, it will become available in the Boot section of the BIOS. If the computer system does not have an integrated NIC, you may need to use NIC management software to configure your NIC to support PXE. Refer to your NIC documentation for support of PXE.

  If a Workstation Is Not PXE Capable: If the workstation is not PXE capable, you may be able to make it capable by updating your BIOS version or NIC driver, using a PXE boot disk,

or purchasing a PXE capable NIC and installing it in your computer. To create a PXE boot disk, use the PXE-On-Disk utility that is installed as part of Preboot Services (PXE Support) in ZfD 3.2. You can access the utility with the Create PXE Disk button in Imaging Boot Disk Creator. (To start this utility from ConsoleOne®, click Tools > ZENworks Utilities > Imaging > Create or Modify Boot Diskette.)

Refer to the *PXE-on-Disk User Guide* for information about creating a PXE boot disk. To access this guide, on a Windows* machine that has ZfD 3.2 PXE components installed on it, click the Start button > Programs > ZEN Preboot Services > PXE on Disk > PXE on Disk Manual. You can also find this guide at the ZfD 3.2 Preboot Services product documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html).

If You Have Previously Installed a ZfD (Linux) Imaging Partition: If you are using a PXE-enabled workstation but have previously installed a Linux imaging partition on the workstation, you can disable or delete the partition. You can disable (and enable) the imaging partition when you boot to Linux using any imaging boot device or method. You can delete the partition only when you are putting an image on the workstation using standard imaging, and only when you boot the workstation from an imaging boot device or method other than the Linux imaging partition.

IMPORTANT: After you have deleted the partition, you need to make sure that the image you put on the workstation was made on a computer without a Linux imaging partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the computer will fail to boot. In addition, if you remove the Linux imaging partition from a Windows NT or Windows 2000 machine, Windows will no longer be able to boot. You should only remove the Linux imaging partition if you are going to restore an image to the workstation.

Refer to the ZfD 3.2 Preboot Services *Installation* guide for information about installing and configuring PXE. To access this guide, start the ZfD 3.2 installation > click English > click Preboot Services Installation Guide. You can also find this guide at the ZfD 3.2 Preboot Services documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html).

Detailed product documentation about configuring PXE is included in the ZfD 3.2 Preboot Services *Administration* guide, which is available at the ZfD 3.2 Preboot Services documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html).

- Diskettes

  If you are unable to use PXE, diskettes are an easy device to prepare. Three diskettes are required, four if you need to image computers that have non-English keyboards. The basic steps to create the diskettes are given in Creating Imaging Boot Diskettes in Preparing for Basic Imaging Operations in *Getting Started*.

  Once you have created the diskettes, you can customize them for the particular imaging tasks for which you will use them, such as one set of diskettes for connecting to a server that holds Windows 95 images, another set for connecting to a server that holds Windows NT* images, and another set for installing ZfD imaging partitions. To customize the diskettes, edit the SETTINGS.TXT file on the third diskette as explained in Imaging Utilities and Options in Workstation Imaging in *Administration*.

- CD

  If you have CD-burning software, you can create a bootable CD for performing imaging operations. This is a bit harder than preparing diskettes, but you have more room to store any custom files that you might want to add, such as images and Linux device drivers. See "Preparing a Bootable CD" on page 113 for instructions.

- Hard-disk partition

If you want to set up a computer for unattended imaging operations and are unable to use PXE, you must create a small ZfD imaging (Linux) partition on the hard disk. If you make the partition big enough, you can even store an image of the computer's hard disk, which can be useful if (for example) the computer becomes hopelessly misconfigured or corrupted.

To create a ZfD imaging partition, you must first create imaging diskettes and boot the computer from them. Then, proceed with Step 4 of Enabling a Workstation for Unattended Imaging Operations in Testing Basic Imaging Operations in *Getting Started*.

The following sections contain additional information:

- "Preparing a Bootable CD" on page 113
- "Adding Linux Device Drivers" on page 113
- "Booting with a Non-English Keyboard" on page 115

Preparing a Bootable CD

If you have CD-burning software, you can use the BOOTCD.ISO image available on the ZfD imaging server to create a ZfD imaging boot CD.

To create a bootable CD:

1. In a temporary working area, create a SETTINGS.TXT file containing the settings you want for the imaging bootup process. For instructions, see Imaging Utilities and Options in Workstation Imaging in *Administration*.
2. Use the Add Linux Drivers button in the Imaging Boot Disk Creator (ZIMGBOOT.EXE) to copy the Linux drivers to a diskette. Copy the A:\DRIVERS directory from the diskette to the temporary working area mentioned above.

   For more information about adding Linux drivers, see the online help for the Imaging Boot Disk Creator or see Using ZIMGBOOT.EXE to Add Linux Drivers in Imaging Boot Disk Creator (ZIMGBOOT.EXE) in Imaging Utilities and Options in *Administration*.
3. In the temporary working area, add any ZfD image files you want to store on the CD.
4. Use your CD-burning software to burn the BOOTCD.ISO image onto the CD. This image is located in the ZENWORKS\IMAGING folder in your ZfD installation (on the imaging server).
5. Use your CD-burning software to add the contents of your temporary working area to the root of the CD, including the SETTINGS.TXT file, any Linux network drivers, and any ZfD image files.

   NOTE: Adding these files makes the CD a multisession CD. To boot a workstation from such a CD, the CD drive must support multisession CDs. For example, in our testing, we successfully booted an HP* vectra VL, a Compaq* Prosignia, and a Dell* Optiplex, but some other workstations failed, including an IBM* PC 300PL, a Dell Dimension XPS T450, and an IBM clone with an Intel* motherboard.
6. Use your CD-burning software to finalize the CD.

For information on how to use the CD to perform disconnected imaging operations, see "Setting Up Disconnected Imaging Operations" on page 120.

Adding Linux Device Drivers

If you need to, you can add Linux device drivers to your boot device or method.

- "Obtaining Linux Drivers" on page 114

- "Adding Linux Drivers to Your Boot Device or Method" on page 114

Obtaining Linux Drivers

To obtain a Linux driver for your particular hardware, you should visit the Web site of the hardware vendor and check for a download site.

There are also some other Web sites where you can obtain drivers:

- Network drivers can be downloaded from the Scyld Computing Corporation* (http://www.scyld.com). Click Network Drivers.
- PCMCIA drivers can be downloaded from the Linux PCMCIA Information Page (http://pcmcia-cs.sourceforge.net).

You can also get additional Linux drivers at the Novell® ZENworks Cool Solutions Web Community (http://www.novell.com/coolsolutions/zenworks/features/a_linux_drivers_zw.html).

To learn more about drivers, including the loading parameters you need to specify, see the Linux Documentation Project (http://www.linuxdoc.org) and visit the following HOWTO (http://www.linuxdoc.org/HOWTO/HOWTO-INDEX/howtos.html) sites:

- Hardware
- PCMCIA
- SCSI
- Ethernet

Adding Linux Drivers to Your Boot Device or Method

Diskettes

For instructions, see Using ZIMGBOOT.EXE to Add Linux Drivers in Imaging Boot Disk Creator (ZIMGBOOT.EXE) in Imaging Utilities and Options in *Administration*.

CD

For instructions, see "Preparing a Bootable CD" on page 113.

Hard-Disk Partition

It is unlikely that you will need to add Linux drivers if you are using a ZfD imaging partition. If you want to update the Linux drivers, however, follow this procedure:

1. Boot the workstation using imaging boot diskettes, an imaging boot CD, or if it is PXE-enabled, boot it from the PXE server.
2. Enter **`manual`** at the boot prompt or select to start in Maintenance Mode from the PXE menu.
3. Enter the following to mount the hard drive:

   ```
   mount /dev/hda1 /mnt/harddisk
   ```

4. Enter the following to mount the diskette that contains the driver files:

   ```
   mount /dev/fd0 /mnt/floppy
   ```

5. Enter the following to copy the files to the appropriate directory on the ZfD imaging partition:

   ```
   cp /mnt/floppy/*.o /mnt/harddisk/lib/modules/2.4.3/drivers/net
   ```

6. Type **`reboot`** > press Enter.

Preboot Services (PXE)

To add Linux drivers for use with PXE, you must have a working Linux workstation capable of mounting a loop device. Red Hat* 7 has this ability compiled in the distribution kernel.

1. On the TFTP server on your PXE server, locate the linux.2 file in \PUBLIC\ZENWORKS\IMAGING\TFTP. Make a backup copy of this file.
2. On the Linux workstation, create a working directory for linux.2.
3. Using a transfer method such as FTP, transfer linux.2 to the directory created in Step 2.
4. Enter the following to rename linux.2 to linux.gz:

   ```
   mv linux.2 linux.gz
   ```

5. Enter the following to extract linux.gz:

   ```
   gzip -d linux.gz
   ```

   This will replace the linux.gz file with a file named linux. This file is a MINIX file system that can be mounted and changed.

6. Enter the following to create a mount point:

   ```
   mkdir /mnt/loop
   ```

7. Enter the following to mount the file system:

   ```
   mount -o loop linux /mnt/loop
   ```

8. Copy the driver files to the appropriate directory in the /mnt/loop directory structure.
9. Enter the following to unmount the updated file system:

   ```
   umount /mnt/loop
   ```

10. Enter the following to zip the file:

    ```
    gzip --v9c linux
    ```

11. Enter the following to rename the file:

    ```
    mv linux.gz linux.2
    ```

12. Using a transfer method such as FTP, transfer linux.2 to the TFTP server.

Booting with a Non-English Keyboard

If you will image computers that have non-English keyboards, the imaging boot device or method must include additional support for that language, in the form of a language diskette. (When booting a computer from the imaging device or method, you will be prompted for this diskette.) For information on preparing this diskette, see the online help in the Imaging Boot Disk Creator (ZIMGBOOT.EXE) utility.

If the Language/Country drop-down list in the Imaging Boot Disk Creator utility doesn't have the keyboard language you need, you can close the utility and reconfigure it to support the additional language. This assumes you can find Linux keyboard support files somewhere on the Web.

Adding Support for Another Keyboard Language

1. Get the Linux .GZ files that contain the keyboard mappings, fonts, and Unicode* mappings for the language that you want to add.

2 From the folder containing the ZIMGBOOT.EXE file, browse to the BOOTDISK folder > copy the .GZ files for the new language to the following subfolders:

- The keyboard map file goes in the KEYMAPS folder.
- The font file goes in the CONSOLEFONTS folder.
- The Unicode map file goes in the CONSOLETRANS folder.

3 Add a section to the ZIMGLANG.INI file using the format illustrated for German in Imaging Bootup Languages (ZIMGLANG.INI) in Imaging Utilities and Options in Workstation Imaging in *Administration*.

3a For the bracketed section heading, specify the language or country name that you want shown in the Imaging Boot Disk Creator utility.

3b On the KEYMAP, FONT, and ACM parameters, specify the names and locations (relative to the BOOTDISK folder) of the keyboard map, font, and Unicode map files, respectively.

4 Save your changes to the ZIMGLANG.INI file.

5 Restart the Imaging Boot Disk Creator utility and verify that the new language appears in the Language/Country drop-down list.

Installing the Imaging Agent to Safeguard Workstation Identity Data

When you lay down a new base image on a Windows workstation, the workstation receives the same identification data as the computer from which the image was taken, including such settings as the IP address and computer (NETBIOS) name. To work around this, you can install the ZfD Imaging Agent (ZISWIN.EXE) on the target workstation before reimaging it. This saves the workstation's current identity settings to an area on the hard disk that's safe from reimaging. When the workstation reboots after being reimaged, the agent restores the original settings.

IMPORTANT: The imaging agent does not save or restore any Windows NT/2000 Domain information. If you change a workstation's domain and then restore an image, the workstation will receive whatever domain is embedded in the new image.

The table below lists the different ways you can install the imaging agent, along with the location of the installation instructions.

Installation Method	See
Do a custom Novell Client installation and choose the Imaging Services option	Overall Software Requirements in Hardware and Software Requirements in Installation and Setup in *Getting Started*
Run the ZISD-9x or ZISD-NT application object on the workstation	Distributing an Application in Application Management in *Getting Started*
Manually install the imaging agent	Step 3 in Enabling a Workstation for Unattended Imaging Operations in Testing Basic Imaging Operations in Workstation Imaging in *Getting Started*

Registering Workstations for Auto-Imaging

When you boot a Windows workstation from an imaging device or method and allow the bootup process to proceed in auto-imaging mode, the imaging engine runs on the workstation and contacts a ZfD imaging server. In order for the workstation to actually be imaged in this mode, you must either define an NDS policy for the ZfD imaging server, or you must do the following *before* booting the workstation from the imaging device or method:

1. Register the workstation as a Workstation object in the NDS tree that contains the ZfD imaging server.

   For instructions on how to do this, see Automatic Workstation Import in *Getting Started*.

2. Set a flag in the Workstation object that triggers the imaging operation you want.

   For instructions on how to do this, see Triggering an Unattended Imaging Operation in Testing Basic Imaging Operations in Workstation Imaging in *Getting Started*.

Setting Up Imaging Services

The following sections cover procedures to configure ZfD imaging services. The procedures that are applicable to you depend on your imaging deployment strategy. (See "Imaging Deployment Strategies" on page 109.)

Defining an Imaging Policy for Unregistered Workstations

If a Windows workstation hasn't been registered as a Workstation object in NDS and you boot that workstation from an imaging device or method in auto-imaging mode, the imaging server is contacted and checks its Imaging Server Policy in NDS to determine which image to lay down on the workstation. If the base image specified by the policy is the same as the base image currently on the workstation (as reported by the imaging engine), the imaging server doesn't send any new images to lay down on the workstation, unless a flag is set in the policy to force down the base image again. If such a flag is set, or if the base image currently on the workstation is different than the base image specified by the policy, the imaging server sends down the new base image and any add-on images specified by the policy, and the imaging engine lays these images down on the workstation.

In addition, if the imaging engine reports to the imaging server that data is missing from the workstation's image-safe area, the imaging server obtains the missing data from the Imaging Server Policy and sends it to the imaging engine, which then saves the data to the image-safe area.

To define the Imaging Server Policy for one or more imaging servers:

1. Prepare the various workstation images that the policy can prescribe. For details, see Preparing Images in Workstation Imaging in *Administration*.
2. If a Server Package hasn't already been created to hold the policies for the target imaging servers, create one as instructed in Creating the Policy Packages in Installation and Setup in *Getting Started*.
3. Right-click the Server Package > click Properties.

4. Enable the Imaging Server policy > click Properties.
5. Follow this step if you are using PXE:

   If you are using PXE but previously booted workstations from a ZENworks imaging (Linux) partition, you can select to disable the imaging partition on the General Imaging Partition property page. The partition is not removed with this option.

   Use the General PXE Settings property page to specify the availability of the PXE menu, which displays when you boot a PXE-enabled workstation. The default PXE menu includes the ability to Start ZENworks Imaging in Automatic Mode, Start ZENworks Imaging in Maintenance Mode, Disable the ZEN Partition, and Enable the ZEN Partition.

   You can also specify a different PXE menu to use. You can create a custom menu using the Menu Editor. On a Windows machine that has Preboot Services (PXE Support) installed on it, click the Start button > Programs > ZEN Preboot Services > ZEN Preboot Services Menu Editor to locate the Menu Editor and the *Menu Editor User Guide*. You can also find this guide at the ZfD 3.2 Preboot Services Product documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html).

   NOTE: Menu Editor is not installed to a NetWare server. If you need to use Menu Editor from a NetWare server, locate the files on the ZfD 3.2 Preboot Services CD in \MENU EDITOR > copy them to your NetWare server. Then, from a Windows machine, you can map a drive to the location on the server and run Menu Editor.

   If you want to specify a different image when using PXE, rather than the default image that is defined, specify the image file and pathname.
6. On the Image Selection tab, click Add > define the conditions under which the target imaging servers should send down a particular image > click OK.

   For details on how to perform this task, click Help in the New Image Selection Rule dialog box.
7. Repeat the previous step as needed to provide rules that will cover all the workstations serviced by the target imaging servers.
8. (Optional) If you want the imaging server to force down the base image determined by this policy even if it's the same as the base image currently on the workstation, select the check box on the bottom of the page.

   WARNING: Use this option with care, because laying down a base image destroys all data that was added to the workstation since the last base image was laid down. In most scenarios, you'll want to use this option only temporarily while a specific workstation is being imaged and not generally for all workstations, unless this policy is designed for a lab environment where you want the workstations to be reimaged every time they reboot. If you select this option as a temporary measure, be sure to deselect it once the specific imaging task is done.
9. On the Image-safe Data tab, fill in the IP Configuration and Windows Networking pages.

   These pages supply image-safe data values that might be missing on the workstations that are serviced by the target imaging servers. For details on these pages, click Help.
10. Click OK to save the policy.
11. On the Associations page, add the containers and/or server objects that represent the target set of imaging servers.
12. Click OK to save the association.

Remember that the policy won't actually be consulted by the associated imaging servers unless the client requesting the imaging operation is an unregistered workstation that has been booted in auto-imaging mode.

Defining General Imaging Server Behavior

Most of the rules that comprise an Imaging Server Policy are in force only when the imaging server is servicing a request to auto-image a workstation. Such rules aren't in force when the imaging server is servicing a manual (command line or menu) imaging request. However, the following two aspects of the Imaging Server Policy are *always* in force, no matter whether the imaging server is servicing an automatic or manual imaging request:

- Whether to allow the creation of new image files that overwrite existing image files on the server
- Whether to confine the creation of new image files on the server to specific areas

To define these general behaviors for one or more imaging servers:

1. If a Server Package hasn't already been created to hold the policies for the target imaging servers, create one as instructed in Creating the Policy Packages in Installation and Setup in *Getting Started*.
2. Right-click the Server Package > click Properties.
3. Enable the Imaging Server policy > click Properties.
4. Fill in the items on the Security tab. For how to do this, click Help.
5. Click OK to save the policy.
6. On the Associations page, add the containers and/or server objects that represent the target set of imaging servers.
7. Click OK to save the association.

Remember that these aspects of the server policy are always in force.

Defining an Imaging Policy for Registered Workstations

If a Windows workstation has been registered as a Workstation object in NDS and you boot that workstation from an imaging device or method in auto-imaging mode, the imaging server is contacted and checks the Workstation object in NDS to see if the administrator has flagged it to receive an image. If this is the case and the administrator hasn't specified which image to use, the imaging server consults the Workstation Imaging Policy associated with the Workstation object to determine which image to send down.

To define the Workstation Imaging Policy for one or more workstations:

1. Prepare the various workstation images that the policy can prescribe. For details, see Preparing Images in Workstation Imaging in *Administration*.
2. If a Workstation Package hasn't already been created to hold the policies for the target workstations, create one as instructed in Creating the Policy Packages in Installation and Setup in *Getting Started*.
3. Right-click the Workstation Package > click Properties.
4. Enable the Workstation Imaging policy > click Properties.
5. Follow this step if you are using PXE:

   If you are using PXE but previously booted workstations from a ZENworks imaging (Linux) partition, you can select to disable the imaging partition on the General Imaging Partition property page. The partition is not removed with this option.

Use the General PXE Settings property page to specify the availability of the PXE menu, which displays when you boot a PXE-enabled workstation. The default PXE menu includes the ability to Start ZENworks Imaging in Automatic Mode, Start ZENworks Imaging in Maintenance Mode, Disable the ZEN Partition, and Enable the ZEN Partition.

You can also specify a different PXE menu to use. You can create a custom menu using the Menu Editor. On a Windows machine that has Preboot Services (PXE Support) installed on it, click the Start button > Programs > ZEN Preboot Services > ZEN Preboot Services Menu Editor to locate the Menu Editor and the *Menu Editor User Guide*. You can also find this guide under Preboot Services at the ZfD 3.2 Preboot Services Product documentation Web site (http://www.novell.com/documentation/lg/zd32pb/index.html).

NOTE: Menu Editor is not installed to a NetWare server. If you need to use Menu Editor from a NetWare server, locate the files on the ZfD 3.2 Preboot Services CD in \MENU EDITOR > copy them to your NetWare server. Then, from a Windows machine, you can map a drive to the location on the server and run Menu Editor.

If you want to specify a different image when using PXE, rather than the default image that is defined, specify the image file and pathname.

6. On the Image Selection tab, click Add > define the conditions under which the imaging server should send down a particular image > click OK.

   For details on how to perform this task, click Help in the New Image Selection Rule dialog box.

7. Repeat the previous step as needed to provide rules that will cover all the target workstations.
8. Click OK to save the policy.
9. On the Associations page, add the container, Workstation Group, or Workstation objects that represent the target set of workstations.
10. Click OK to save the association.

Remember that the policy won't actually be consulted by the imaging server unless you (or another administrator) flags a Workstation object to receive an image on the next boot.

Setting Up Disconnected Imaging Operations

Disconnected imaging operations are inherently manual in the sense that they don't involve the network and thus can't be automated through NDS.

To perform a disconnected imaging operation on a computer, you must have a storage device to hold the image that will be created or laid down, and that storage device must be locally accessible to the imaging engine (in Linux) when you boot the computer from the imaging device. The following sections explain how to set up and perform disconnected operations using different storage devices:

- "Using a CD" on page 120
- "Using a Hard Disk or Jaz Drive" on page 122

Using a CD

Because a CD is read-only, you can only use it as the storage medium for an image that will be laid down, not for an image that will be created. The steps to lay down an image from a CD depend on whether the CD is the bootable imaging CD or some other (non-bootable) CD.

To lay down an image from the imaging boot CD:

1 Use your CD-burning software to put the source image on the imaging boot CD. See "Preparing a Bootable CD" on page 113 for details.

2 Boot the target computer from the CD and type **manual** at the boot prompt.

If the computer fails to boot, see Can't Boot a Workstation from the Imaging CD in Troubleshooting Workstation Imaging in *Troubleshooting*.

3 At the Linux prompt, type **img dump** to view the available partitions. Note the partition number of the imaging CD.

or

Type **img** to display a menu > select Dump > No Geometry.

4 To lay down the image, you have two choices:

- You can use a command of the following format:

  img restorel*pNumber /path/image*.zmg

  where *pNumber* is the partition number of the imaging CD and *path* and *image* are the image path and filename from the root of the CD.

- You can type **img** to display a menu > select Restore an Image > Local Image. Select Local Linux File System (because the image resides on the imaging CD, which is the current local Linux file system). Type the image path and filename. Specify any advanced parameters, such as s*fileset* or a*partition*:p*partition*.

For details on these and other related img command parameters, see Imaging Engine (img: Command Line and Menu) in Imaging Utilities and Options in Workstation Imaging in *Administration*.

5 When the imaging is done, remove the CD and do the following to boot the computer with the new image:

5a At the Linux prompt, type **lilo.s** > press Enter.

5b Press Ctrl+Alt+Delete.

HINT: If the computer doesn't boot to the new operating system (that is, if the Linux prompt reappears), enter the **lilo.s** command again and reboot the computer a second time.

To lay down an image from another (non-bootable) CD:

1 Use your CD-burning software to burn the source image onto a CD.

2 Boot the target computer from a ZfD imaging device and type **manual** at the boot prompt. Insert the second and third diskettes if you are prompted for them.

3 Insert the CD that contains the source image.

4 At the Linux prompt, type **cdrom.s** to mount the CD.

This mounts the CD to /mnt/cdrom.

5 To lay down the image, you have two choices:

- You can use a command of the following format:

  img restorel /mnt/cdrom/*path/image*.zmg

  where *path* and *image* are the path and filename of the image relative to the root of the CD.

- You can type **img** to display a menu > select Restore an Image > Local Image. Select Local Linux File System (because the image resides on the imaging CD, which is the

current local Linux file system). Type the image path and filename. Specify any advanced parameters, such as s*fileset* or a*partition*:p*partition*.

For details on other related command parameters, see Imaging Engine (img: Command Line and Menu) in Imaging Utilities and Options in Workstation Imaging in *Administration*.

6 When the imaging is done, remove the imaging device (if applicable) and do the following to boot the computer with the new image:

6a At the Linux prompt, type **lilo.s** > press Enter.

6b Press Ctrl+Alt+Delete.

HINT: If the computer doesn't boot to the new operating system (that is, if the Linux prompt reappears), enter the **lilo.s** command again and reboot the computer a second time.

Using a Hard Disk or Jaz Drive

When you boot a computer from a ZfD imaging device, you can create an image on, or lay down an image from, any primary FAT16 or FAT32 partition on an IDE or SCSI hard drive or Iomega* Jaz* drive. You can also use the local ZfD imaging (Linux) partition if one is installed. Any target partition must have sufficient space.

When you create an image, the partition where you will store the image is itself excluded from the image. When you lay down an image, the source partition will not itself be altered.

To create an image on a hard disk or Jaz drive:

1 Boot the source computer from a ZfD imaging device and type **manual** at the boot prompt. Insert the second and third diskettes if you are prompted for them.

2 At the Linux prompt, type **img dump** to view the available partitions.

or

Type **img** to display a menu > select Dump > No Geometry.

Note the number of the FAT partition where you'll store the new image.

3 To create the new image, you have two choices:

- You can use a command of the following format:

  img makel[*pNumber*] [comp=*comp_level*] /*path*/*image*.zmg

  where *pNumber* is the number of the partition to store the image in, and *comp_level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed and is used by default if you do not specify this parameter. 6 is the same as Balanced. 9 is the same as Optimize for Space. (Optimize for Speed takes the least amount of time but creates the largest image file. Optimize for Space creates the smallest image file but may take a significant amount of time. Balanced is a compromise between compression time and image file size.) *Path* and *image* are the path and filename of the new image relative to the partition root. If you omit the partition number, the local ZfD imaging (Linux) partition is used.

- You can type **img** to display a menu > select Make an Image > Local Image. Select the partition to store the image in, or Local Linux File System to store the image in the local ZfD imaging (Linux) partition. Type the image path and filename. Select a compression option. (Optimize for Speed takes the least amount of time but creates the largest image file. Optimize for Space creates the smallest image file but may take a significant amount of time. Balanced is a compromise between compression time and image file size.) Specify any advanced parameters, such as x*partition*. If you want, specify additional

information in the Description (a description of the image), Machine Name (the computer on which the image is being stored), Author (the name of the person entering this information), and Comments (any additional comments) fields.

For details on other related img command parameters, see Imaging Engine (img: Command Line and Menu) in Imaging Utilities and Options in Workstation Imaging in *Administration*.

To lay down an image from a hard disk or Jaz drive:

1. Boot the target computer from a ZfD imaging device and type **`manual`** at the boot prompt. Insert the second and third diskettes if you are prompted for them.
2. At the Linux prompt, type **`img dump`** to view the available partitions.

   or

   Type **`img`** to display a menu > select Dump > No Geometry.

   Note the number of the FAT partition where the source image is stored.
3. To lay down the image, you have two choices:
   - You can use a command of the following format:

     `img restorel[`*`pNumber`*`] /`*`path`*`/`*`image`*`.zmg`

     where *pNumber* is the number of the partition where the source image is stored, and *path* and *image* are the image path and filename relative to the partition root. If you omit the partition number, the local ZfD imaging (Linux) partition is used.
   - You can type **`img`** to display a menu > select Restore an Image > Local Image. Select Local Linux File System if the image is stored in the local ZfD imaging (Linux) partition, or select the partition where the image is stored. Type the image path and filename. Specify any advanced parameters, such as s*fileset* or a*partition*:p*partition*.

   For details on other related img command parameters, see Imaging Engine (img: Command Line and Menu) in Imaging Utilities and Options in Workstation Imaging in *Administration*.
4. When the imaging is done, remove the imaging device (if applicable) and do the following to boot the computer with the new image:

   4a At the Linux prompt, type **`lilo.s`** > press Enter.

   4b Press Ctrl+Alt+Delete.

   HINT: If the computer doesn't boot to the new operating system (that is, if the Linux prompt reappears), enter the **`lilo.s`** command again and reboot the computer a second time.

Performing Manual Imaging Operations

If you encounter a situation where the auto-imaging behavior that you have defined in NDS policies and settings won't accomplish the result you need, you can perform a manual (command line) imaging operation as follows:

1. Boot the computer from a ZfD imaging device or method and type **`manual`** at the boot prompt. Insert the second and third diskettes if you are prompted for them.
2. At the Linux prompt, use the **`img`** command to perform the specific imaging operation you want. For more information, see the table below.

For information on	See
All the various **img** command and menu options you can use	Imaging Engine (img: Command Line and Menu) in Imaging Utilities and Options in Workstation Imaging in *Administration*
Performing a disconnected (entirely local) imaging operation	"Setting Up Disconnected Imaging Operations" on page 120
Taking an image of a computer and storing it on a ZfD imaging server	Manually Taking an Image of a Workstation in Testing Basic Imaging Operations in Workstation Imaging in *Getting Started*
Retrieving an image from a ZfD imaging server and laying it down on a computer	Manually Putting an Image on a Workstation in Testing Basic Imaging Operations in Workstation Imaging in *Getting Started*
Taking an image of one computer and multicasting it to several other computers	Multicasting Images in Workstation Imaging in *Administration*

6 Remote Management

ZENworks® for Desktops 3.2 (ZfD 3.2) Remote Management includes features that enable an administrator to manage a remote Windows* 95, Windows 98, Windows NT*, or Windows 2000 workstation.

This document covers the following information:

What's New in Remote Management

Remote Management provides the following new features:

- The performance of Remote Control, especially on a WAN, has been enhanced through using improved compression.

  For details, see Enhancing the Remote Control Performance Over a WAN or a Slow Link in Managing Remote Workstations in *Administration*.

- The performance enhancement drivers minimize the CPU utilization on Windows 95/98/NT/2000 for color settings using more than 256 colors.
- Use the Num Lock and the Caps Lock keys in the MS-DOS environment on a Windows 9x workstation.

Deploying Remote Management

The following sections provide information about deploying ZfD 3.2 Remote Management:

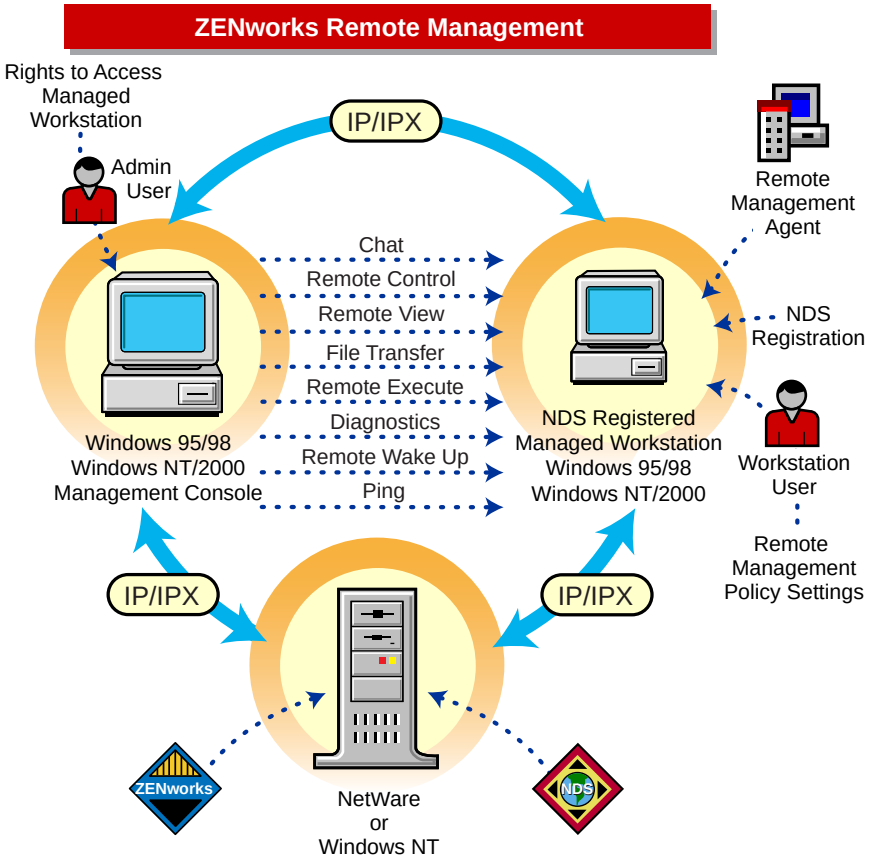
Planning for Installing the Remote Management Component

The Remote Management Agent should be installed on the managed workstation so that the administrator can remotely manage that workstation.

The Remote Management Agent starts automatically when the managed workstation boots up. When you initiate a Remote Management session with a managed workstation, the Remote Management Agent uses NDS® to verify whether you have the Remote Management rights. On successful verification, the Remote Management session proceeds.

You can use the Remote Management policy to specify the preferred protocol (IP or IPX™) that the agent should use to communicate with the management console during a remote session. For details, see "Setting Up the Remote Management Policy" on page 129.

If you select a protocol that is not available on that managed workstation, the agent will attempt to use the available protocol. The management console attempts to contact the agent using the network addresses stored within the Workstation object in NDS. It will cycle once through the network addresses trying to communicate with the agent on the managed workstation. For IP addresses in the workstation, the management console attempts to contact the agent using IP. For IPX addresses stored in the Workstation object, the management console attempts to contact the agent using IPX. However, for the management console to communicate with the managed workstation using IPX, ensure that the IP as well as IPX stacks are installed on the managed workstation. If only the IPX stack is installed, the management console will not be able to communicate with the managed workstation using IPX. For any two machines to communicate, there must be a common protocol stack available on both machines. This has been depicted in the following illustration.



IMPORTANT: IPX support for Chat, Diagnostics, File Transfer, and Remote Wake Up is not available.

Installing the Remote Management Component

Before you install the Remote Management component, ensure that all the installation prerequisites for Remote Management are met. For details, see Installation Prerequisites for Remote Management in Remote Management in *Getting Started*. ZfD 3.2 Remote Management functionality can be used to remotely manage Windows 95/98 or Windows NT/2000 workstations. If you need to remotely manage Windows NT/2000 servers, you can use the ZENworks for Severs Remote Management functionality. For more information, see the *ZENworks for Servers* documentation (http://www.novell.com/documentation).

To install the Remote Management Agent, ensure you have administrator rights.

To remotely access a workstation from the ZfD 3.2 management console, the appropriate Remote Management Agent must be loaded on that workstation. The Remote Management Agent is a service installed on the Windows 95/98/NT/2000 workstation and runs automatically after installation. The agent can be installed using the Novell Application Launcher™ (NAL), the login script or RMSETUP.EXE.

The preferred method for installing the agent is to add the Remote Management Install Application object to the Application Launcher and associate the Application object with the managed workstation. The Remote Management Install Application object is created in NDS during ZfD 3.2 installation.

The following sections provide information about installing the Remote Management Agent on Windows 95/98/NT/2000 workstation:

- “Installing the Remote Management Agent using the Application Launcher” on page 127
- “Installing the Remote Management Agent using the Login Script” on page 128
- “Installing the Remote Management Agent using the RMSETUP.EXE Program” on page 128

IMPORTANT: For Windows NT/2000 managed workstations, you must associate the Application object with the Workstation object or the Container of the Workstation object. You will not be able to launch the Application object if you associate it with a User object.

Installing the Remote Management Agent using the Application Launcher

To install the Remote Management Agent using the Application Launcher:

1. From the management console, right-click a managed workstation.
2. Click Properties > Applications.
3. Click Add > browse to select Remote Management Install.
4. From the Applications Page, select one of the following association for Remote Management Install.

Application Object Option	Explanation
Force Run	Runs the Remote Management Install Application object as soon as the application starts at the managed workstation.
App Launcher	Displays the Remote Management Install Application object icon in the Application Launcher and Application Explorer (browser view) depending on which ones you make available at the managed workstation.

Application Object Option	Explanation
Start Menu	Displays the Remote Management Install Application object icon on the Windows 95/98 or Windows NT/2000 Start menu under Novell Application Launcher.
Desktop	Displays the Remote Management Install Application object icon on the Windows 95/98 or Windows NT/2000 desktop area.
System Tray	Displays the Remote Management Agent icon on the system tray.

5. Click OK.
6. Double-click the Remote Management Agent from the Application Explorer.

   NOTE: Upgrade the ZfD3.2 Remote Management files on the ZENworks server before running the Remote Management Install object from the Application Explorer.

Installing the Remote Management Agent using the Login Script

If the NAL components are not installed on the ZENworks server and the target machine, you can add the Remote Management Agent install program (RMSETUP.EXE) in the login script, at any user/container object level.

To add RMSETUP.EXE to the login script:

1. From ConsoleOne®, right-click the container or any user object, then click Properties > Login Script.
2. Add the following line to the login script:

   ***#ZENworks_server_name*\SYS\PUBLIC\ZENWORKS\RMSETUP.EXE**
3. Click Apply > Close.
4. From the target workstation, log in as user where the modified login script is associated.

Installing the Remote Management Agent using the RMSETUP.EXE Program

1. From the workstation where you want to install the Remote Management Agent, map to the SYS:\PUBLIC\ZENWORKS directory located on the ZfD server.
2. Double-click RMSETUP.EXE

   This automatically installs the Remote Management Agent files on the managed workstation.

Setting Up Remote Management Security

In order for the Remote Management Agent to accept a Remote Management request, the managed workstation must be registered in NDS and be imported as an NDS Workstation object. The Remote Management Agents use NDS authentication to verify that the user requesting to remotely access the managed workstation is authorized to do so. The effective policy settings based on which the administrator performs Remote Management sessions on the managed workstation are taken from the NDS Workstation object and the User object of the user logged in to the managed workstation.

The ZfD 3.2 management console runs from ConsoleOne. The Remote Management Agents are NDS authentication-aware and policy-aware and will not allow unauthorized Remote Management sessions.

The following sections provide information about setting up security for Remote Management sessions:

- "Setting Up the Remote Management Policy" on page 129
- "Setting up the Required Rights for the Management Console User" on page 132
- "Authenticating Remote Management Sessions" on page 132
- "Monitoring Login and Logout Events" on page 132

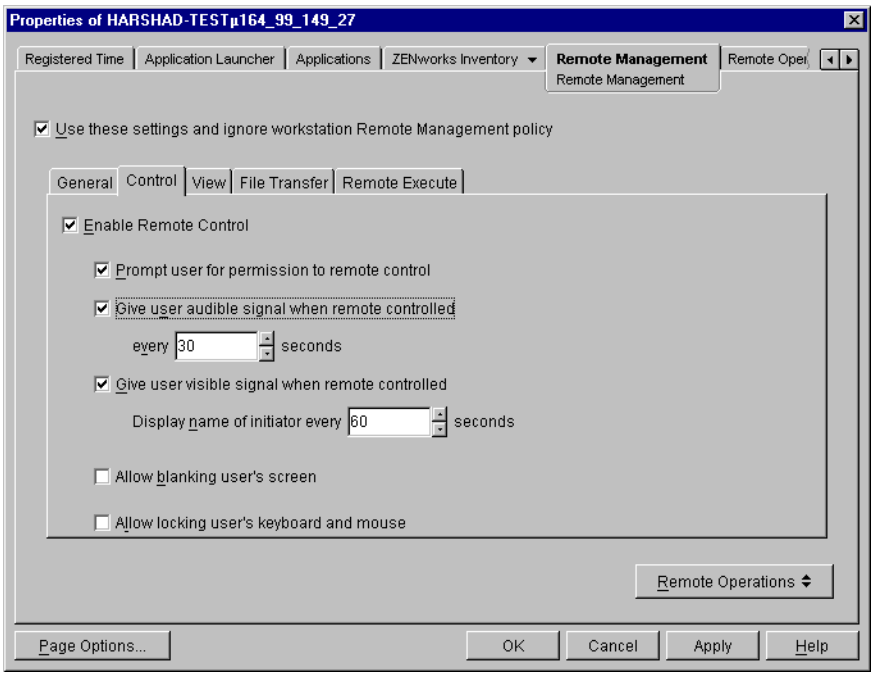
Setting Up the Remote Management Policy

The Remote Management policy is an NDS object in a policy package. Policy packages are NDS objects that contain policies grouped according to the object type. Object types can be Workstation object, User object, User Group, or Container object.

The Remote Management policy enables the administrator to specify security settings for various Remote Management sessions. The administrator can use the ZENworks Policy wizard to create a policy package or use an existing Remote Management policy for an object. The policy packages are categorized into Workstation Policy Packages and User Policy Packages. The Workstation Policy Package and the User Policy Package are further categorized based on the operating system of the workstation or the operating system that the user is logged in to. Each policy package has a set of default policies that you can use. By default, the Remote Management policy is available from all the listed policy packages provided by ZfD 3.2, including:

- Win95-98 User Package
- Win95-98 Workstation Package
- WinNT-2000 User Package
- WinNT-2000 Workstation Package

The following figure displays the Remote Control security options available from the Remote Management policy.



The following table provides a description of security options available in the Remote Management policy.

Parameter	Applicable for	Description
Enable Remote Management session	Chat, Diagnostics, File Transfer, Remote Control, Remote Execute, and Remote View	Indicates whether the administrator is allowed to perform the remote session on the managed workstation. Ensure that the Remote Management session is enabled on the Workstation policy for the Workstation object and User policy for the user logged in to the managed workstation.
Display Remote Management Agent icon	Chat, Diagnostics, File Transfer, Remote Control, Remote Execute, and Remote View	Indicates whether the Remote Management Agent should be displayed on the managed workstation each time the administrator initiates a Remote Management session. If this option is checked on the effective Workstation policy for the Workstation object, the Remote Management icon will be displayed on the managed workstation.
Select protocol to use during Remote Management sessions	Remote Control and Remote View	Indicates the protocol that should be used during the Remote Management session. If the selection is made on the effective Workstation policy for the Workstation object, the selected protocol will be used for the Remote Control or Remote View session.

Parameter	Applicable for	Description
Prompt user for permission	File Transfer, Remote Control, Remote Execute, and Remote View	Indicates whether the administrator should obtain permission from the user at the managed workstation each time the administrator wants to perform the remote session on the managed workstation. If this option is checked on the effective Workstation policy for the Workstation object or the effective User policy for the user logged in to the managed workstation, a Remote Management session will proceed only if the user logged in to the managed workstation provides the permission when prompted.
Give user audible signal	Remote Control and Remote View	Indicates whether an audible signal should be sent to the managed workstation each time the administrator accesses the managed workstation. If this option is checked on the effective Workstation policy for the Workstation object or the effective User policy for the user logged in to the managed workstation, the user at the managed workstation will receive an audible signal each time the administrator accesses the managed workstation.
Give user visible signal	Remote Control and Remote View	Indicates whether a visible signal should be sent to the managed workstation each time the administrator accesses the managed workstation. If this option is checked on the effective Workstation policy for the Workstation object or the effective User policy for the user logged in to the managed workstation, the user at the managed workstation will receive a visible signal when the administrator accesses the managed workstation.
Allow locking keyboard and mouse controls of managed workstation	Remote Control	Indicates whether the administrator is allowed to lock the keyboard and mouse controls of the managed workstation. When this option is selected, the Locking Controls button will be displayed in the toolbar of the Viewing Window. If this option is checked on the effective Workstation policy for the Workstation object and the User object, the Locking Controls button will be displayed in the toolbar of the Viewing Window.
Allow blanking screen of managed workstation	Remote Control	Indicates whether the administrator is allowed to blank the managed workstation screen. When this option is selected, the Screen Blanking button will be displayed in the toolbar of the Viewing Window. When you enable this option, the Locking Controls option will be enabled automatically. If this option is checked on the effective Workstation policy for the Workstation object and the User object, the Screen Blanking button will be displayed in the toolbar of the Viewing Window.

The administrator can change the default settings on any page of the Remote Management policy. If you change the values of the default protocol and Remote Management Agent icon settings, you have to restart the Remote Management Agent for the changes to take effect. The new settings will apply for all ensuing Remote Management sessions.

NOTE: To traverse the options of the Remote Operations button, press Ctrl+PageUp or Ctrl+PageDown.

Setting up the Required Rights for the Management Console User

You can use the Manage Remote Operators wizard to set up the required rights for the management console user. Alternatively, you can use the Remote Operators tab to add the user as a management console user while giving the appropriate Remote Management rights.

To set required rights using the Remote Operator tab:

1. Right-click the workstation object from the management console.
2. Click Properties > the Remote Operator tab > Add.
3. In the Select Objects dialog box, do the following:
   - **3a** Select an object type from the Object Type drop-down list.
   - **3b** To list the contents of a higher container, select the container from the Look in drop-down list.
   - **3c** Select an object and click OK.
4. Click Apply > OK.

Authenticating Remote Management Sessions

Remote Management session authentication in ZENworks 2 required the management console and managed workstation to always contact the Master Replica of the NDS partition that held the Workstation object. This dependency on the Master Replica would sometimes slow down the authentication process if the Master Replica was not on the same network as the management console and managed workstation. This constraint has been removed in ZfD 3 (with the exception listed below) to speed up the authentication wherever possible while ensuring the same level of seamless authentication.

With ZfD 3, the management console contacts any read/write replica to which the console user has access. This replica is almost always the nearest one. The reference of the replica contacted by the management console is then sent to the managed workstation.

The managed workstation uses this information and communicates with the same replica, thus ensuring that the managed workstation and the management console use the same NDS information.

HINT: If the managed workstation fails to contact the replica for which the reference has been sent by the management console, the Master Replica is still used for the purpose of authentication.

Monitoring Login and Logout Events

ZfD takes full advantage of the security functionality of NDS. NDS functionality ensures secure Remote Management sessions when users log out or new users log in to the management console or the managed workstation during a Remote Management session. The Remote Management session will terminate, restart, or continue based on the Remote Management security settings for the new user.

Action	Scenario
Session Continue	• When the remote management security settings for the new user on the managed workstation are similar to the settings for the current user • When a new user logs into the managed workstation and the Audible Signal or Visible Signal settings are different, session will continue with newer settings
Session Terminate	• When a new user logs in to the management console • When a new user logs in to the managed workstation and the Remote Control option is disabled
Session Restart	• When a new user logs in to the managed workstation and the Screen Blank or Lock Controls settings are different, the session will restart with newer settings • When a new user logs in to the managed workstation and if permission for a remote session is required from the user at the managed workstation

Tasks Supported by the Remote Management Agent

The following sections describe the Remote Management tasks of ZfD3.2 that the Remote Management Agent supports:

- "Remotely Powering Up a Network Node" on page 133
- "Remotely Controlling a Managed Workstation" on page 133
- "Remotely Viewing the Desktop of a Managed Workstation" on page 134
- "Remotely Executing an Executable on a Managed Workstation" on page 134
- "Remotely Diagnosing Problems on a Managed Workstation" on page 134
- "Performing File Transfer Operations between the Management Console and a Managed Workstation" on page 134
- "Communicating with a User at a Managed Workstation" on page 134
- "Recording Events as Log Files" on page 135

Remotely Powering Up a Network Node

You can remotely power up a powered-down node in your network if the network card on the node is Wake on LAN* enabled. This feature lets the administrator manage nodes during off-hours to minimize the downtime users experience for system maintenance and upgrades. It also facilitates power savings while keeping systems available for maintenance. Ensure that you meet the prerequisites for initiating a Remote Wake Up session. For details, see Managing a Remote Wake Up Session in Managing Remote Workstations in *Administration*.

Remotely Controlling a Managed Workstation

You can control a managed workstation from ConsoleOne using the Remote Control feature so that you can provide assistance to the user at the managed workstation to resolve workstation problems.

Remote Control establishes connections between the management console and the managed workstation. With remote control connections, the administrator can go beyond viewing the managed workstation to taking control of it.

Remotely Viewing the Desktop of a Managed Workstation

You can view the desktop of the managed workstation from your desktop using the Remote View feature.

Remote View lets you connect with a managed workstation so you can view the managed workstation instead of controlling it. This will help you troubleshoot problems that the user encounters. For example, you can observe how the user at the managed workstation performs certain tasks to see if the user performs a task incorrectly.

Remotely Executing an Executable on a Managed Workstation

Remote Execute lets you run any executable on the managed workstation from the management console. An application can be remotely executed by specifying its executable name in the Remote Execute window if the program is in the path of the managed workstation or by entering the complete path of the application if it is not in the path of the managed workstation.

You can determine the value of the path from the Environment window launched from the Diagnostic feature of ZfD.

Remotely Diagnosing Problems on a Managed Workstation

Diagnostics shorten problem resolution times and assist users without requiring a technician to come to the troubled workstation. This increases user productivity by keeping desktops up and running.

Remote diagnostic information of managed workstations is available over IP only; IPX is not supported. Remote diagnostics is not supported on Windows 3.*x* managed workstations.

Performing File Transfer Operations between the Management Console and a Managed Workstation

File Transfer lets you perform file operations between the management console and a managed workstation. To transfer files between the management console and the managed workstation, ensure that the Remote Management Agent is installed on the managed workstation.

Using File Transfer, you can move or copy files between the management console and a managed workstation. You can also rename and delete files, and create directories on the management console and on the managed workstation. From the File Transfer window, you can view the properties of files and directories on the management console and on the managed workstation, including size of the file, and the date and time of file creation. File Transfer also lets you open files with the associated application on the management console.

The File Transfer program does not allow access to non-fixed drives on the managed workstation. File Transfer is not supported on Windows 3.*x* managed workstations.

Communicating with a User at a Managed Workstation

Chat is a real-time messaging tool that lets the management console user communicate with a user at the managed workstation. Only a management console user logged in as an administrator can initiate a chat session. To chat with the user at the managed workstation, you need to ensure that the Remote Management Agent is installed on the managed workstation.

When the management console user initiates a chat session with the user at the managed workstation, the user at the managed workstation will be prompted for permission to initiate the chat session. The chat session begins when the user at the managed workstation provides the permission to initiate the chat session. During the chat session, you can copy and paste text in the

message area. Either the management console user or the user at the managed workstation can close the chat session.

Chat is not supported on Windows 3.*x* managed workstations.

Recording Events as Log Files

The Windows NT/2000 event logging mechanism allows applications running on the managed workstation to record events as log files. You can use the Event Viewer to view the event logs. The Event Viewer maintains Application, Security, and System log files. The events for Remote Management sessions are stored in the Application log file. The managed workstation on which the Remote Management Agent is installed maintains this log information as an audit log.

IMPORTANT: ZENworks 2 stored audit information of Remote Management events in the SECURITY log file. ZfD stores the audit information in the APPLICATION log file. You can save the information of previous events using the Save As option from the File menu of the Event Viewer.

Initiating Remote Management Sessions

Remote Management security is enabled when a remote management session is initiated by the administrative user (the network administrator or another user). The following table provides information about how you can initiate a Remote Management session:

Remote Management Session	To Initiate
Ping	Right-click the managed workstation > click Actions > click Ping Remote Management Agent.
Remote Control	Right-click the managed workstation > click Actions > click Remote Control.
Remote View	Right-click the managed workstation > click Actions > click Remote View.
File Transfer	Right-click the managed workstation > click Actions > click File Transfer.
Remote Execute	Right-click the managed workstation > click Actions > click Remote Execute.
Chat	Right-click the managed workstation > click Actions > Chat.
Diagnostics	Right-click the managed workstation > click Actions > click Diagnostics.
Remote Wake Up	Right-click the managed workstation > click Actions > click Remote Wake Up.

ManageWise and ZfD Interoperability

The following section provides information about how you can manage a remote workstation from the ManageWise® Desktop Manager in a scenario where the managed workstation has the ZfD 2 or later Remote Management Agent installed on it.

Managing Remote Workstations from the ManageWise Console

The following prerequisites must be met before you begin to remotely access the managed workstation from the ManageWise Desktop Manager:

- Register and import the managed workstation in to NDS
- Acquire the rights to remotely access the managed workstation

To initiate a Remote Management session from the ManageWise Desktop Manager:

1. Log in to the ManageWise server as a member of ManageWise group.

   This ensures that the scan information is sent to the ManageWise Inventory database with the following ZfD attribute information:

   ZEN_DIST_NAME

   ZEN_TREE_NAME

2. To view the inventory attributes from the ManageWise Desktop Manager, right-click the managed workstation > click Inventory Information.

   The Device Inventory information is displayed.

3. If the ZfD 2 or later Remote Management Agent is installed on the managed workstation, map to the SYS: volume on the ZfD server. If the ZfD 2 or later Remote Management Agent is installed on the managed workstation, map to the SYS: volume on ZfD 2 or later server.

4. Click the managed workstation > Tools > click one of the following remote operations:

   - Control Station
   - Chat
   - File Transfer
   - Diagnostics
   - Ping

5. Enter the name of the ZfD 2 or later server.

6. Click OK.

   NOTE: If you import a managed workstation from the ManageWise Segment Map and remotely control that workstation, the following message is displayed: "The operation is not supported for this node." This message indicates that you can remotely control the managed workstation only from the ManageWise Desktop Manager.

7 Workstation Inventory

Novell® ZENworks® for Desktops 3.2 (ZfD 3.2) inventory management gathers hardware and software inventory information for workstations into a centralized Inventory database. Using this database, the network administrator views, queries, or generates inventory reports for complete inventory information for the enterprise.

ZfD inventory is targeted at large global enterprises with up to 250,000 workstations spread across the world. Network sizes in the mid-size (100-1,000 nodes) PC LAN and WAN environment and smaller size PC LAN environments can also benefit by the scalable design of ZfD inventory.

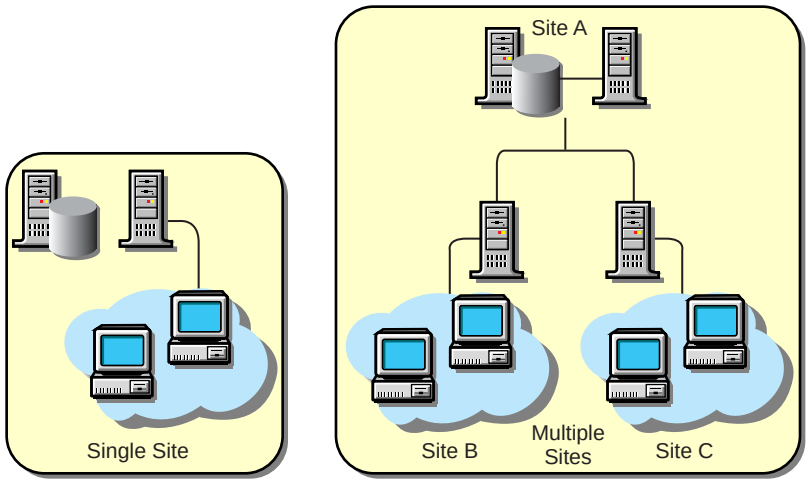
This document covers the following information:

Inventory Terminology

The following inventory terms are used in this document:

Inventory Sites

A single site consists of a simple network environment of workstations and at least one server. A site is typically a geographical location. There can be multiple sites. The following illustration depicts a single site with a server and workstations attached to it. This illustration also depicts multiple sites.



Inventory Server

Workstations to be scanned are connected to the inventory server in a LAN environment. The scanners send the scan data to the attached inventory server, which should be the nearest inventory server.

In ZfD, you identify an inventory server for each workstation in the network using the Workstation Inventory policy based in Novell eDirectory™.

Database Server

The Inventory database stores the scan information of the workstations at a site.

At any site, a server that has an Inventory database is a database server. A database on a server has scan information for all the workstations attached to that server and also the scan information of all the workstations attached to its lower-level servers, if any.

The Inventory database is maintained in Sybase* or Oracle*.

ZfD contains ten database files. Each file can grow to 2 GB on the database server. The total database size can be a maximum of 20 GB.

Root Server

The Root Server is the highest-level server in the inventory tree hierarchy. This server has an Inventory database that contains the inventory information of all lower-level servers. At the Root Server level, you can view complete inventory information for the entire enterprise.

Intermediate Server

The Intermediate Server is a staging server for moving the data from the lower-level servers up the server hierarchy.

NDS Tree

The eDirectory Services tree consists of eDirectory objects such as multiple levels of organizational units, users, groups, and other network resources. This hierarchical structure is referred to as the eDirectory Tree in this document. For more information, see the eDirectory documentation Web site (http://www.novell.com/documentation).

What's in ZfD Inventory Management

ZfD provides the following new features to achieve higher scalability:

- Minimizes the scanning data traffic on the network by employing a delta scan of workstations.

  The scanners collect hardware and software information from the workstations. Complete inventory scanning of a large number of workstations is time-consuming. Moreover, most workstations may not have new hardware or software changes since the last scan.

  In ZfD, the scanner tracks the complete inventory of the workstation in an initial full scan. In the next scanning process, the Scanner compares the current inventory data to history it maintains and collects the delta changes in the inventory.

- Provides roll-up of inventory information across servers for large networks.

  ZfD supports roll-up of scan data in large networks with a central database. The inventory data is sent across the servers to the centralized database. In such roll-ups of inventory data, only the changes are moved to the intermediate servers, if any, and finally to the highest level server with the database.

- Provides validity of scan data.

  The inventory components verify the validity of the scan data files before processing the scan data.

- Allows compression of data for roll-up.

  The scan data is compressed and only the compressed scan data is transferred to the next-level server.

- Allows roll-up of changed scan data only.

  Because the scanners report the delta changes in the inventory, the roll-up of scan data transfers only changed inventory information for the workstations. Also, the servers do not retain the scan data once it is transferred to the database.

- Provides WAN-friendly roll-up of scan data.

  In ZfD, the roll-up of scan data handles WAN-related problems, such as the WAN link being down. If the WAN link goes down, the remaining data is transferred after the link is up.

- Supports DMI 2.0 compliance for compatibility with CIM 2.2-compliant SQL databases.

  ZfD scans for DMI 2.0-instrumented workstations and maps the scan data to the CIM 2.2 schema.

- Allows software scanning using Microsoft* Installer (MSI).

ZfD lets you scan the installed applications on the workstations using the information from Microsoft Installer.

- Supports maintaining the Inventory database in Sybase.

  ZfD configures the Inventory setup for maintaining the inventory information in a Sybase database.

- Provides maintenance of the Inventory database in Oracle.

  Allows the Inventory database to be configured for any existing Oracle setup in your network.

- Provides an optimized database schema.

  The Inventory database is optimized in terms of speed and storage. The database is scalable to the enterprise level and accommodates the inventory information for several thousand workstations.

- Provides simplified database management tools (backup, deletion, organizing database spaces).

  The Backup tool allows you to back up the Inventory database at frequent intervals. The NDS-DB Sync tool verifies that all eDirectory workstation objects exist in the database, and it deletes all obsolete workstation objects from the database.

  The AlterDBSpace tool for Sybase organizes the database files across multiple volumes on the server.

- Provides a database extraction wizard for using the inventory data in external databases, reporting tools, and other applications.

  ZfD lets you export the inventory information in to a comma separated value (CSV) file format.

- Provides predefined inventory reporting.

  You can use the set of predefined reports to filter the inventory information and generate the reports from the Inventory database.

- Allows definition of inventory roles for servers.

  ZfD allows you to configure the inventory setup in your network based on your network configuration. The servers that you deploy for inventory management can be configured at any time.

- Performs inventory operations on geographically separate sites.

  You can view, query, or generate the inventory information from the site databases. A site database has the inventory information for all workstations specific to the site.

- Provides status reporting (status reports, eDirectory reporting pages, export, XML status report).

  ZfD provides a status reporting mechanism that indicates success or failure of inventory scanning for troubleshooting. You can export the status reports to a CSV file or tab-delimited file, or view the status reports in any third-party XML browser.

- Provides migration tools for reuse of ZENworks 2 Inventory policies and databases.

  ZfD allows the reuse of the existing Inventory policies for ZENworks 2 to configure the workstations in ZfD 3.2 You can also migrate the ZENworks 2 Inventory database to ZfD 3.2.

What's New in ZfD 3.2 Support Pack 1

ZfD 3.2 Support Pack 1 (SP1) provides a few new features and some bug fixes.

For more information on the resolved issues, see the TID10071863 at Novell Support Web site (http://support.novell.com/search/kb_index.jsp).

SP1 provides the following new features for Workstation Inventory:

- New Workstation Inventory snap-in: Reset Component Status

  ZfD 3.2 SP1 provides a new Workstation Inventory snap-in, Reset Component Status, that resets the status attribute of the Inventory Service object to its initial state.

  The status attribute contains the upgrade information of the ZfD Inventory server.

  When the Inventory Service object's status attribute is reset to its initial state, the Upgrade Service updates the schema and data of the Inventory database. This makes the Inventory database compatible with the ZfD 3.2 SP1 Inventory components.

  Use Reset Component Status if you want to run the Upgrade Service in the following scenarios:

  - Install or reinstall the existing database on the same or a different machine
  - Restore an existing database
  - Connect to different type of database

  You can run the Reset Component Status using either of the following methods:

  - In ConsoleOne®, right-click the Inventory Service object > click ResetComponentStatus.
  - In ConsoleOne, select the Inventory Service object, click the Tools menu, then click ResetComponentStatus.

  After resetting the component status, you must perform the following tasks:

  - Restart the Inventory Service Manager.
  - Trigger a Full scan on the Inventory Service object to rescan all the inventoried workstations.

- You can now configure the following scan parameters by using the SCANSOURCE.INI file:

  - Floppy drive scan parameters such as doFloppyScan, doDMIFloppyScan, and doWMIFloppyScan
  - Logical drive scan parameters such as doWMILogicalDriveScan and doLogicalDriveScan

  By default, the values of these parameters are set to TRUE.

  Following are the valid configuration settings:

  - ```
    [FLOPPY]
    doFloppyScan = FALSE
    ```

    The Inventory scanner will not scan for the floppy drive.

  - ```
    [FLOPPY]
    doDMIFloppyScan = FALSE
    ```

The Inventory scanner will scan for the floppy drive but will not scan from DMI. The floppy drive can be scanned from WMI or Probe.

- `[FLOPPY]`

  `doWMIFloppyScan = FALSE`

  The Inventory scanner will scan for the floppy drive but will not scan from WMI. The floppy drive can be scanned from DMI or Probe.

- `[FLOPPY]`

  `doWMIFloppyScan = FALSE`

  `doDMIFloppyScan = FALSE`

  The Inventory scanner will scan for the floppy drive but will not scan from WMI and DMI. The floppy drive can be scanned only from Probe.

- `[LOGICALDRIVE]`

  `doLogicalDriveScan = FALSE`

  The Inventory scanner will not scan for the logical drives.

- `[LOGICALDRIVE]`

  `doWMILogicalDriveScan = FALSE`

  The Inventory scanner will scan for the logical drives but will not scan from WMI. The logical drive is scanned from Probe.

- You can now disable scanning of DMI

  To disable scanning of DMI, edit the *Inventory_server_installation_path*\PUBLIC\ZENWORKS\SCANSOURCE.INI file to add the following entry in the [SOURCE] section:

  `doDMIScan= FALSE`

  By default, the SCANSOURCE.INI file does contain this entry indicating that the DMI scanning is enabled.

- You can now configure the Inventory scanner to periodically send full scans

  On the Inventory server, edit the PUBLIC\ZENWORKS\SCANSOURCE.INI file to add the following entry in the [SOURCE] section:

  `FullScanSchedule=`*`interval_for_full_scan`*

  The value of *interval_for_full_scan* must be between 5 and 100.

  For example, if the value of FullScanSchedule is set to 10, the Inventory scanner will send a full scan after every ten delta scans.

Overview of Inventory Components

Before planning ZfD inventory deployment, you should understand the inventory components, which interact together to perform inventory functions.

The following sections help you to understand ZfD inventory:

- “Inventory Components in ZfD” on page 143
- “Inventory Terminology” on page 137

Inventory Components in ZfD

ZfD inventory uses the following independent components for inventory scanning at workstations:

Inventory Scanners

Platform-dependent scanners determine the hardware and software configurations of workstations. These scanners are located on the ZfD Inventory Server. When executed on the workstations, the scanners collect the inventory information for the workstations and store the scan data as .STR files on the servers.

The WINSCAN.EXE scanner scans Windows* 95/98 workstations over IP/IPX™. The NTSCAN32.EXE scanner scans Windows NT*/2000 workstations over IP/IPX.

Using the Workstation Inventory policy, you can configure the scan settings so you can schedule the scanning on the workstations, enable a software scan, customize software scanning, and specify the location of the scan data files.

Inventory Components on Servers

The inventory components process the scan data. The following components are Java* programs that work identically on NetWare® and Windows NT/2000 servers:

- Selector

  The Selector processes the scan data files to determine whether the new scan data should be merged with the existing data and places the files in the appropriate directories for the Sender and the Storer.

- Sender and Receiver

  The Sender and the Receiver on the servers compress the scan files and then transfer the files from the lower-level servers to the higher-level servers for roll-up of inventory information. By using the Roll-Up policy, you can configure the next level destination server for roll-up, and also schedule the roll-up time.

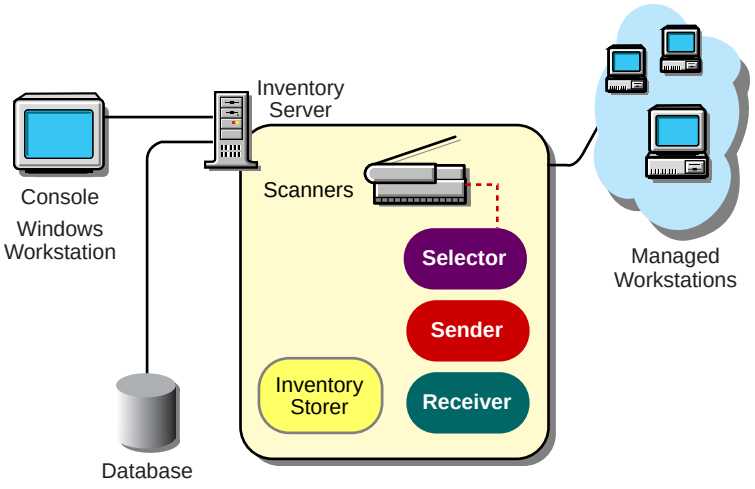
- Inventory Storer

  The Storer stores the collected inventory information (.STR files) in the Inventory database. By using the Database Location policy, you can configure the properties of the Inventory Database object in ZfD 3.2 and associate the Database object to a server.

Inventory Database

The Inventory database functions as a repository of workstation hardware and software information. In ZfD 3.2, the database is a relational database management system (RDBMS) maintained in Sybase or Oracle.

The following illustration shows the list of inventory components on the server and workstation. This illustration also depicts how the inventory components interact with each other.



Front End Console

The ZfD Console uses ConsoleOne, the Novell single management tool for administration. This is a Java-based console that includes snap-ins for inventory management operations.

Inventory Server Configurations

The following sections will help you configure your ZfD servers:

- “Deploying Inventory in a LAN Environment” on page 144
- “Deploying Inventory over a WAN Environment” on page 146

IMPORTANT: The recommendations discussed in the scenarios are generic because of the unique nature of the topology; further refinements may become necessary.

Deploying Inventory in a LAN Environment

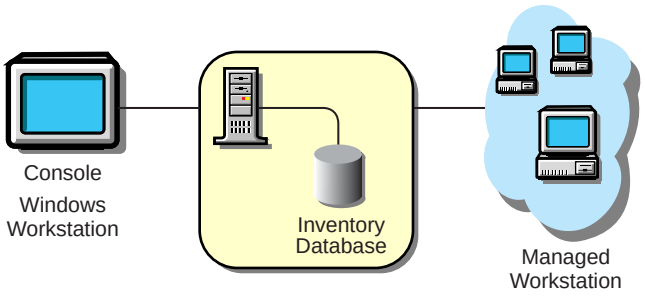
In ZfD, the deployment of inventory in a LAN environment implies deploying the product on a single inventory site.

The following scenarios and recommendations are addressed:

- “Scenario 1: LAN Environment with up to 5,000 Workstations” on page 144
- “Scenario 2: LAN Environment with more than 5,000 Workstations” on page 145
- “Recommendations for Deployment in a LAN Environment” on page 145

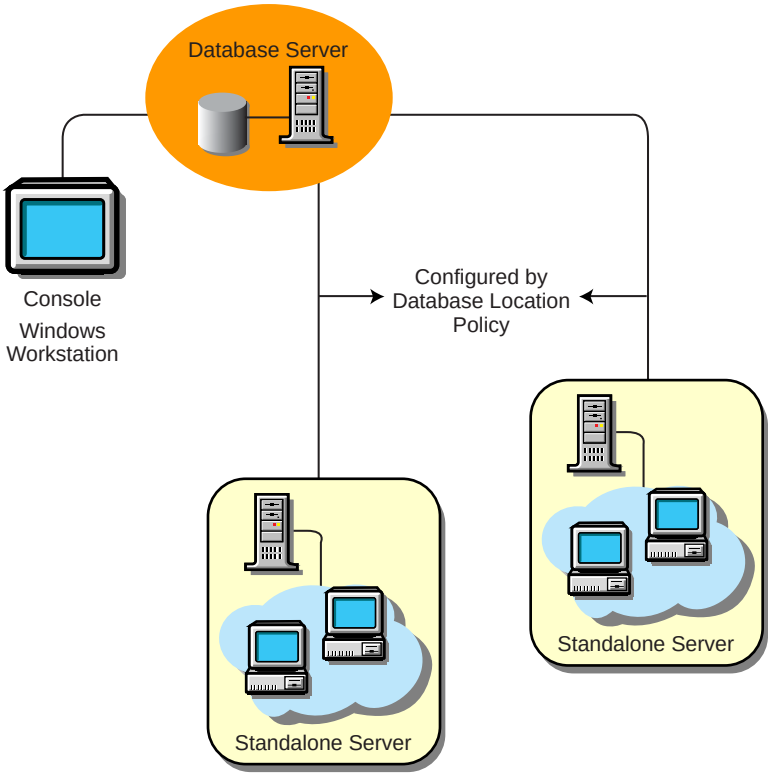
Scenario 1: LAN Environment with up to 5,000 Workstations

In this type of inventory configuration, the inventory server components and database are located on a Standalone Server. The Standalone Server is an inventory server with an Inventory database. There is no roll-up of data and the Sender-Receiver components are not used. This scenario is illustrated in the following figure.



Scenario 2: LAN Environment with more than 5,000 Workstations

In this type of configuration, there are multiple inventory servers without databases. These inventory servers (two Standalone Servers) are connected to a database server. The Database Location policy configures the database server for the Standalone Servers. This inventory deployment is illustrated in the following figure.



Follow this configuration for deploying inventory up to 10,000 workstations.

For deploying inventory on more than 10,000 workstations, attach one inventory server per 5,000 workstations, with two or three inventory servers per Inventory database.

Recommendations for Deployment in a LAN Environment

- Minimum base server configuration includes 256 MB RAM and a database cache of 64 MB. For a higher workstation range, the server configuration is 512 MB RAM and a database cache of 128 MB.

- All workstations should send the scan data to the nearest inventory server on the LAN; policies must be created based on this information. To achieve this for 10,000 workstations, two or three inventory servers per Inventory database server should be sufficient.
- When you configure the inventory scanning for workstations, we recommend staggering the inventory scanning times or scan some workstations at one time.
- The transmission of scan data from inventory servers can take several hours or even more than a day. Workstation scanning is an ongoing background process, which continues until there is data to upload without any user intervention.
- If many workstations are attached to the same inventory server, we recommend that you do not schedule the scan of all workstations at the same time, because this will stress the eDirectory and the inventory server File System Services.
- When you schedule the roll-up of data in the Inventory policies, we recommend the roll-up frequency should be at least one day. If the roll-up of scan data is scheduled too frequently, for example less than one hour, there may be some performance degradation of the inventory server.
- Ensure that the time synchronization radius is set within 2 seconds.
- For all databases, the optimal database cache size requirement for the server may vary because of the server environment. Determine the database cache size that needs to be set by trying a range of cache sizes in the runtime environment. The default Sybase database cache size is 32 MB.

Deploying Inventory over a WAN Environment

In a WAN environment, complete the following tasks, in order, to design the inventory tree and deploy inventory:

- "1. List the sites in the enterprise" on page 146
- "2. Which is the ideal place for the Root Server?" on page 147
- "3. Is any other database needed?" on page 147

  "Optional step: If another database is needed" on page 148
- "4. Identify the route for Inventory data" on page 148
- "5. Identify servers on each site for Inventory, Intermediate and Database Servers" on page 148
- "6. Create the tree of servers for company Inventory collection" on page 149
- "7. Create an implementation plan" on page 150
- "8. Start the actual deployment" on page 150

"Guidelines for Creating Policies in a WAN" on page 155 covers recommendations for deployment.

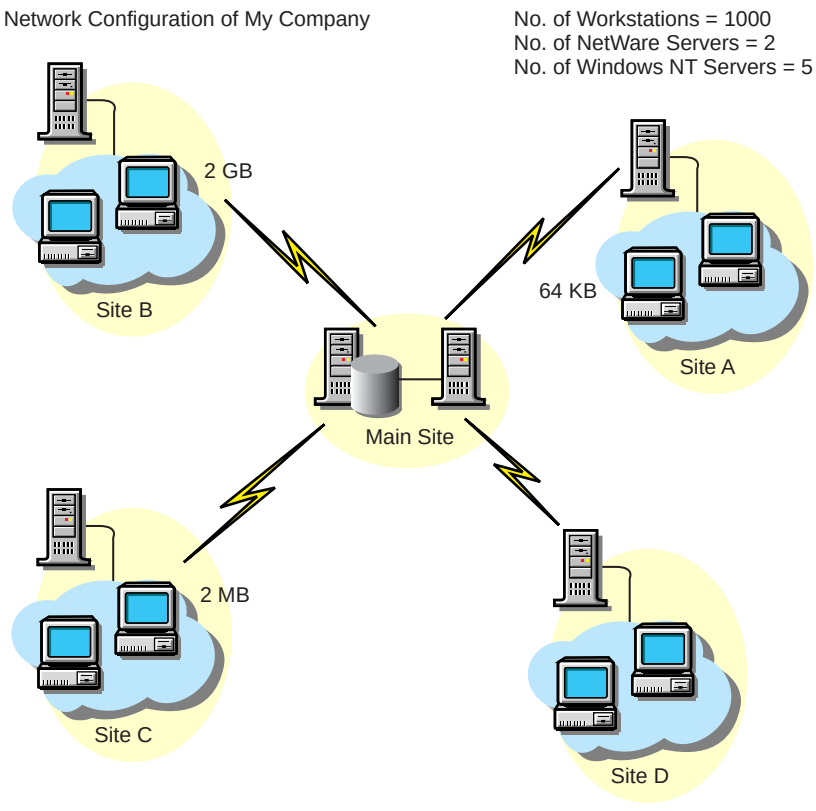
1. List the sites in the enterprise

Describe the entire network of your company.

- List the various sites in your company.
- List the physical links between the various sites.
- Identify the type of links in terms of bandwidth and reliability.

The following figure illustrates the network organization of a company with servers in different locations.

This illustration depicts four sites (Site A, Site, B, Site C, and Site D) connected to a central site. It depicts the physical links between the sites and the type of links in terms of bandwidth.



2. Which is the ideal place for the Root Server?

The Root Server in the Inventory Tree is the highest-level server. Necessarily, an Inventory database is attached to the Root Server.

The inventory information available from the Inventory database of the Root Server will consist of all information from lower-level sites on the network and from the Root Server site.

Factors that you must include:

- The Root Server should be on a site that has high network bandwidth.
- A Console administrator can collect workstation inventory information from any of the sites connected on high-speed links from the Root Server, or from the Root Server level site.
- A database server of suitable configuration should be provided for the inventory server. For a network with 250,000 workstations, the recommended configuration for the Root Server is 25 GB of disk space and 1 GB RAM.

3. Is any other database needed?

Besides the database at the Root Server, you can maintain database servers at different sites.

You may want to maintain additional databases if there are sites or subtrees that are managed for inventory at different locations, and these sites are connected to the network over a slow link.

You should also determine if there are specific reasons to have a separate database for a single site or a set of sites. There may be some organizational needs for your company to have the database server on different sites, even if there is no product deployment need to have any other database.

NOTE: For a majority of enterprises, there may be no need to have any other database besides the enterprise-wide single database. All site-specific reports can be easily generated from this database.

Optional step: If another database is needed

- If you decide to have additional database servers, identify the sites that need a database. Additionally, you need to examine whether the database will cater to the local site or a site with many subsites (subtrees). Also, identify the sites that require data in each Inventory database.
- All the sites served by a single database should typically access this database instead of the database at the Root Server for inventory management. This reduces the load on the database at Root Server.
- Database administrators should be available for these sites.

4. Identify the route for Inventory data

Identify the routes for inventory data for all sites to the nearest database, and then identify the route to the database on the Root Server.

To devise a route plan:

- Each route can have an intermediate server at a staging site. The Intermediate Server receives and transmits the data to the next destination. These are application-layer level routes for inventory data. There can be various network-layer level routes between two adjacent servers, which will be determined and managed by the routers in the network.
- The route provides information indicating how inventory data travels from a particular site to its final destination, which is the database at the Root Server.
- There may be multiple routes. Choose the fastest and most reliable route. To determine the route, consider the physical network links.
- Routes identified and made operational can be changed later, although there may be some cost in terms of management and traffic generation. If there is no intermediate database involved, you can change the route by only changing the eDirectory-based policy.
- Put Intermediate Servers on sites where the link parameters change substantially. Criteria to consider are difference in bandwidth, difference in reliability of the links, and the need for different scheduling.
- Availability of servers on the intermediate site for staging the inventory data should be considered in deciding the sites for Intermediate Servers. Provide enough disk space on these servers to store all the inventory data on the disk until the Roll-Up policy sends it to the next destination.
- Workstations should not be connected to the inventory server over a WAN because the workstation scanning should not be done across a WAN.

5. Identify servers on each site for Inventory, Intermediate and Database Servers

A single server can have different roles if it has sufficient resources. For example, an inventory server can be a Leaf Server with Database. You can also designate a server as an Intermediate Server with Database, which receives inventory from the workstations and also has an Inventory database. A server can have any combination of roles.

In ZfD, you choose the role for each server. See "Implementing the Inventory Server Roles" on page 156 for more information.

The number of workstations attached to the server also determines the load. The following table lists the disk space requirements for the server:

Server Type	Disk Space Requirements
Leaf Server	(*n1 x s*) + (*n1 x z*)
Leaf Server with Database	(*n1 x s* x 2) + {(*n1 x dbg*)}
Intermediate Server	*n2 x z*
Intermediate Server with Database	(*n2 x z*) + (*n2 x s*) + {(*n2 x dbg)}*
Intermediate Server with Workstations	(*n1 x s x 2)* + (*n2 x z*)
Intermediate Server with Database and Workstations	(*n1 x s x 2)* + (*n2 x z*) + *(n2 x s*) + {(*n1 x dbg)* + (*n2 x dbg*)}
Root Server	(*n2 x z)* + *(n2 x s*) + {(*n2 x dbg*)}
Root Server with Workstations	(*n1 x s x 2)* + (*n2 x z*) + *(n2 x s*) + {(*n1 x dbg)* + (*n2 x dbg*)}
Standalone Server	(*n1 x s x 1)* + {(*n1 x dbg*)}

In the table, *n1* is the number of workstations attached to the server.

s is the size of the scan data files. This file size varies depending on the data collected. Calculate 50 to 60 KB scan data from each workstation to calculate the load.

dbg is the storage space of the scan data in the database. Calculate 100 to 120 KB per workstation as the disk space for the database.

n2 is the number of workstations rolled up to the server.

z is the size of the compressed scan data file per workstation. Calculate 7 to 10 KB for the roll-up of 50 KB scan data.

{ } denotes the disk space of the database server, depending on whether the database is on the same server or if it is connected to the server. If the database is on the same server, calculate the total disk space including the database space for the server. For example, if the Leaf Server with Database has the Inventory database on the same server, calculate the requirements for storage of scan data, including the database disk space.

6. Create the tree of servers for company Inventory collection

Ensure that the Inventory tree you design follow these guidelines:

- The root of the tree is the Root Server.
- Servers on each site of the tree you design represent all the sites in the company.
- At least one server per site is mandatory.

- Assuming that there are workstations to be scanned on each site, there should be an inventory server role on each site.
- Optionally, there will be databases and Intermediate Servers on different sites.

7. Create an implementation plan

After you design the tree, you should develop an implementation plan to cover the phased deployment plan for the network.

Some guidelines for the implementation plan:

- Start the deployment from the Root Server site and connect the servers on other sites to the Root Server.
- The main criterion is the number of workstations on each site and on each server.
- Deploy the product on approximately 5,000 workstations per day.

8. Start the actual deployment

After your implementation plan is finalized, start the actual deployment according to the plan.

Follow these steps:

1. Install the servers on the sites.
2. Create the policies applicable to workstations.
3. Create the Roll-Up policies to schedule the roll-up for each server.

Adding a Database server to an existing Inventory setup

If you have already configured the servers for inventory setup, and you need to add another database server, follow these instructions:

1 Run the installation program to install the Inventory database on the server.

The installation program installs the Sybase database. If you are maintaining the database in Oracle, make sure that the Oracle database exists. See "Configuring the Inventory Database for Oracle" on page 169.

2 Shut down the Inventory Services.

3 Based on the database you select, make sure that you configure the database. See "Configure the Policies for the Database" on page 166.

4 Modify the role of the existing server for the Inventory Service object.

If you are adding a new server, you need not modify the role of the server. If you want to change the role of the server, for example, from Leaf Server to Leaf Server with Database, you need to modify the role of the server in the Inventory Service object.

4a In ConsoleOne, right-click the Inventory Service object (*Servername*_ZenInvservice) > click Properties > click the Inventory Service object Properties tab.

4b Choose the new role of the Inventory Service object > click Apply.

You will see a list of actions that you should follow based on the chosen role. For example, if you change the Root Server to Root Server with Workstations, you need to configure the Workstation Inventory policy for the workstations that you have attached. Similarly, to change the role to any other server, you need to follow the instructions to make the role change effective.

Follow the actions that you need to change the role.

5 Make sure that you enforce Full Scan for the Inventory Service object.

5a In ConsoleOne, right-click the Inventory Service object (*servername*_ZenInvservice) > click Properties > click the Inventory Service object Properties tab.

5b Check the Enforce Full Scan option > click OK.

6 Bring up the Inventory service.

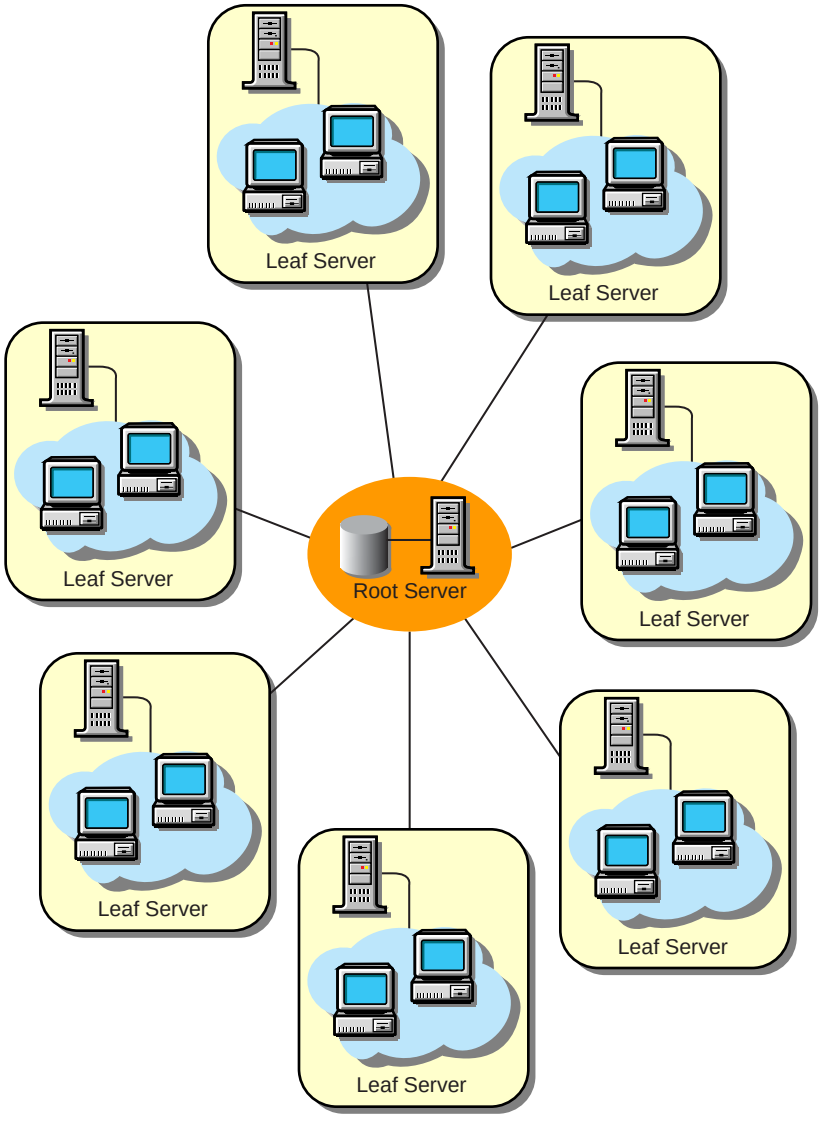
Possible Inventory Server Configurations for a WAN

The following sections cover these scenarios:

- "Scenario 1: WAN Inventory Deployment for up to 50 Inventory Sites without Intermediate Servers" on page 151
- "Scenario 2: Up to 50 Intermediate Servers Connected to the Root Server" on page 152
- "Scenario 3: Intermediate Servers with Database Connected to the Root Server" on page 153
- "Scenario 4: Database on Inventory Servers and Intermediate Servers Connected to a Root Server" on page 154

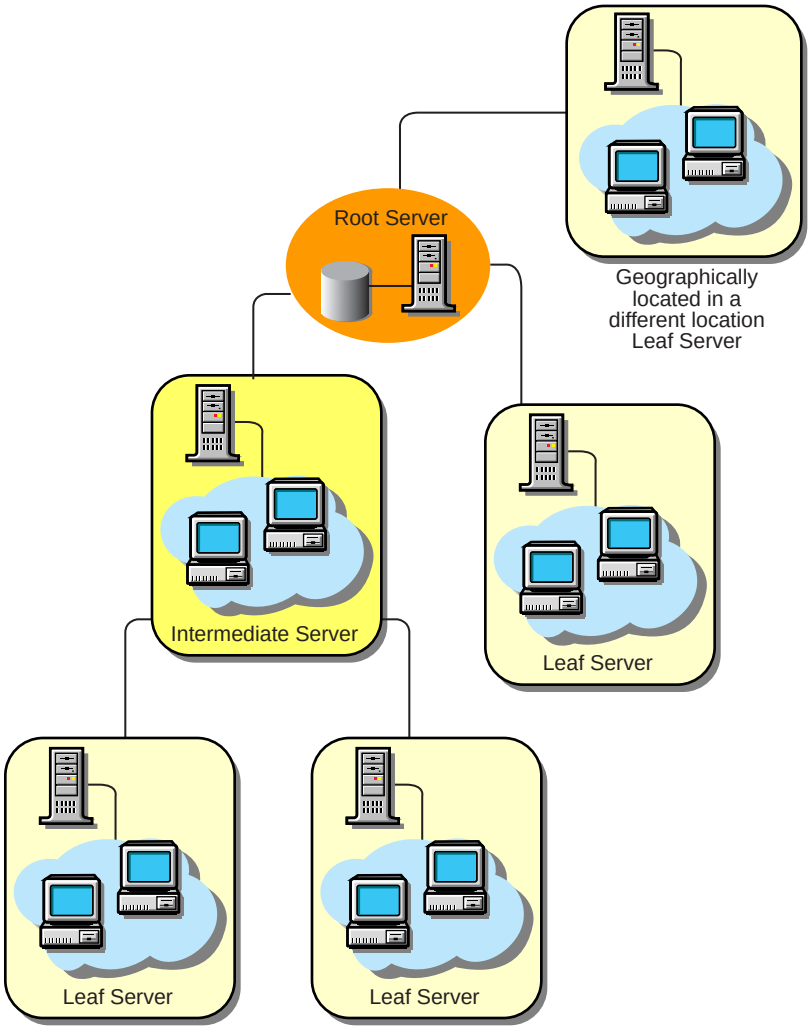
Scenario 1: WAN Inventory Deployment for up to 50 Inventory Sites without Intermediate Servers

All inventory servers are connected to a central enterprise database server. The Leaf Servers do not have a database and Intermediate Servers are not required. This scenario is illustrated in the following figure:



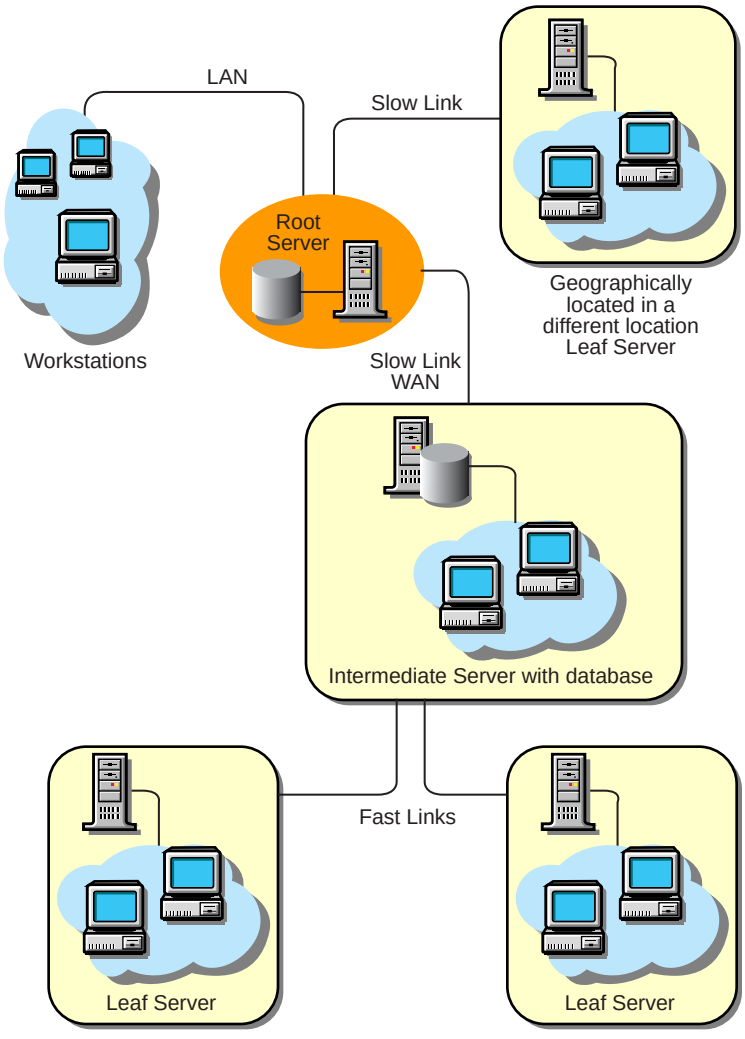
Scenario 2: Up to 50 Intermediate Servers Connected to the Root Server

In this configuration, the Leaf Servers roll up data to the next-level Intermediate Server and finally to the Root Server. Another server at a different location is also connected to the Root Server. This scenario is illustrated in the following figure:



Scenario 3: Intermediate Servers with Database Connected to the Root Server

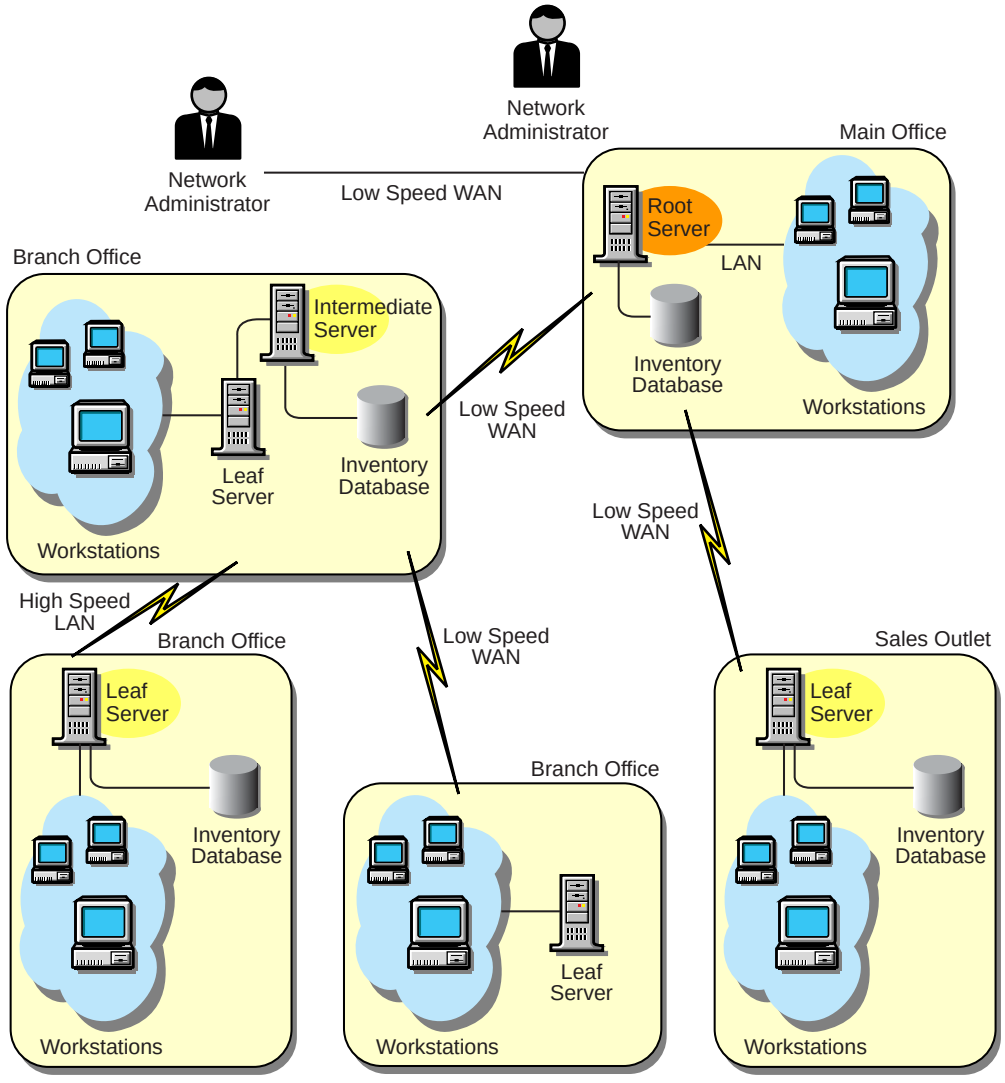
In this configuration, the inventory servers are connected to the Intermediate Server over fast WAN links. The Intermediate Server also has an Inventory database and transmits the information to the Root Server. Other servers are also connected to the Root Server. This scenario is illustrated in the following figure:



Scenario 4: Database on Inventory Servers and Intermediate Servers Connected to a Root Server

In this configuration, there are branch offices and a main office. Both branch offices store inventory information.

At one branch office, the server is a Leaf Server with Inventory Database, and the other branch office has a Leaf Server. At the next level, there is another branch office with an Intermediate Server with Database. The two branch offices at the lower level roll up data to this Intermediate Server. In turn, this Intermediate Server with Database rolls up data to the main office at the next level. There is also another sales outlet with a Leaf Server with Database at a sales outlet. This server directly rolls up data to the main office. The sales outlet and the two branch offices connect to the main office over low-speed WAN. One branch office connects to the main site over high-speed WAN. This scenario is illustrated in the following figure:



Guidelines for Creating Policies in a WAN

In this type of inventory deployment, the scanners transmit information to the servers over a WAN or dial-up connection.

- Because there are eDirectory objects on a WAN, the design of the eDirectory tree and the inventory-related objects, User objects, and User policies must be planned. Planning should follow eDirectory tree design recommendations. For more information, see the eDirectory documentation Web site (http://www.novell.com/documentation). Also, ensure that the time synchronization radius is set within 2 seconds.
- All inventory policies and workstation objects should be in the local partition. A local read/write replica must exist on the geographical location. If possible, you should prevent the inventory components, such as the scanners and the Scheduler, from accessing the WAN to read the workstation policies.
- If the objects are accessed over a WAN, (for instance, for scanning mobile user's workstations), scanning should still work, although with slower performance.
- When you configure the inventory scanning of workstations, we recommend staggering the inventory scanning to scan at different times or to scan some workstations at a time.

- If many workstations are attached to the same inventory server, we recommend that you do not schedule the scan of all workstations at the same time, because this will stress the eDirectory and the inventory server File System Service
- You can attach as many workstations to the server as determined by the number of clients supported by NetWare or Windows NT/2000 servers.
- When you schedule the roll-up of data in the Inventory policies, we recommend the roll-up frequency should be at least one day. If the roll-up of scan data is scheduled too frequently, for example less than one hour, there may be some performance degradation of the inventory server.

Implementing the Inventory Server Roles

This section describes the following roles that you assign for a server:

- "Root Server" on page 156
- "Root Server with Workstations" on page 157
- "Leaf Server" on page 160
- "Leaf Server with Database" on page 161
- "Intermediate Server" on page 158
- "Intermediate Server with Database" on page 159
- "Intermediate Server with Database and Workstations" on page 160
- "Standalone Server" on page 161

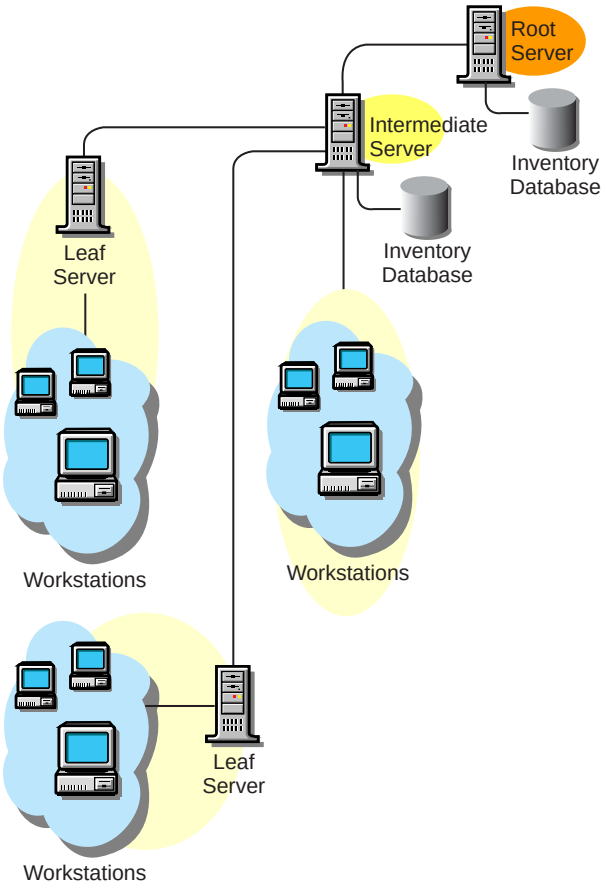
Root Server

The Root Server has the following characteristics:

- This server is the topmost server in the inventory server tree hierarchy.
- The Root Server has an Inventory database.

  The Inventory database at the Root Server contains the inventory information for all lower-level servers. At the Root Server level, you can view complete inventory information.

  In the following illustration, a Leaf Server connects to the Intermediate Server, and these Intermediate Servers are attached to the Root Server.

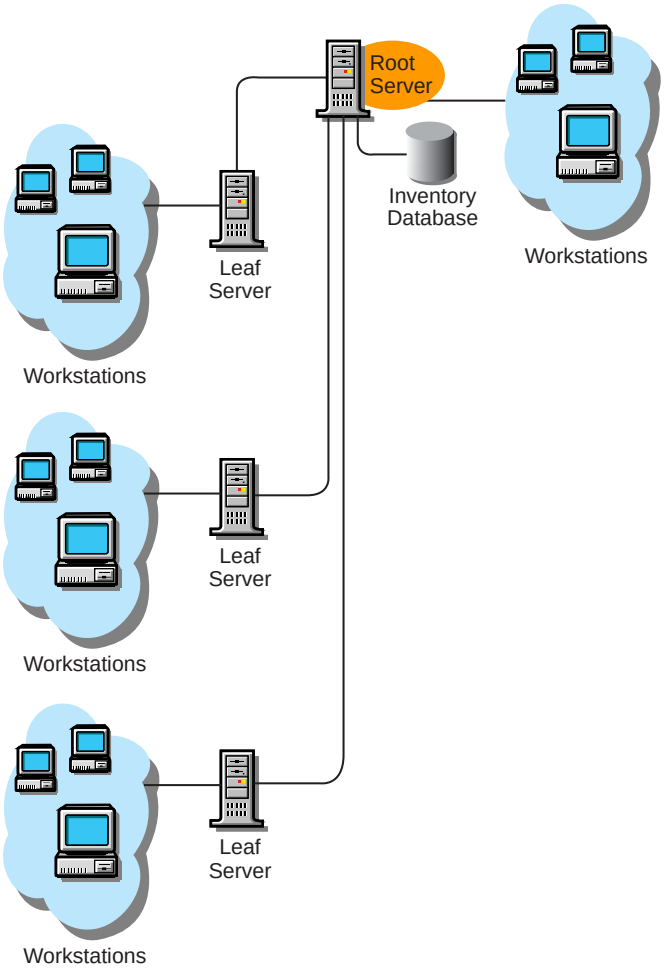


Root Server with Workstations

The Root Server with Workstations has the following characteristics:

- This server is the topmost server in the inventory server tree hierarchy.
- The Root Server with Workstations is also an inventory server with many workstations attached to it. There are workstations residing on a LAN.
- This server maintains an Inventory database.

The following illustration depicts a Root Server with Workstations:

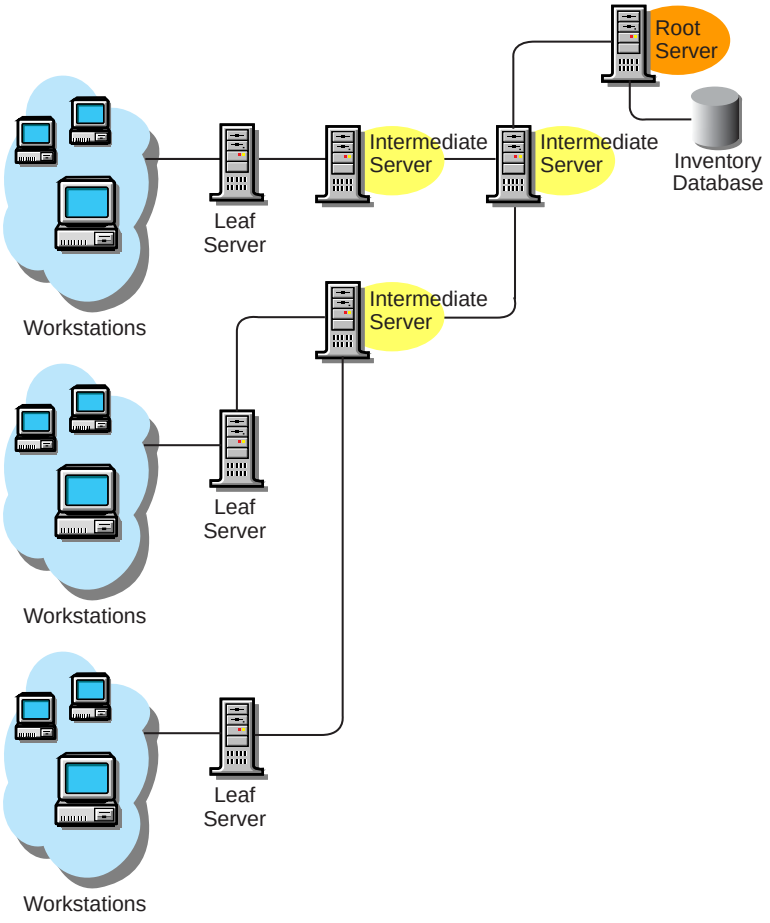


Intermediate Server

The Intermediate Server has the following characteristics:

- The server moves the scan information to the next-level server or to the Root Server.
- This server does not have workstations attached to it and does not have an Inventory database.
- An Intermediate Server acts as a staging server for the lower-level Leaf Servers.
- There can be one or more Intermediate Servers.

The following illustration depicts Intermediate Servers:



There are many Leaf Servers and Intermediate servers at different levels. The Intermediate server is a staging server for uploading the scan information to the next-level server. The last Intermediate Server is attached to the topmost Root Server. This scenario is typical if there are many Leaf Servers in different geographical locations. All the Leaf Servers move the scan data to the Intermediate Server.

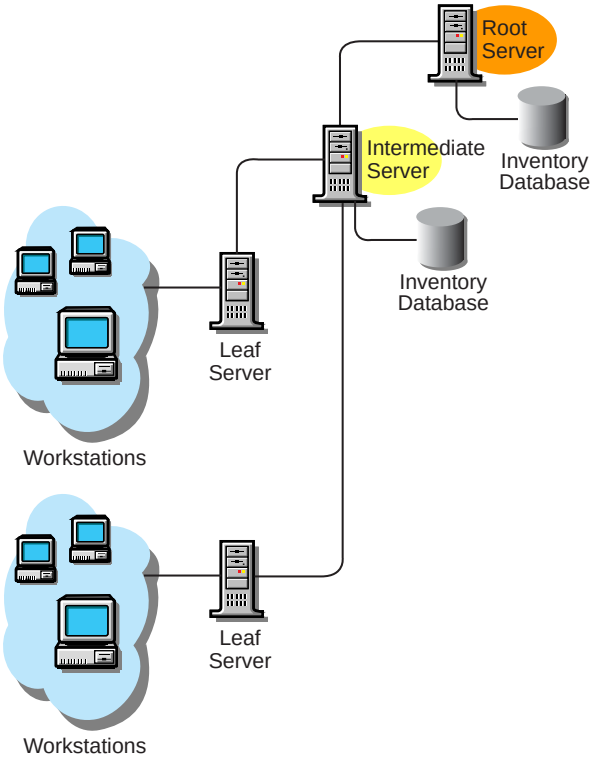
In some scenarios, the Leaf Server connects to the Intermediate Server over a WAN.

Intermediate Server with Database

The Intermediate Server with Database has the following characteristics:

- The server moves the scan information to the next-level Intermediate Server or the Root Server.
- The server has an Inventory database.
- An Intermediate Server acts as a staging server for the lower-level Leaf Servers.
- There can be one or more Intermediate Servers.

In the scenario illustrated in the following figure, there are many Leaf Servers attached to the Intermediate Server. A consolidated Inventory database of all Leaf Servers is available at the Intermediate Server level.



Intermediate Server with Workstations

The Intermediate Server with Workstations has the following characteristics:

- The server moves the scan information to the next-level Intermediate Server or to the Root Server.
- There are many workstations attached to this server.
- The server does not have an Inventory database.
- There can be one or more Intermediate Servers.
- An Intermediate Server acts as an intermediate server for the lower-level Leaf Servers.

Intermediate Server with Database and Workstations

The Intermediate Server with Database and Workstations has the following characteristics:

- The server moves the scan information to the next-level Intermediate Server or to the Root Server.
- There are many workstations attached to this server.
- The server also maintains an Inventory database.
- There can be one or more Intermediate Servers.
- An Intermediate Server acts as a staging server for the lower-level Leaf Servers.

Leaf Server

The Leaf Server has the following characteristics:

- The server is an inventory server with workstations attached to it.
- The server is at the lowest level in the hierarchy.
- This server moves the scan data to the next-level Intermediate Server or to a Root Server.
- A simple Leaf Server does not have an Inventory database. An Inventory database is not required for the inventory site because there may be only a few workstations attached to the server.

Leaf Server with Database

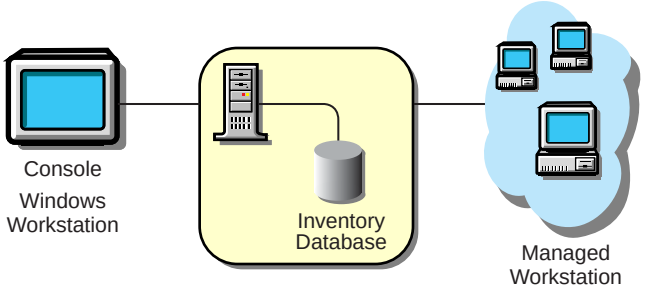
The Leaf Server with Database has the following characteristics:

- The server is an inventory server with many workstations attached to it.
- This server moves the scan data to the next-level server.
- This server has an Inventory database. You can assign a server as a Leaf Server with Database to maintain the inventory information for workstations specific to the inventory site.

Standalone Server

The Standalone Server has the following characteristics:

- This server has workstations attached to it.
- The server maintains the Inventory database.
- There is no roll-up of scan information and there are no requirements for Intermediate Servers and the Root Server.



Installing Workstation Inventory in an Existing ZfD 3 Setup

If you are installing over an existing ZfD 3 setup, follow these guidelines:

- If you are planning to install the ZfD Inventory database maintained in Sybase on a server, ensure that you shut down the existing Sybase database before running the ZfD installation program.
- Prior to installing ZfD 3.2, ensure that you have made a reliable backup of the Inventory database. After installing ZfD 3.2, you should back up the Inventory database again.

  Before you back up the database, ensure that when you run the Inventory Services, the Inventory Upgrade Service completes ZfD 3.2 updates. To check this, run listser, to display an Upgrade Service Stopped message.

When you want to restore the database backup, use the backup copy that was created after installing ZfD 3.2.

The backup database that you created before installing ZfD 3.2 is not supported in ZfD 3.2.

- If you install ZfD 3.2 on an Inventory server and there is a database server connected to the Inventory server, ensure that you install ZfD 3.2 on the database server also. Otherwise, Inventory will not function properly.
- Before you run the installation program, follow the instructions to deactivate the scanner, see "Installing Workstation Inventory to NetWare Servers" on page 162 or "Installing Workstation Inventory to Windows NT/2000 Servers" on page 162.
- If you choose an Upgrade install, ZfD 3.2 enhancements will not be installed on the server under the following conditions:
  - If the server does not have ZfD installed.
  - If you have already done a Full Install of ZfD 3.2, and are attempting to reinstall ZfD 3.2.

Installing Workstation Inventory to NetWare Servers

If the scanner is running on the workstations, the ZfD installation will not overwrite the files.

To work around this situation, follow these steps on the servers where Inventory is installed:

1. In Windows Explorer, right-click the NTSCAN32.EXE Scanner file in the PUBLIC\ZENWORKS directory > click Properties > NetWare Rights.
2. Double-click [Root]. In the Trustees option, uncheck the Read [R] and the FileScan [F] rights > click Apply > Close.
3. In Windows Explorer, right-click the WINSCAN.EXE Scanner file in the \PUBLIC\ZENWORKS directory > click Properties > NetWare Rights.
4. Double-click [Root]. In the Trustees option, uncheck the Read [R] and the FileScan [F] rights > click Apply > Close.

   Wait for some time before proceeding with the installation, in case the scanning is still in progress.
5. Complete the ZfD 3.2 installation.
6. In Windows Explorer, right-click the PUBLIC\ZENWORKS\NTSCAN32.EXE file > click Properties > NetWare Rights.
7. Double-click [Root]. In the Trustees option, check the Read [R] and FileScan [F] rights > click Apply > Close.
8. In Windows Explorer, right-click the PUBLIC\ZENWORKS\WINSCAN.EXE file > click Properties > NetWare Rights.
9. Double-click [Root]. In the Trustees option, check the Read [R] and FileScan [F] rights, click Apply > Close.

Installing Workstation Inventory to Windows NT/2000 Servers

If the scanner is running on the workstations, the ZfD 3.2 installation will not overwrite the files.

To work around this situation, follow these steps on the servers where inventory is installed:

1. In Windows Explorer, right-click NTSCAN32.EXE in the PUBLIC\ZENWORKS directory > click Properties > Security > Permissions.
2. Click Add > select Administrators > Add.
3. In the Type of Access field, select Full Control > click OK.
4. From the list, click Everyone > Remove > click OK twice.
5. In Windows Explorer, right-click WINSCAN.EXE in the PUBLIC\ZENWORKS directory > click Properties > Security > Permissions.
6. Click Add > select Administrators > Add.
7. In the Type of Access field, select Full Control > click OK.

   Wait for some time before proceeding with the installation, in case the scanning is still in progress.
8. Complete the ZfD 3.2 installation.
9. In Windows Explorer, right-click NTSCAN32.EXE in the PUBLIC\ZENWORKS directory > click Properties > the Security tab > Permissions.
10. Click Add > select Everyone > click Add.
11. In the Type of Access field, select Full Control > click OK.

    On Windows 2000 servers, select the Read/Execute option > click OK.
12. From the list, click Administrators > Remove > click OK twice.
13. In Windows Explorer, right-click WINSCAN.EXE in the PUBLIC\ZENWORKS directory > click Properties > the Security > Permissions.
14. Click Add > select Everyone > click Add.
15. In the Type of Access field, select Full Control > click OK.

    On Windows 2000 servers, select the Read/Execute option > click OK.
16. From the list, click Administrators > Remove > click OK twice.

Installing Workstation Inventory in an Existing ZENworks 2 Setup

If you are installing over an existing ZENworks 2 setup, follow these guidelines:

- If you are planning to install the ZfD Inventory database maintained in Sybase on a server, ensure that you shut down the existing Sybase database before running the ZfD installation program.
- If the installation program prompts you to choose either Upgrade or Full Install. Choose Full Install.

Configuring Servers for Workstation Inventory

The following table lists the actions that you should follow to setup the server for Workstation Inventory.

To set up this type of server:	Do this:
Standalone Server	1. Assign the role as Standalone Server during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168. 3. Follow the steps in "Configure the Policies for the Database" on page 166.
Root Server	1. Assign the role as Root Server during installation. 2. Follow the steps in "Configure the Policies for the Database" on page 166.
Root Server with Workstations	1. Assign the role as Root Server with Workstations during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168. 3. Follow the steps in "Configure the Policies for the Database" on page 166.
Intermediate Server	1. Assign the role as Intermediate Server during installation. 2. Follow the steps in "Configure the Roll-Up Policy" on page 167.
Intermediate Server with Database	1. Assign the role as Intermediate Server with Database during installation. 2. Follow the steps in "Configure the Roll-Up Policy" on page 167 3. Follow the steps in "Configure the Policies for the Database" on page 166.
Intermediate Server with Database & Workstations	1. Assign the role as Intermediate Server with Database & Workstations during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168 3. Follow the steps in "Configure the Roll-Up Policy" on page 167 4. Follow the steps in "Configure the Policies for the Database" on page 166.
Leaf Server with Database	1. Assign the role as Leaf Server with Database during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168 3. Follow the steps in "Configure the Roll-Up Policy" on page 167 4. Follow the steps in "Configure the Policies for the Database" on page 166.

To set up this type of server:	Do this:
Leaf Server	1. Assign the role as Leaf Server during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168. 3. Follow the steps in "Configure the Roll-Up Policy" on page 167
Intermediate Server with Workstations	1. Assign the role as Intermediate Server with Workstations during installation. 2. Follow the steps in "Configure the Inventory Policies for Workstations" on page 168. 3. Follow the steps in "Configure the Roll-Up Policy" on page 167.

Configuring Policies

After you install the Inventory components on servers and workstations, you must configure the server policies and workstation policies in ConsoleOne.

Create the appropriate policy packages, then configure the policies you need, enable them, and associate each package with a server or container. The following table is an overview of the packages, policies, and objects that you need to configure for Workstation Inventory:

Policy / Package / Objects	Description of the Configuration Settings
Server Package	Contains the Roll-Up policy to identify the next-level server.
Service Location Package	Contains the Database Location policy to associate the database.
Workstation Package	Contains the Workstation Inventory policy with the inventory scan settings.
Inventory Service object	Server object created in eDirectory with the following attributes: ZEN:INV-Host-Server, ZEN:INVRole, and ZEN:InvScan-File-Path.
Database object	Contains the configurable parameters for the database.
Workstation Inventory policy contained in the Workstation Package	Contains the inventory settings for the workstations.
Roll-Up policy contained in the Server Package	Contains the server settings for a roll-up of scan data.
Database Location policy contained in the Service Location policy	Contains the location of the database.

NOTE: If you have installed ZfD 3.2 on existing ZfD3/SP1 server, and you have chosen to retain configuration and policy settings, do not configure the policy settings.

Complete the steps in the following sections to configure the Workstation Inventory settings:

- "Configuring Servers for Workstation Inventory" on page 164
- "Configure the Roll-Up Policy" on page 167
- "Configure the Policies for the Database" on page 166
- "Configure the Inventory Policies for Workstations" on page 168

After completing these steps, you need to ensure that the database is up and running.

IMPORTANT: After installing and configuring Workstation Inventory, you must run the Inventory Services on the server. To run the Inventory Services on a NetWare server, enter **`startinv`**. On a Windows NT/2000 server, start the Inventory Service Manager (ZENworks Inventory Service).

Configure the Policies for the Database

The installation program creates the database object for Sybase and configures the database server.

To configure the Inventory database in Sybase:

1. In ConsoleOne, right-click the Policy Packages container > click New > Policy Package > Service Location Package > ZENworks Database > Next.
2. Type the name for the Service Location Package > click Next > click Finish.

   This procedure creates the Service Location package.
3. In ConsoleOne, right-click the Service Location Package > click Properties > click Policies.
4. Check the check box under the Enabled column for the ZENworks Database policy.
5. Click Properties.
6. Browse to the DN of the ZENworks Database object > click OK twice.
7. Click the Associations tab > Add.
8. Browse to select the container under which the Inventory Service object is present > click OK twice.

   The database settings for Sybase are:

   - **Driver:** *com.sybase.jdbc.SybDriver*
   - **Protocol:** *jdbc:*
   - **SubProtocol:** *sybase:*
   - **SubName:** *Tds:*
   - **Port:** *2639*
   - **SID Service Name:** Not applicable for Sybase

For an Oracle database, you must create the Database object and configure the object.

To configure the Inventory database in Oracle:

1. In ConsoleOne, right-click a location in the tree for the Database object > click New > Object > ZENworks Database > OK.
2. Type a name for the Database object > click OK.
3. Browse for the DN of the server or type the IP address of the server.

   For a NetWare 4.*x* server, specify the IP address.
4. In ConsoleOne, right-click the Database object > click Properties > ZENworks Database.
5. Type the values for the following options:

   - **Database (Read-Write) User Name:** *MW_DBA*
   - **Database (Read-Write) Password:** *novell*

6 In ConsoleOne, right-click the Database object > Properties > Jdbc Driver Information > Populate Fields with Default Values for an Oracle Database > Populate Now > OK.

The database settings for Oracle are:

- **Driver:** *oracle.jdbc.driver.OracleDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *oracle*:
- **SubName:** *thin:@*
- **Port:** *1521*
- **SID Service Name (Service ID of the Oracle database):** *orcl*

7 In ConsoleOne, right-click the Policy Packages container > click New > Policy Package > Service Location Package > ZENworks Database > Next.

8 Type the name for the Service Location Package > click Next > Finish.

9 In ConsoleOne, right-click the Service Location Package > click Properties > Policies.

10 Check the check box under the Enabled column for the ZENworks Database policy.

11 Click Properties.

12 Browse to the DN of the ZENworks Database object > click OK twice.

13 Click the Associations tab > Add.

14 Browse to select the container under which the Inventory Service object is present > click OK twice.

Configure the Roll-Up Policy

If there is a need for roll-up of scan data in your inventory setup, you can specify the details, such as the next-level server (DN of the Inventory Service object) for roll-up in the Roll-Up policy that is contained in the Server Package.

To configure the Roll-Up policy:

1 In ConsoleOne, right-click the Policy Packages container > click New > Policy Package > Server Package > zeininvRollUpPolicy > Next.

2 Type the name for the Server Package > click Next > click Finish.

3 In ConsoleOne, right-click the Server Package > click Properties > Policies. Click any of these: General, NetWare, or WinNT-2000.

4 Check the check box under the Enabled column for the zeninvRollup policy.

5 Click Properties.

6 Browse to select the DN of the Inventory Service object > click OK.

7 Click the Associations tab > Add.

The first time you enable the Roll-Up policy, you will prompted to associate the policy package. The policy you configured and enabled earlier will not be in effect until you associate this policy package with a server. Browse for the server that you want to associate the Roll-Up policy to > click OK twice.

8 In ConsoleOne, right-click the Server Package > click Properties > Policies. Click any of these: General, NetWare, or WinNT-2000.

9 Click the Roll-Up Policy row > Properties > Roll-Up Policy tab > Roll-Up Schedule. Modify the settings for scheduling the roll-up time > click OK.

When you schedule the roll-up of data in the Inventory policies, we recommend the roll-up frequency should be at least one day. It is likely that if the roll-up of scan data is scheduled too frequently, for example less than one hour, there may be some performance degradation of the Inventory server.

Configure the Inventory Policies for Workstations

In the Workstation Inventory policy, you configure the following settings for scanning workstations:

- Scanning time at the workstations
- Inventory server to which the workstations will send scan data
- Include software scanning of workstations
- List of software applications for scanning

To configure the Workstation Inventory policy:

1 In ConsoleOne, right-click the Policy Packages Container > click New > click Policy Package > Workstation Package > Workstation Inventory > Next.

2 Type the name for the Workstation Package > click Next > Finish.

3 In ConsoleOne, right-click the Workstation Package > click Properties > Policies > click any of these: Win95-98 or WinNT-2000.

4 Check the Workstation Inventory Policy > click OK.

5 Click the Associations tab > Add.

6 Browse to select the container object under which the workstations are registered > click OK twice.

7 In ConsoleOne, right-click the Workstation Package > click Properties > Policies > click any of these: Win95-98 or WinNT-2000.

8 Click the Workstation Inventory row > Properties > the Workstation Inventory Policy tab.

9 Browse to select the DN of the Inventory Service object.

10 Check the Enable the software scan option to include software scanning of workstations.

11 Click the Custom Scan Editor button to select the software that you want to scan for at the workstations > modify the list.

12 Click OK.

13 In ConsoleOne, right-click the Workstation Package > click Properties > Policies > click any of these: Win95-98 or WinNT-2000.

14 Click the Workstation Inventory Policy row > Properties > the Policy Schedule tab.

15 Modify the settings for scheduling the scan of the workstations > click OK twice.

16 In ConsoleOne, right-click the Inventory Service object (*servername*_ZenInvService) > click Properties > the Inventory Service object Properties tab.

17 Check Enable Scan of Workstations > click OK.

If you have configured the Inventory server that is a Windows NT/2000 server and there are Windows 95/98 workstations that will send their scan data to that Windows NT/2000 server, you must do the following for the scanners to collect data:

- If there are eDirectory users who are also Windows NT/2000 domain users, ensure that the users logged in are valid users of the Windows NT/2000 domain in the existing share created by ZfD.
- If there are users logged in to a different domain, ensure that the users are trusted users of the domain in the existing share created by ZfD.
- If there are eDirectory users who are not users of any Windows NT/2000 domain, ensure that the users do not log in to eDirectory during workstation startup. However, these users can log in to eDirectory later.

Configuring the Inventory Database for Oracle

The following sections explain how to configure the Inventory database for Oracle; in this setup, the Inventory database is not mounted with other Oracle databases.

- "Configuring the Inventory Database for Oracle on a NetWare Server" on page 169
- "Configuring the Inventory Database for Oracle on a Windows NT/2000 Server" on page 172
- "Loading the Inventory Database as a Separate Oracle Instance" on page 175
- "Loading the Oracle Database on a NetWare Server" on page 183
- "Loading the Oracle Database on a Windows NT/2000 Server" on page 183

To use ZfD 3.2 Inventory Database on Oracle 8i for Linux and Solaris, see Using the ZfD 3.2 Inventory Database on Oracle 8i for Linux and Solaris in Workstation Inventory in *Administration.*

To upgrade the ZfD 3.2 Inventory Database on Oracle 8.1.*x*, see Upgrading the ZfD 3.2 Inventory Database on Oracle 8.1.x in Workstation Inventory in *Administration.*

Configuring the Inventory Database for Oracle on a NetWare Server

You must manually install the Inventory database for Oracle on NetWare servers.

Prerequisites for configuring the database include the following:

- Oracle 8i (8.1.5.0.4) Enterprise Edition on NetWare must be installed on the server before configuring the Inventory database.
- Workstation Inventory requires that you have a minimum of five user licenses.
- Oracle files should not be installed on an NFS-mounted volume on the file server.
- Oracle data files must reside on volumes that have block suballocation turned off.

To configure the database:

1. Extract the INVORACLE8INW.ZIP file from the \ZENWORKS\PRODUCTS\DATABASE\ORACLE directory in the ZfD 3.2 *Program* CD to any volume other than SYS: on the NetWare server.

   After extraction, you will see the following list of system files and Database Space files in this directory.

Filenames	Contents Description
CIM1.ORA, CIM2.ORA, CIM3.ORA, CIM4.ORA, CIM5.ORA, CIM6.ORA, CIM7.ORA, CIM8.ORA, and CIM9.ORA	Table spaces that contain the inventory information for ZfD
CTL1.ORA	Oracle control file
INIT.ORA	Database startup file
LOG1.ORA, LOG2.ORA	Online Redo log file
RBS1.ORA	Rollback segment file containing table space for rollback
SYS1.ORA	SYS schema file containing the data dictionary
TMP1.ORA	Temporary table space
_DBINT.SQL	Contains the Inventory database site name
_START.SQL	Contains the location of the database startup file
ALTERCTRL.SQL	Contains the location of table spaces
MGMTDBO.NCF	ZfD Inventory database startup file for Oracle on NetWare
\TRACE*oracle_log_files*	Contains the Oracle log files

2. Copy the MGMTDBO.NCF file from *volume*\ZFD3\ORACLE to the SYS:\SYSTEM directory on the database server.

   where *volume* is the volume on which the .ZIP file was extracted.

3. Specify the site details of the database.

   3a. Copy the _DBINIT.SQL file from *volume*\ZFD3\ORACLE to the SYS:\SYSTEM directory on the database server.

   where *volume* is the volume on which the .ZIP file was extracted.

   3b. Edit the following lines in the _DBINIT.SQL file to specify the site ID and site name for the database:

   ```
   siteid:=site_ID;
   ```

   ```
   siteName:='site_name';
   ```

   where *site_ID* uniquely identifies the database and '*site_name*' provides a description for the database site.

   If you do not specify the site ID, the default values specified in the file apply.

   3c. Save the changes you make.

4. Create the Oracle Control file.

   4a. Edit the ALTERCTRL.SQL file located in *volume*\ZFD3\ORACLE to specify the path to which you have extracted the .ZIP file.

where *volume* is the volume on which the .ZIP file was extracted.

For example, modify the existing DATA:\ZFD3\ORACLE\DATABASE path to ORACLE:\ZFD3\ORACLE\DATABASE in ALTERCTRL.SQL.

In this .SQL file, modify the path for these parameters, if required.

```
startup nomount pfile=oracle:\zfd3\oracle\database\INIT.ORA

logfile group 1 'oracle:\zfd3\oracle\database\log1.ora' size 256K,

logfile group 2 'oracle:\zfd3\oracle\database\log2.ora' size 256K

datafile 'oracle:\zfd3\oracle\database\sys1.ora',

'oracle:\zfd3\oracle\database\rbs1.ora',

'oracle:\zfd3\oracle\database\cim1.ora',

'oracle:\zfd3\oracle\database\cim2.ora',

'oracle:\zfd3\oracle\database\cim3.ora',

'oracle:\zfd3\oracle\database\cim4.ora',

'oracle:\zfd3\oracle\database\cim5.ora',

'oracle:\zfd3\oracle\database\cim6.ora',

'oracle:\zfd3\oracle\database\cim7.ora',

'oracle:\zfd3\oracle\database\cim8.ora',

'oracle:\zfd3\oracle\database\cim9.ora',

'oracle:\zfd3\oracle\database\tmp1.ora'
```

4b Save the changes.

4c Edit the INIT.ORA file located in *volume*\ZFD3\ORACLE\DATABASE to specify the path to which you have extracted the .ZIP file.

where *volume* is the volume on which the .ZIP file was extracted.

Modify the path for the following parameters:

```
control_files=location_of_CTLl.ORA\CTL1.ORA

background_dump_dest=location_of_TRACE_dir\TRACE

user_dump_dest=location_of_TRACE_dir\TRACE
```

4d Save the changes.

4e To load Oracle, enter **`oraload`**.

4f To load the Oracle Server Manager, enter **`svrmgr31`**.

Connect as an administrator. For example, if the administrator's internal name is *internal*, enter `connect internal/password_for_administrator` at the Server Manager prompt.

5 Enter **`shutdown normal`**.

6 At the Server Manager prompt, enter **`@complete_path_of_alterctrl.sql\alterctrl`**.

You should see the window, which indicates that the database is mounted and loaded.

7 To exit the Server Manager, enter **exit**.

8 Copy *volume*\ZFD3\ORACLE_START.SQL to SYS:\SYSTEM directory on the database server.

where *volume* is the volume on which the .ZIP file was extracted.

8a Edit the _START.SQL file to specify the location of the INIT.ORA file in the following parameter.

```
startup pfile=location_of_the_INIT.ORA\INIT.ORA
```

9 Load the Inventory database. At the database server console, enter **mgmtdbo** > type the password for the Database Administrator (DBA).

10 Initialize the database.

10a To load the Oracle Server Manager, enter **svrmgr31**.

To connect to the database, at the Server Manager prompt, enter **connect mw_dba/ novell.**

10b At the Server Manager prompt, enter **@sys:\system_dbinit.sql.** This command initializes the database.

10c To verify that the initialization was successful: at the Server Manager prompt, enter **select getsiteid() from dual;** to display the site ID of the database. To display the site name of the database, enter **select * from zenworks.site;**

10d At the Server Manager prompt, enter **disconnect.**

10e To exit the Server Manager, enter **exit.**

Configuring the Inventory Database for Oracle on a Windows NT/2000 Server

You must manually install the Inventory database for Oracle on Windows NT/2000 servers.

Prerequisites for configuring the database include the following:

- Oracle 8i Enterprise Edition must be installed on the server before configuring the Inventory database.
- To maintain the Inventory database in Oracle, Workstation Inventory requires that you have a minimum of five user licenses.

To configure the database:

1 Extract the INVORACLE8INT.ZIP file from the \ZENWORKS\PRODUCTS\DATABASE\ORACLE directory located in the ZfD 3.2 *Program* CD to a drive, which preferably has NTFS.

After extraction, you will see the following list of system files and Database Space files in this directory:

Filenames/Directory	Contents Description
CIM1.ORA, CIM2.ORA, CIM3.ORA, CIM4.ORA, CIM5.ORA, CIM6.ORA, CIM7.ORA, CIM8.ORA, and CIM9.ORA	Table spaces that contain the inventory information for ZfD
CTL1.ORA	Oracle control file

Filenames/Directory	Contents Description
INIT.ORA	Database startup file
LOG1.ORA, LOG2.ORA	Online Redo log file
RBS1.ORA	Rollback segment file containing table space for rollback
SYS1.ORA	SYS schema file containing the data dictionary
TMP1.ORA	Temporary table space
_DBINT.SQL	Contains the Inventory database site name
_START.SQL	Contains the location of the database startup file
ALTERCTRL.SQL	Contains the location of table spaces
MGMTDBO.BAT	ZfD Inventory database startup file for Oracle on Windows NT/2000
\TRACE*oracle_log_files*	Contains the Oracle log files

2 Specify the site details of the database.

2a Edit the following lines in the _DBINIT.SQL file to specify the site ID and site name for the database.

```
siteid:=site_ID;
siteName:='site_name';
```

where *site_ID* uniquely identifies the database, and *'site_name*' provides a description for the database site.

If you do not specify a site ID, the default values specified in the file apply.

2b Save the changes you make.

3 Create the Oracle Control file.

3a Edit the ALTERCTRL.SQL located in *drive*\ZFD3\ORACLE to specify the path strings to which you have extracted the file.

where *drive* is the drive on which the .ZIP file was extracted.

For example, modify the existing *D:\ZFD3\ORACLE\DATABASE* path to *C:\ZFD3\ORACLE\DATABASE* in ALTERCTRL.SQL.

In this .SQL file, modify the path for these parameters, if required.

```
startup nomount pfile=c:\zfd3\oracle\database\INIT.ORA
logfile group 1 'c:\zfd3\oracle\database\log1.ora' size 256K,
logfile group 2 'c:\zfd3\oracle\database\log2.ora' size 256K
datafile
'c:\zfd3\oracle\database\sys1.ora',
'c:\zfd3\oracle\database\rbs1.ora',
'c:\zfd3\oracle\database\cim1.ora',
```

'c:\zfd3\oracle\database\cim2.ora',

'c:\zfd3\oracle\database\cim3.ora',

'c:\zfd3\oracle\database\cim4.ora',

'c:\zfd3\oracle\database\cim5.ora',

'c:\zfd3\oracle\database\cim6.ora',

'c:\zfd3\oracle\database\cim7.ora',

'c:\zfd3\oracle\database\cim8.ora',

'c:\zfd3\oracle\database\cim9.ora',

'c:\zfd3\oracle\database\tmp1.ora'

3b Save the changes.

3c Edit the INIT.ORA located in *drive*\ZFD3\ORACLE\DATABASE.

where *drive* is the drive on which the .ZIP file was extracted.

Modify the path for the following parameters:

`control_files=`*`location_of_CTL`*`l.ORA\CTL1.ORA`

`background_dump_dest=`*`location_of_TRACE_dir`*`\TRACE`

`user_dump_dest=`*`location_of_TRACE_dir`*`\TRACE`

3d Save the changes.

3e Ensure that Oracle is loaded on the database server.

3f Load the Oracle Server Manager, click Start from the Windows taskbar > Run > enter **`svrmgrl.`**

Connect as an administrator. For example, if the administrator's internal name is *internal*, at the Server Manager prompt, enter **`connect internal/`** ***`password_for_administrator.`***

3g Enter **`shutdown normal`**.

3h At the Server Manager prompt, enter **`@complete_path_of_alterctrl.sql\alterctrl.`**

You should see the window, which indicates that the database is mounted and loaded.

3i To exit the Server Manager, enter **`exit`**.

4 Copy *drive*\ZFD3\ORACLE_START.SQL to the \ZFD3\ORACLE on the database server. where *drive* is the drive on which the .ZIP file was extracted.

4a Edit the _START.SQL file to specify the location of the INIT.ORA file in the following parameter.

`startup pfile=`*`location_of_INIT.ORA\INIT.ORA`*

5 Load the Inventory database: At the database server from the path where the MGMTDBO.BAT is located, enter **`mgmtdbo.`**

6 Type the password for the Database Administrator (DBA).

7 Initialize the database.

7a To load the Oracle Server Manager, enter **`svrmgrl`**. To connect to the database, enter **`connect mw_dba/novell`** *at the Server Manager prompt.*

7b To initialize the database, enter **`@complete_location_of_dbinit.sql\dbinit.sql at the Server Manager prompt`**

7c To verify that the initialization was successful, enter **`select getsiteid() from dual;`** at the Server Manager prompt.

To display the site ID of the database, enter **`select * from zenworks.site`** to display the site name of the database.

7d At the Server Manager prompt, enter **`disconnect`**.

7e To exit the Server Manager, enter **`exit`**.

Loading the Inventory Database as a Separate Oracle Instance

The following sections explain the steps for configuring and running multiple Oracle* 8i database instances:

- "Configuring and Running Multiple Oracle Database Instances on a NetWare 5.x Server" on page 175
- "Configuring and Running Multiple Oracle Database Instances on a Windows NT/2000 Server" on page 179

Configuring and Running Multiple Oracle Database Instances on a NetWare 5.*x* Server

Prerequisites for configuring the database include the following:

- Oracle 8i (8.1.5.0.4) or later Enterprise Edition on a NetWare 5.*x* server must be installed on the server before configuring the Inventory database.
- Workstation Inventory requires that you have a minimum of five user licenses.
- You have already installed ZfD 3.2 Workstation Inventory. For more information, see Workstation Inventory in *Getting Started*.

To configure and run multiple Oracle database instances:

1. Unload Oracle. At the database server prompt, enter **`oraunld`**.
2. Invoke the Net8 configuration utility. At the database server prompt, run `easycfg.ncf` to load the Net8 Easy configuration window.
3. Define a unique Oracle instance.
   - **3a** Click Config > Listener > Database > Add.
   - **3b** Assign values for Database Instance and Database Name in the Adding Instances Address window.

     For example, assign Database Instance=*zfd3 and Database Name=mgmtdb*. In this configuration, the database instance is zfd3. You can specify any database instance name. The Database Domain field should be left blank.
   - **3c** Click Accept > Save.
4. Configure the Listener for IPC. To run an Oracle system, the IPC and TCP addresses should be already be configured.

4a Click Config > Listener > Address. Ensure that IPC and TCP addresses are configured for the server.

The setting for IPC is *servername*_LSNR, and TCP is *IPaddress or hostname*. If these settings exist, click Cancel. Otherwise, assign the values for these settings > click Save.

5 Create an IPC alias.

5a Click Config > Database Alias. The window will list the aliases for IPC, SPX, TCP, and others. Click Add to add an alias name for the new instance.

Enter the following details:

- **Database Alias:** *servername-databaseinstance-IPC*. For example, the database alias is *austr*, where *austr* is the servername, *zfd3* is the database instance created earlier.
- **Protocol:** *IPC*
- **Service/Host Name or Key Name:** *server_name_LSNR*
- **Database Instance:** *zfd3*

5b Click Accept > Save.

5c To verify the configured alias name in the list window: Click Config > Database Alias > select the newly created alias > click View.

View the properties of the database alias. Ensure that the properties are correct.If the property settings are incorrect, delete the alias (click Delete) and repeat the step 5.

6 Exit the EasyCfg tool. Click Config > Exit.

7 Create a password file for logging as *Internal* user for this instance. Enter **`load orapwd81 file=`*`oracle_volume:oracle_home\database\pwddatabase_instance.ora`*` password=password entries=2`** where *oracle_volume* is the NetWare volume name of your Oracle installation, *PWDdatabase_instance*.ORA is the password file name, and *password* is any password that you specify.

For example, `load orapwd81 file=oracle:\orahome1\database\pwdzfd3.ora password=`*`mgmtdb`* `entries=2.` This password file will be created in the *oracle_volume:*\DATABASE directory. Ensure that the file exists in the directory.

8 Load the Oracle NLM™ software. At the database server prompt, enter **`oraload`**.

9 To set the newly created ZfD instance, load the Oracle Server Manager. At the database server prompt, enter **`svrmgr31`**.

10 Enter the following commands: **`set instance servername-`*`databaseinstance`***. For example, `set instance` *`austr-zfd3-ipc.`* This displays that the newly created ZfD3 instance is started.

11 Enter **`connect internal/`*`password`*** where *password* is the password created in Step 7 on page 176.

12 Mount the Inventory database. Extract the INVORACLE8INW.ZIP file from the \ZENWORKS\PRODUCTS\DATABASE\ORACLE directory in the ZfD 3.2 *Program* CD to any volume other than SYS: on the NetWare server. After extraction, you will see the following list of system files and Database Space files in this directory.

Filenames	Contents Description
CIM1.ORA, CIM2.ORA, CIM3.ORA, CIM4.ORA, CIM5.ORA, CIM6.ORA, CIM7.ORA, CIM8.ORA, and CIM9.ORA	Table spaces that contain the inventory information for ZfD
CTL1.ORA	Oracle control file
INIT.ORA	Database startup file
LOG1.ORA, LOG2.ORA	Online Redo log file
RBS1.ORA	Rollback segment file containing table space for rollback
SYS1.ORA	SYS schema file containing the data dictionary
TMP1.ORA	Temporary table space
_DBINT.SQL	Contains the Inventory database site name
_START.SQL	Contains the location of the database startup file
ALTERCTRL.SQL	Contains the location of table spaces
MGMTDBO.NCF	ZENworks Inventory database startup file for Oracle on NetWare
\TRACE*oracle_log_files*	Contains the Oracle log files

13 Copy the MGMTDBO.NCF file from *volume*\ZFD3\ORACLE to the SYS:\SYSTEM directory on the database server, where *volume* is the volume on which the .ZIP file was extracted.

14 Specify the site details of the database. Copy the _DBINIT.SQL file from *volume*\ZFD3\ORACLE to the SYS:\SYSTEM directory on the database server, where *volume* is the volume on which the .ZIP file was extracted.

15 Edit the following lines in the _DBINIT.SQL file to specify the site ID and site name for the database:

```
siteid:=site_ID;

sitename:='site_name';
```

where *site_ID* uniquely identifies the database and '*site_name*' provides a description for the database site. If you do not specify the site ID, the default values specified in the file apply. Save the changes you make.

16 Create the Oracle Control file. Edit the ALTERCTRL.SQL file located in *volume*\ZFD3\ORACLE to specify the path to which you have extracted the .ZIP file, where *volume* is the volume on which the .ZIP file was extracted. For example, modify the existing DATA:\ZFD3\ORACLE\DATABASE path to ORACLE:\ZFD3\ORACLE\DATABASE in ALTERCTRL.SQL. In this .SQL file, modify the path for these parameters, if required.

```
startup nomount pfile=oracle:\zfd3\oracle\database\INIT.ORA

logfile group 1 'oracle:\zfd3\oracle\database\log1.ora' size 256K,

logfile group 2 'oracle:\zfd3\oracle\database\log2.ora' size 256K,
```

```
datafile'oracle:\zfd3\oracle\database\sys1.ora'
'oracle:\zfd3\oracle\database\rbs1.ora';
'oracle:\zfd3\oracle\database\cim1.ora';
'oracle:\zfd3\oracle\database\cim2.ora';
'oracle:\zfd3\oracle\database\cim3.ora';
'oracle:\zfd3\oracle\database\cim4.ora';
'oracle:\zfd3\oracle\database\cim5.ora';
'oracle:\zfd3\oracle\database\cim6.ora';
'oracle:\zfd3\oracle\database\cim7.ora';
'oracle:\zfd3\oracle\database\cim8.ora';
'oracle:\zfd3\oracle\database\cim9.ora';
'oracle:\zfd3\oracle\database\tmp1.ora';
```

17 Save the changes.

18 Edit the INIT.ORA file located in *volume*\ZFD3\ORACLE\DATABASE to specify the path to which you have extracted the .ZIP file.

where *volume* is the volume on which the .ZIP file was extracted.

Modify the path for the following parameters:

```
control_files=location_of_CTL1.ORA\CTL1.ORA
background_dump_dest=location_of_TRACE_dir\TRACE
user_dump_dest=location_of_TRACE_dir\TRACE
```

Save the changes.

At the Server Manager prompt, enter **`@complete_path_of_alterctrl.sql\alterctrl`**

You should see the window, which indicates that the database is mounted and loaded.

Exit the Server Manager. Enter **`exit`**.

19 Modify the _START.SQL file located in SYS:\SYSTEM. Enter the following lines in the file:

```
set instance servername-databaseinstance-IPC
shutdown normal
```

20 Create the Database object. In ConsoleOne, right-click a location in the tree for the Database object > click New > Object > ZENworks Database > OK.

21 Type a name for the Database object > click OK

22 Configure the Database Server options of the Database object. In ConsoleOne, right-click the Database object > click Properties > click ZENworks Database.

23 Browse for the DN of the server or type the IP address of the server.

24 Type the values for the following options:

- **Database (Read-Write) User Name:** *MW_DBA*
- **Database (Read-Write) Password:** *novell*

25 Click OK.

26 Ensure that the JDBC Driver properties are correct for your database configuration. In ConsoleOne, right-click the Database object > click Properties > Jdbc Driver Information > Populate Fields with Default Values for an Oracle Database > Populate Now.

The database settings for Oracle are:

- **Driver:** *oracle.jdbc.driver.OracleDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *oracle*:
- **SubName:** *thin:@*
- **Port:** *1521*
- **SID Service Name (Service ID of the Oracle database):** *orcl*. The value for the SID is the same as assigned for the Database Instance. See Step 5 on page 176.

27 Click OK.

28 At the database server prompt, enter **`mgmtdbo`** > enter the password created in Step 7 on page 176.

29 Start other Oracle database instances. Run the Oracle Server Manager, set the applications instance, and mount the database.

If you are loading multiple databases in separate Oracle instances, then each database reserves a separate Oracle SGA memory, where Oracle keeps all the database resources. In such environments, you should increase the amount of memory on the server. Refer to the documentation provided by Oracle.

Configuring and Running Multiple Oracle Database Instances on a Windows NT/2000 Server

Prerequisites for configuring the database include the following:

- Oracle 8i (8.1.5.0.4) Enterprise Edition must be installed on the Windows NT/2000 server before configuring the Inventory database.
- To maintain the Inventory database in Oracle, Workstation Inventory requires that you have a minimum of five user licenses.
- You have already installed ZfD 3.2 Workstation Inventory. For more information, see Workstation Inventory in *Getting Started*.

To configure and run Oracle instances:

1 At the database server, run the Oracle Database Configuration Assistant. From the desktop Start menu, click Programs > Oracle > Database Administration > Oracle Database Configuration Assistant.

2 Click Create a Database > Next > Typical > Next > Copy Existing Database Files from the CD > Next.

3 Enter the following details:

- **Global Database Alias:** `mgmtdb.`*your_windows_nt/2000_name*
- **SID:** The value is automatically filled as *mgmtdb*.

4 Click Finish.

This allows for Oracle database creation. This process takes a significant amount of time. Ensure that the OracleServiceMGMTDB service is created and started.

5 Load the Inventory database.

Run the Oracle Server Manager. From the desktop menu, click Start > Run > SVRMGRL. Enter the following commands:

```
set instance mgmtdb
connect internal/password_for_administrator
```

6 Mount the Inventory database.

Extract the INVORACLE8INT.ZIP file from the \ZENWORKS\PRODUCTS\DATABASE\ORACLE directory located in the ZfD 3.2 *Program* CD to a drive, which preferably has NTFS.

After extraction, you will see the following list of system files and Database Space files in this directory:

Filenames/Directory	Contents Description
CIM1.ORA, CIM2.ORA, CIM3.ORA, CIM4.ORA, CIM5.ORA, CIM6.ORA, CIM7.ORA, CIM8.ORA, and CIM9.ORA	Table spaces that contain the inventory information for ZfD
CTL1.ORA	Oracle control file
INIT.ORA	Database startup file
LOG1.ORA, LOG2.ORA	Online Redo log file
RBS1.ORA	Rollback segment file containing table space for rollback
SYS1.ORA	SYS schema file containing the data dictionary
TMP1.ORA	Temporary table space
_DBINT.SQL	Contains the Inventory database site name
_START.SQL	Contains the location of the database startup file
ALTERCTRL.SQL	Contains the location of table spaces
MGMTDBO.BAT	ZENworks Inventory database startup file for Oracle on Windows NT/2000
\TRACE*oracle_log_files*	Contains the Oracle log files

7 Specify the site details of the database.

8 Edit the following lines in the _DBINIT.SQL file to specify the site ID and site name for the database.

```
siteid:=site_ID;
sitename:='site_name';
```

where *site_ID* uniquely identifies the database, and *'site_name'* provides a description for the database site. If you do not specify a site ID, the default values specified in the file apply.

9. Save the changes you make.
10. Create the Oracle Control file.
11. Edit the ALTERCTRL.SQL file located in *drive*\ZFD3\ORACLE to specify the path strings to which you have extracted the file, where *drive* is the drive on which the .ZIP file was extracted.

    For example, modify the existing *D:\ZFD3\ORACLE\DATABASE* path to *C:\ZFD3\ORACLE\DATABASE* in ALTERCTRL.SQL.
12. In this .SQL file, modify the path for these parameters, if required.

```
startup nomount pfile=c:\zfd3\oracle\database\INIT.ORA

logfile group 1 'c:\zfd3\oracle\database\log1.ora' size 256K,

logfile group 2 'c:\zfd3\oracle\database\log2.ora' size 256K datafile

'c:\zfd3\oracle\database\sys1.ora',

'c:\zfd3\oracle\database\rbs1.ora',

'c:\zfd3\oracle\database\cim1.ora',

'c:\zfd3\oracle\database\cim2.ora',

'c:\zfd3\oracle\database\cim3.ora',

'c:\zfd3\oracle\database\cim4.ora',

'c:\zfd3\oracle\database\cim5.ora',

'c:\zfd3\oracle\database\cim6.ora',

'c:\zfd3\oracle\database\cim7.ora',

'c:\zfd3\oracle\database\cim8.ora',

'c:\zfd3\oracle\database\cim9.ora',

'c:\zfd3\oracle\database\tmp1.ora',
```

13. Save the changes.
14. Edit the INIT.ORA located in *drive*\ZFD3\ORACLE\DATABASE, where *drive* is the drive on which the .ZIP file was extracted.
15. Modify the path for the following parameters:

```
control_files=location_of_CTLl.ORA\CTL1.ORA

background_dump_dest=location_of_TRACE_dir\TRACE

user_dump_dest=location_of_TRACE_dir\TRACE
```

16. Save the changes.
17. Ensure that Oracle is loaded on the database server.
18. Load the Oracle Server Manager. Click Start from the Windows taskbar > Run > enter **`svrmgrl`**.
19. Connect as an administrator. For example, if the administrator's internal name is *internal*, enter **`connect internal/`*`password_for_administrator`*** *at the Server Manager prompt.*
20. Enter **`shutdown normal`**.

At the Server Manager prompt, enter
@complete_path_of_alterctrl.sql\alterctrl.

You should see the window that indicates that the database is mounted and loaded.

Enter **exit** to exit the Server Manager.

21. Copy *drive*\ZFD3\ORACLE_START.SQL to the \ZFD3\ORACLE directory on the database server, where *drive* is the drive on which the .ZIP file was extracted. Modify the _START.SQL file. Enter the following line in the file:

```
set instance mgmtdb

shutdown normal
```

22. Modify the properties of the database object. Create the Database object. In ConsoleOne, right-click a location in the tree for the Database object > click New > Object > ZENworks Database > OK.
23. Type a name for the Database object > click OK.
24. In ConsoleOne, right-click the Database object > click Properties > ZENworks Database.
25. Browse for the DN of the server or type the IP address of the server.
26. Type the values for the following options:
    - **Database (Read-Write) User Name:** *MW_DBA*
    - **Database (Read-Write) Password:** *novell*
27. Click OK.
28. Ensure that the JDBC Driver properties are correct as per your database configuration. In ConsoleOne, right-click the Database object > click Properties > Jdbc Driver Information > Populate Fields with Default Values for an Oracle Database > click Populate Now.

    The database settings for Oracle are:
    - **Driver:** *oracle.jdbc.driver.OracleDriver*
    - **Protocol:** *jdbc:*
    - **SubProtocol:** *oracle*:
    - **SubName:** *thin:@*
    - **Port:** *1521*
    - **SID Service Name (Service ID of the Oracle database):** *mgmtdb*. The value for the SID is the same as assigned for the Database Instance. See Step 5 on page 176.
29. At the database server console, from the path where the MGMTDBO.BAT(\ZFD3\ORACLE) is located, enter **mgmtdbo** > enter the password for the Database Administrator (DBA).
30. Start other Oracle database instances. Run the Oracle Server Manager, set the applications instance, and mount the database.

If you are loading multiple databases in separate Oracle instances, then each database reserves a separate Oracle SGA memory, where Oracle keeps all the database resources. In such environments, you should increase the amount of memory on the server. Refer to the documentation provided by Oracle.

Loading the Oracle Database on a NetWare Server

On NetWare servers, the MGMTDBO.NCF file in the SYS:\SYSTEM directory loads the Inventory database, MGMTDB (db_name), which is maintained in Oracle.

To load the database:

1. Enter **mgmtdbo**, at the server console > type the password for the Database Administrator (DBA).

Loading the Oracle Database on a Windows NT/2000 Server

To load the Inventory database, MGMTDB (db_name) on a Windows NT/2000 server:

1. Enter **mgmtdbo** at the database server console, from the path where the MGMTDBO.BAT(\ZFD3\ORACLE) is located > enter the password for the Database Administrator (DBA).

Deploying ZfD in Novell Cluster Services

To use ZfD with Novell Cluster Services, ZfD should be installed on all cluster nodes. After installation, ZfD should be configured for the cluster environment.

The following sections cover:

- "Cluster Terminology" on page 183
- "Setting Up Inventory in Novell Cluster Services" on page 183

Cluster Terminology

This document uses the following terms:

- Virtual server (Shared disk system)

  A virtual server is a cluster-enabled server.

- Cluster volume

  A cluster volume resides on a virtual server which is connected to and accessible from all servers in the cluster.

- Cluster node

  A cluster node is a server that is running Novell Cluster Services and is a member of an existing cluster.

For more information about Novell Cluster Services, see the Novell Cluster Services documentation (http://www.novell.com/documentation).

Setting Up Inventory in Novell Cluster Services

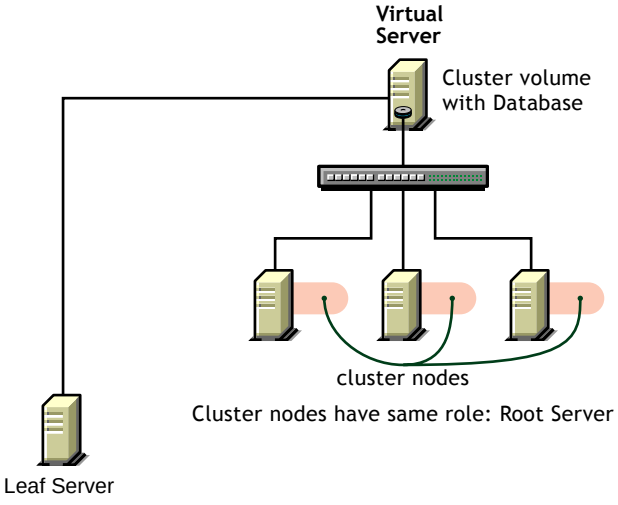
To set up Inventory:

1. Ensure that the installation prerequisites are met.

   For more information, see Installation Prerequisites in Integrating ZfD 3.2 or ZfD 3.2 SP1 with Novell Cluster Services in *Administration*.

2 Run the ZfD installation program.

During the installation, ensure that you specify the same role for all cluster nodes. For example, in one of the ZfD deployment scenarios, ZfD Inventory is installed on all cluster nodes. All cluster nodes have the same Inventory role. In the following illustration, at the topmost level, all the cluster nodes are Root Servers.



For more information, see Installing ZfD Components in the Cluster in Integrating ZfD 3.2 or ZfD 3.2 SP1 with Novell Cluster Services in *Administration*.

NOTE: In roll-up scenarios, servers in a non-cluster setup can roll up inventory data to servers in a cluster.

3 Configure Inventory on the cluster nodes.

For more information, see Configuring ZfD Components after Installing Clustering Services in Integrating ZfD 3.2 or ZfD 3.2 SP1 with Novell Cluster Services in *Administration*.

Migrating Workstation Inventory from ZENworks 2

To gain the maximum benefit of an enterprise-wide inventory solution, you need to plan for migrating the inventory information for the workstations in ZENworks 2 to ZfD 3.2.

ZfD 3.2 allows migration of inventory policies associated with a ZENworks 2 inventory server. When you migrate the inventory policy, the inventory information of the workstations associated with the inventory server will be added in ZfD 3.2. Also, all components on a particular server and all workstations associated to the server are migrated together. When policies are migrated to ZfD 3.2, there is some additional configuration needed for ZfD 3.2. For example, the SCANDIR path must be set in ZfD 3.2 because this path setting did not exist in ZENworks 2. Besides policies, you must also migrate the ZENworks 2 Inventory database to ZfD 3.2.

As a guideline, always plan and phase the migration.

Follow this procedure to migrate:

1. Create a deployment plan for ZfD 3.2 assuming there is no ZENworks 2 in the network.

   See “Deploying Inventory over a WAN Environment” on page 146 for more information.

Optimize on the number of databases and routes for inventory flow without any consideration of the current ZENworks 2 deployment.

2. Create a phased migration plan.

   Identify the sites and servers to move at the same time.

   It is much easier to migrate a single ZENworks 2 database and all servers and sites connected the database at the same time.

   If a database server and all servers and sites cannot be moved at the same time, use another server temporarily on the ZfD 3.2 site for the database to ease the migration. This server should have the appropriate role such as Intermediate Server or Root Server, as determined by the needs of ZfD 3.2.

   If an alternative server is not available, consider sending the inventory data from the servers at the lower level of the hierarchy directly to the next level during migration. If this is not feasible, another approach is to not to scan some of the workstations that are still on the ZENworks 2 tree during migration. This can be an acceptable solution because it should be possible to migrate all the servers and workstations served by a single database server during the course of two or three days, and it may not be an issue if some workstations are not scanned for that period.

   If you use the option of migrating the ZENworks 2 database server to ZfD 3.2, migrate as many inventory servers simultaneously as possible. The other servers will wait and get errors connecting to the database for a few days until they are migrated. The ZENworks 2 Inventory policy for those servers can be disabled until they are also migrated.

3. Migrate the ZENworks databases to the database at the Root Sever of ZfD 3.2.

   All databases in ZENworks 2 can be migrated one after the other to a database at the Root Server in ZfD 3.2. There is no need to migrate the ZENworks 2 data to an intermediate database and then build ZfD 3.2 data.

   In evaluating the need for intermediate database, consider the power and deployment of ZfD 3.2. Fewer databases should suffice in ZfD 3.2 than were used in ZENworks 2.

4. Migrate the policies.

   The most important policy to migrate is the Inventory policy applicable to the workstations. Use the Migration tool to migrate the old data and provide the new data, such as the SCANDIR path so the migrated policy will work in a ZfD 3.2 environment.

   If you want to use the ZENworks 2 setup after you have done a partial or incremental deployment and have a combination of ZENworks 2 and ZfD 3.2 servers, you must associate the ZENworks 2 container package (with the Search Policy enabled) to the container or the containers with the user and workstation objects. This is required because the schema is extended for ZfD 3.2 if it is installed in the same tree.

5. Create ZfD 3.2 policies.

   Create all additional ZfD 3.2 policies and setups according to the ZfD 3.2 deployment plan.

A Documentation Updates

This section lists updates to the *Deployment* guide that have been made since the initial release of Novell® ZENworks® for Desktops 3.2. The information will help you to keep current on documentation updates and, in some cases, software updates (such as a Support Pack release).

The information is grouped according to the date when the *Deployment* guide was updated and republished:

- October 31, 2002 (ZfD 3.2 Support Pack 1)

October 31, 2002 (ZfD 3.2 Support Pack 1)

Location	Update
"ZfD 3.2 Support Pack 1" on page 25	Added this new section to provide references for more information about installing, setting up, and using ZENworks for Desktops Support Pack 1.
"What's New in ZfD 3.2 Support Pack 1" on page 141	Added this new section to accommodate a list of changes included in the Workstation Inventory portion of ZENworks for Desktops 3.2 Support Pack 1.