CHAPTER 3

Setting up ZENworks in Your Tree

This chapter provides a quick overview of the ZENworks system and a high-level view of the changes that will occur within your tree. Make sure you understand this system and how it will impact your current Novell Directory Services installations. Other chapters will get into the details of installation and feature execution.

General ZENworks Architecture

Novell ZENworks requires some changes to your tree structure in addition to extensions to the Novell Administrator (NWAdmin). Additionally, a new client needs to be placed on the workstation with the addition of some agents. This section details the changes that need to occur for you to implement ZENworks into your tree.

Objects in NDS and Impact on the Tree

When you install ZENworks into your tree, not only does it copy the executable files necessary to run the software, it also extends the schema in your tree. The schema extension in your tree introduces several new objects and attributes to your system. Each object is discussed in detail in future chapters.

- *Policy Package Object.* The Policy Package Object is created to hold policies that affect behavior of the agents and programs associated with ZENworks. The ZENworks system looks for these policies when dealing with both users and workstations. A Policy Package Object can be created for each of the supported workstation systems (Windows 3.1, Windows 95/98, Windows NT) and each of the user types (Windows 3.1 User, Windows 95/98 User, Windows NT User), along with miscellaneous collections of policies in a Container Policy.
- *Workstation Object.* This object is created when you import workstations into your tree. This object holds information about the workstation, such as its network addresses and inventory information.
- *Workstation Group Object.* This object is a new group object that enables you to group a set of workstations together. Once the workstations are identified in the group object, you can apply rights and associations to the group just as you do with user groups today.

- *Cookie Attribute on Container Object.* This attribute is used in the process of registering the workstation to the tree. The first time a user logs in to a workstation, the agents register information into the container of the user object. This registration information is placed in this attribute. Additionally, when you import the workstation, this attribute is modified with the DN of the created workstation. The next time someone logs in to the workstation (after your import) the workstation discovers its DN by looking into this attribute, where it originally registered.
- *Associated Workstations on User Object.* This simply keeps track of the workstations that a user registered with NDS by being the first user to log into the tree through that workstation.

The introduction of most of these objects to the tree is of minimal impact. The only object you need to consider is the workstation object. Individually, this object will only introduce approximately 4KB of information. However, the culmination of all workstation objects in your environment needs to be managed carefully, and you must use good design techniques in the placement of your partitions to make your tree most efficient. Included with the ZENworks CD from Novell is a document in the Docs directory called ZENDSGN.HTM that offers some guidelines for tree design.

Administration Through Novell Administrator

When you install ZENworks, additional snap-ins are delivered to the Novell Administrator. The latest version of the Novell Administrator, NWAdmin32, is introduced to your system, and the snap-ins for ZENworks are placed in NWAdmin32's directory structure. Because Novell realizes that you may not want to convert immediately to the new NWAdmin32, ZENworks also places these snap-ins into the appropriate directories to work with NWAdmin95 and NWAdminNT.

The NWAdmin32 program has had enhancements made to it that allow ZENworks administration to be less cluttered. When using the other version of the Novell Administrator, you see additional objects in the tree that you don't see with NWAdmin32. This is because support objects are administered through the policy package and not as individual objects.

The administration of ZENworks follows the familiar method of administering Novell Directories. ZENworks leverages all the features of the Directory including inheritance, rights, and standard associations.

Novell Client

ZENworks required some enhancements to the Novell client, and consequently the new client is included in the ZENworks package. Future clients delivered from Novell will continue to have support for ZENworks regardless of which bundled system is shipped. These enhancements include the addition of agents that are specific to ZENworks and hook into specific events that occur on the workstation, such as user login, user logout, screen saver activation, and so on. These hooks allow ZENworks agents to be notified when these events occur so they can begin doing their work.

When you install ZENworks into your network, you have the option of copying the clients to the servers. If you do this, your end-users can then have their login scripts modified to include calls to the client's ACU (Automatic Client Update) system, which will check its client to see if it is as new as the one on the server. If changes have been made to the client on the server and it is newer than the client on the workstation (resulting in the need to have the workstation), then the new client is automatically installed on the workstation.

Novell Workstation Agents

For convenience, several ZENworks agents that are necessary to interact with the Remote Control and Software Distributions system have been included with the client that is now being delivered from Novell. In particular, these items are Novell Workstation Manager, ZENworks Remote Control, and the Novell Application Launcher service. Currently, the Novell Workstation Manager and Novell Application Launcher services can only be installed with the clients. The Remote Control facilities, in addition to being included with the clients, are also delivered as application objects in the tree when ZENworks is installed. Once delivered as application objects, this service can then be installed independently on any workstation by associating the application object with the user object in the tree, and having the user run the ZENworks Application Launcher.

Policy Packages and Policies

To help in the administration of all of the features and policies of ZENworks, the policies are conveniently grouped into policy packages. These policy packages are logical grouping of policies that are valuable for a user or device. There are policy packages for Windows 3.1 users, Windows 95/98 users and Windows NT users. There are also policy packages for Windows 3.1 workstations, Windows 95/98 workstations and Windows NT workstations.

Policies that are appropriate for each package are included in each policy package, and are effective only for the devices and users that are associated with that package. Although some policies are the same in a Windows 95 workstation package and a Windows NT workstation package, the actual policies are kept independent. In other words, individual policies are not shared between policy packages.

Policy packages may be associated to the various appropriate objects. For example, user policy packages may be associated with a single user, a group of users, or a container. Workstation policy packages may be associated with a single workstation, a group of workstations, or a container. A single policy package may also be associated with several users, groups, and containers.

Because the system looks for policies by searching up the tree from the user or workstation object (depending on the application), there is a desire to keep this search from proceeding too far up the tree. Therefore, ZENworks included a search policy found in the Container policy package. This policy limits the number of levels and the search order that all ZENworks systems use to discover and apply policies.

ZENworks Policy and Policy Package Wizards

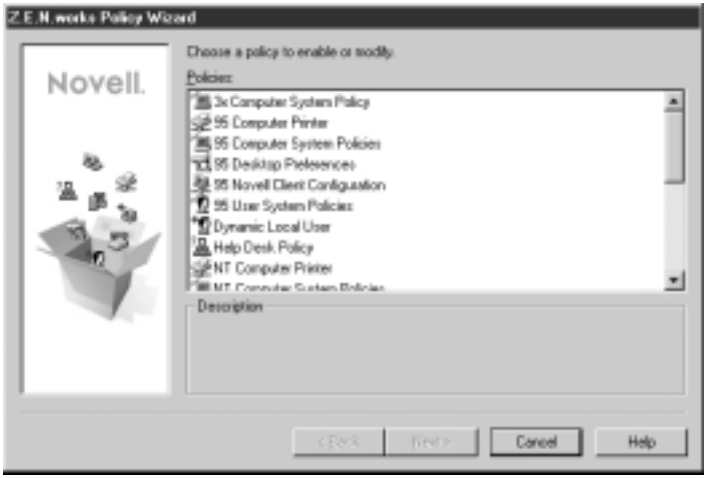
To assist you in constructing policies, ZENworks has included two wizards in the product. The two wizards are the ZENworks Policy Wizard and the Policy Package Wizard.

ZENworks Policy Wizard

The ZENworks Policy Wizard is activated from within NWAdmin by selecting the Tools ➪ ZENworks Policy Wizard menu choice. This wizard is used to construct the proper policy packages and policies when you know what policy you want but you need some help knowing what packages to make.

When the Policy Wizard is launched, a screen similar to the one in Figure 3.1 appears, enabling you to create and modify all the policies in the system.

FIGURE 3.1 *The main window in the ZENworks Policy Wizard utility*



The best way to understand how to use the Policy Wizard is to take a look at a the following examples.

Example of Enabling an NT Novell Client Configuration Policy

For the first example, we will enable an NT Novell Client Configuration policy.

The first step is to select NT Novell Client Configuration from the main screen in the Policy Wizard and click the Next button.

When the policy type is selected, you have the option to use an existing package, or you can create a new one, as shown in Figure 3.2. If the Use an existing policy package option is selected, a dialog box appears, enabling you to specify a context for the policy package object or navigate to it, as shown in Figure 3.3. If the Create the policy package option is selected, you are given the option to specify a name and select the context it will be created in, as shown in Figure 3.4.

FIGURE 3.2 *The Create new policy package option*

FIGURE 3.3 *The Use existing policy package option in the Policy Wizard utility*

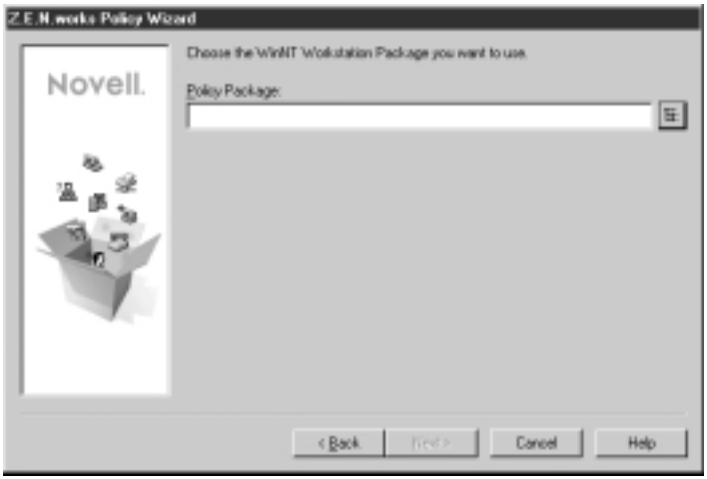
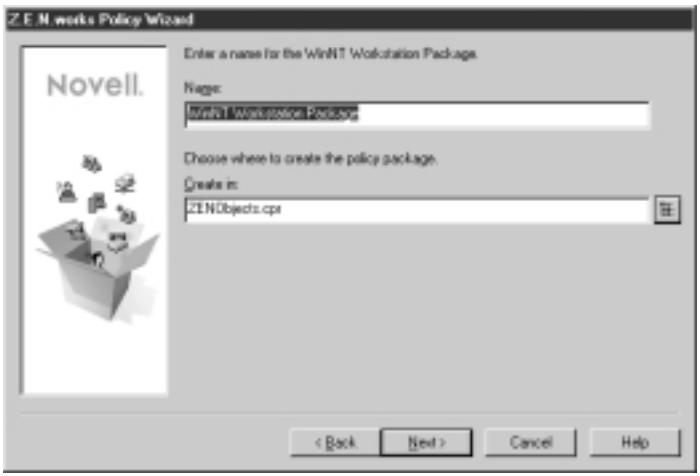
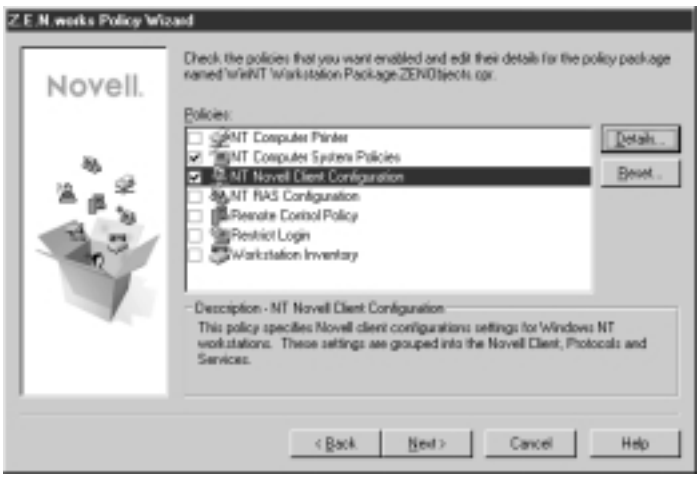


FIGURE 3.4 *The Use existing policy package option enables you to specify the creation context*



When the policy package has been established, a new screen similar to the one in Figure 3.5 is displayed. From this screen, you can view and select policies you wish to be enabled, as well as edit properties of those policy objects.

FIGURE 3.5 *The policy settings window*



To edit the properties of a policy from this window, highlight it and click the Details button shown in Figure 3.5. This brings up the normal screens associated with the policy and enables you to modify the attributes of the policy.

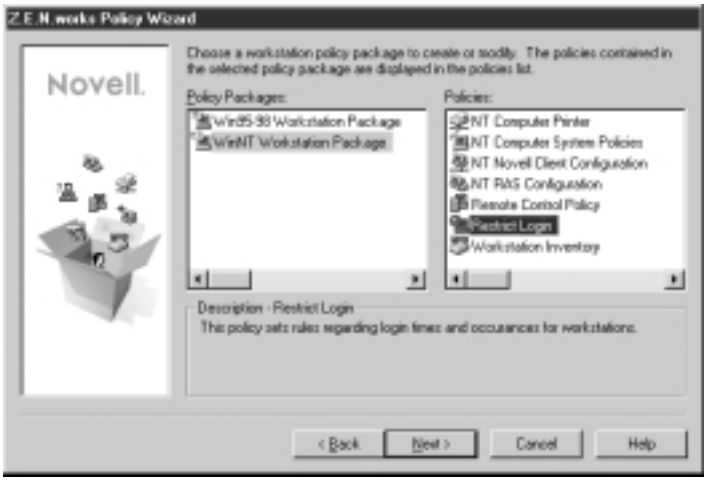
Example of Enabling a Restrict Login Policy

Now that an NT Novell Client Configuration policy and a WinNT Workstation Package exists, let's look at an example of enabling a Restrict Login Policy for that package.

The first step is to select the Restrict Login policy from the main window in the Policy Wizard. A new window appears, similar to the one in Figure 3.6. From this window, select WinNT Workstation Package and the Restrict Login policy, and then click Next.

At this point, you may wonder why you see a different screen than in the first example. This is because the Restrict Login policy is a valid policy for either the Windows 95/98 Workstation Package or the Windows NT Workstation Package, whereas the NT Novell Client Configuration Policy in the first example is only valid for the Windows NT Workstation Package. Consequently, this screen is skipped in the first example and displayed in this case.

FIGURE 3.6 *The Restrict Login policy*



Next you would select Use existing policy package and find the policy created in the previous example. A new window appears with the Restrict Login policy already selected, as shown in Figure 3.7.

FIGURE 3.7 *The policy settings window*

To set up the login restrictions for this WinNT Workstation package, click the Details button and make the necessary changes in the specific policy.

Policy Package Wizard

The Policy Package Wizard is activated when you create a policy package from the Create menu choice. The first screen, shown in Figure 3.8, presents you with the list of all available policy packages and the list of policies that are contained in each policy package.

Select a policy package, and click Next. The dialog box that appears asks you to enter the name of the policy package and the container where the package should reside. This screen is similar to Figure 3.4.

After selecting the name and container, you are presented with the set of policies that are available with this policy package. You can then select each policy you want to activate and adjust the values for each by highlighting the policy and pressing the Details button. This screen is similar to Figure 3.5.

The next screen of the wizard enables you to select the containers, users, or groups that should be associated with the policy. The association will activate this policy for those users or workstations. Figure 3.9 is a sample of this screen. The wizard places a default value of the current container to be associated with the policy package. You can add and remove associations through this screen. When you've finished, press the Next button to move on to a summary screen.

FIGURE 3.8 *Initial screen from the Policy Package Wizard*

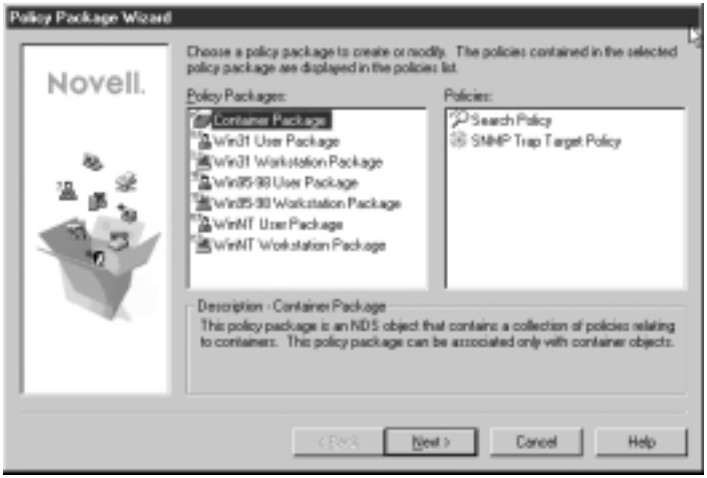
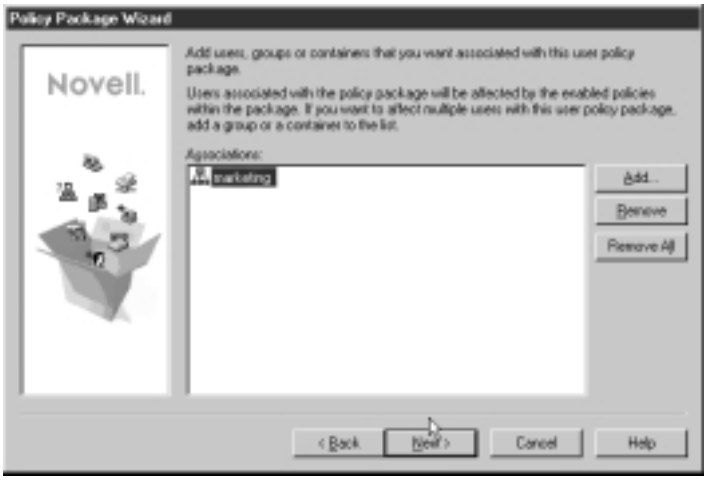


FIGURE 3.9 *Associations screen*



The summary screen displays a description of what the wizard will be doing. This description reiterates the package type to be created, the name of the package, the container holding the package, the enabled policies in the package, and the associated objects. When you press the Finish button on this screen, the policy package is created and the associations are made.

Setting Up Workstations in the Tree

Before you can start managing the workstation, you must create workstation objects and associate them with physical workstations. This step is not necessary if you do not want to manage the physical device, but instead want to manage only the desktop. For example, if you only want to deliver applications to the workstation and apply Microsoft policies to the desktop when a user is logged in to the workstation, then associating a user policy to the particular user accomplishes all this. However, should you want to manage the physical inventory and perform remote control functions, in addition to managing the workstation accounts, then you must first have the workstation object.

You must perform the following steps to place a functioning Import Policy in your tree:

1. Create a policy package.
2. Turn on the Import Policy in the policy package.
3. Associate the policy package with a user container.
4. Allow login cycles to register the workstation to the tree.
5. Import the workstations into the tree. (This creates the workstation object.)
6. Associate other policies to the workstation objects to effect management.

Creating a Policy Package

Before you can start working with ZENworks workstation features, you must first create a policy package to hold the policies associated with users and workstations. To get the ball rolling, you must first create a user policy package. To create a user policy package, follow these steps:

1. Start NWAdmin32.
2. Select a container to hold the policy package object.
3. Select the Create menu choice and create a policy package object.

4. In the Policy Package Wizard, select a user policy package for the type of package, and name the object. Follow the wizard along and associate the policy package with the container that has the user objects for which you would like to have these policies in effect. Remember that these policies will be effective in subcontainers as well, so you can associate the policy package high enough in the tree to affect as many users as desired.

Creating a Workstation Import Policy

Now that you have created a user policy package and associated it with a container that holds the users you want to affect, you can create a workstation import policy. To create the Workstation Import Policy, follow these steps:

1. Start NWAdmin32.
2. Browse to the container that has the user policy package you want to administer.
3. Select the user policy package and request details on the object.
4. Select the workstation import policy from the list of policies available. When you select and activate the import policy, the checkbox to the side is checked.
5. Perform details of the workstation import policy if desired.
6. Select OK and close out the dialog boxes.

When you've created a workstation import policy, the workstations that are registered with their cookie to the tree can have workstation objects associated with their physical devices.

In Step 5, you had the option of modifying the details of the import policy. Let's discuss briefly some of these options. If you decide to take the default import policy, then workstations, when created, will be located in the same container as the user object and will be named by the concatenation of the user login name and the MAC address of the network card. The user object that is associated with the workstation and is used in its naming is the first user to log in to the network on that physical workstation. By going into the details of the import policy, you can change the policy to identify under which container you want the workstation object to reside (this can be absolute or relative to the user container) and select options on how to name the workstation object. The import process uses the information in the cookie to generate the name of the workstation object and the initial data that is placed in the object.

Associations of Policy Packages

The ZENworks system will always start with the relevant user or workstation object, depending on the feature being executed. Once the user or workstation object is located, then the system will "walk the tree" until it locates the first policy package it can find. Generally, when a package is found, the configuration set in that policy is applied to the system, and the ZENworks feature activates. Some features, such as the Microsoft Windows desktop policies, are an accumulation of several ZAW/ZAK policies to which the user may be associated. These policies require that the search proceed to the root of the tree.

"Walking" to the root of the tree for policy packages can be time-consuming, especially if the tree spans across a WAN link. Therefore, ZENworks introduced the Search Policy, contained in the Container Policy Package. This Search Policy limits the levels of containers that all processes search to find their policies.

Novell Workstation Registration

Once an import policy has been created and associated with user objects, either by direct association or by association to the user's container, the workstations that have registered their cookie with the tree may now be imported.

The first person to log in to the tree from the workstation (once the ZENworks-enabled Novell Client has been installed on the workstation) will initialize the ZENworks agents on the workstation. The first thing these agents do is to register the workstation with the tree of the user. A workstation is only registered once, in one tree.

The registration of the workstation results in information being placed on the workstation and in the immediate container of the user object. This information includes the name of the user that is logged in when this cookie was created, the computer name, the MAC/IPX address of the workstation, the IP address, the workstation DNS name, the type of CPU, the operating system on the workstation, and the preferred server. This cookie is placed in the container and is then used later by the import process. The workstation remembers where it placed this cookie and goes back there to look for its workstation object when it is finally created. Each of these fields may or may not have values in the registration, based on the environment of your system.

Some administrators set up a workstation and validate that it can successfully connect to the network before allowing the end user to use the workstation. In this case, all the workstations would then be associated with the administrator rather than the end user of the workstation. Therefore, ZENworks includes the tool unreg.exe in the SYS:\PUBLIC directory; this tool, when run on a workstation, will essentially reset the workstation registration back to being unregistered. After the

administrator runs this tool, the administrator can then give the workstation to the end user; then, when the end user logs in to the network, his or her user object will be associated with the workstation. This technique can also be used for having a workstation reregister. If you delete the workstation object in the tree and then run unreg.exe, the workstation will then redo the process of registration the next time a user logs in to the network.

Importing Workstations

Once the registration of the workstation has occurred and this cookie has been placed in the tree, and a workstation import policy has been created, you can import these cookies and create workstation objects from this information. This process will also automatically notify the workstation that an object has been created for it, and will allow it to know the name of its object. You import workstations by following these steps:

1. Start NWAdmin32.
2. Browse to the container where you want to start importing workstations.
3. Import Workstations by doing either of the following:
   a. Launch Tools ➪ Import Workstations. This brings up a set of dialog boxes to walk you through importing the workstations whose registration cookies are found in the current container and all subcontainers.
   b. Activate details on the container object and select the Workstation Registration tab. From there, you can select individual cookies and import the workstations from that page.
   c. Run the WSIMPORT.EXE utility found in the SYS:\public\winnt directory. This utility is a separate Windows utility that imports workstations into the tree. The tool can be scheduled through the ZENworks scheduling facilities should you want your workstation to automatically import workstations. You can also use WSIMPORT to remove cookies and old workstation objects from the tree. Obviously, you must be the administrator in order to have these operations succeed. The WSIMPORT.EXE utility has the following command-line options: wsimport [context | /T treename | /S [-] | /H | /C | /R days | /?].

The WSIMPORT.EXE command-line options are:

- context — This is the context in the tree where you wish the wsimport to begin its work. Remember, if the context has a space in it, you need

to enclose the context in double quotes. If no context is specified, then the current context of the workstation user is used.

- /T treename — This enables you to specify the tree you wish wsimport to work on. It is assumed that the context specified or defaulted is in the tree; if not, an error will occur.
- /S [-] — This tells wsimport to include subcontainers in its work. The default is for it to walk the tree into subcontainers. With the /S- option, you can turn off the subcontainers, and wsimport will only do its work in the context specified.
- /H — This option runs wsimport in hidden mode with no user interface or dialog boxes.
- /C — This option requests that all the registration cookies in the containers be removed.
- /R #days — This option removes all the workstation objects that are older than *#days* from the current date. The workstation object has a registration page indicating the last time a workstation has touched the workstation object (it happens at each login). If this date is older than *#days* specified from today's date, then the object will be removed from the tree.
- /? — This is a brief command-line help dialog.

Here are a couple of examples to help out. The next line will import all workstations from the marketing.xyz context and below in the company tree. Remember, it will use the import policy that is associated with the marketing.xyz or above containers.

```
wsimport marketing.xyz /T company /S
```

The next example will remove all workstations that have not been accessed in the last 60 days from the xyz container of the company tree.

```
wsimport  xyz /T company /R 60
```

When you import workstations, the workstation object is created, and the cookie left by the workstation is updated to reflect the name of the workstation object that was made for that entry. The next time any user logs in to the network from that workstation, the agents will look up their cookie in the tree and will now discover that they have an associated workstation object. This workstation object name is then saved on the physical workstation, so that now the agents know the object in the tree that represents this workstation.

Until this registration process is completed (1. Workstation places cookie in tree; 2. Administration imports the workstation; 3. The user logs into the NDS tree again), the workstation physical device does not have a complete association with the tree and the workstation object. Without this association, the features that require rights or access to attributes on the workstation object will not function properly. This includes most of the remote management functionality and the hardware and software scanning features.

Creating Other Policies

When you have your users associated with their appropriate policy packages, you can then create other policies in that package and have them affect the user's environment. This also is true with workstation objects and their associated policy packages.

Remote Management Rights

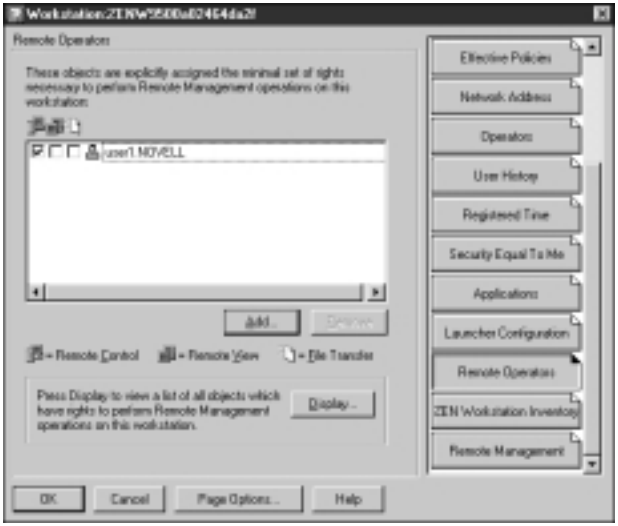
A majority of the remote management features are available to users and administrators via rights in the NDS tree on the objects that represent the target device. For example, in order to remote control a target workstation, you must have rights in the target workstation object in order to perform the remote control function.

You must grant individuals rights in the tree to allow them to perform remote management functions on workstations and user desktops. The following objects in the tree may be granted remote management rights: user, group, organizational role, organization, organization unit, country, locality, [Root], [Public]. There are two methods that you can use to set up these rights. The following subsections discuss these methods.

Remote Operators Page

There is a Remote Operators page associated with each workstation object. Figure 3.10 displays this page.

FIGURE 3.10 *Remote Operators page in a workstation object*



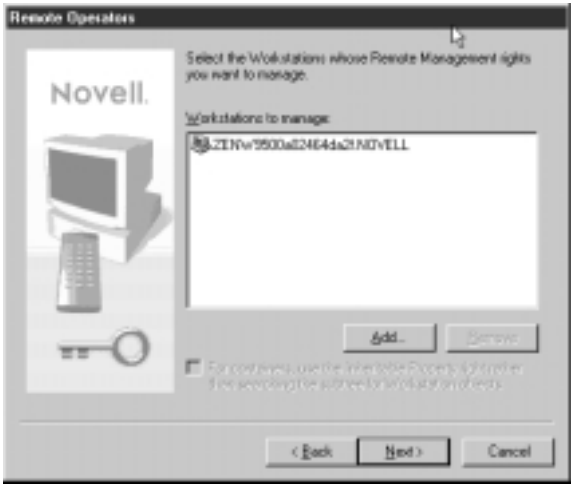
From within this page, you may add either users or groups to the list of operators. With each addition, you can check which of the remote management utilities this addition has rights to perform. The three choices available are Remote Control, Remote View, and File Transfer. By checking the box underneath the icon associated with each of these functions, you grant that user or group the rights to perform those functions on this particular workstation.

Remote Operators Wizard

Another method of granting users or groups access to the remote management functions is through the Remote Operators Wizard. Figure 3.11 displays the initial page of the wizard.

The wizard walks you through selecting the workstation object or containers and then identifying the remote management operations. Following these selections, you must identify the users, groups, or containers to which you want to grant these rights. Once this is specified, the wizard looks up all the workstation objects in the tree below the specified container, and sets the appropriate rights for each of the users, groups, or containers.

FIGURE 3.11 *ZENworks Remote Operators Wizard*



Reporting

ZENworks has introduced some reporting capabilities to Novell management utilities. As information is stored in the database for hardware and software scanning and for the SNMP trap information that is a result of application distribution, it is important to be able to retrieve this information and review reports. Currently, you cannot retrieve any reports from ZENworks unless you have installed the database. Also, if you want application reports you must have an SNMP trap target policy that sends the SNMP information to the database, and you must have run the workstation inventory in order to get inventory information out of the database.

Currently, ZENworks reporting relies on an ODBC driver to the embedded ZENworks database. Before you can perform any reporting functions against the database, you must first properly install the ODBC drivers on your administrator workstation. This is best accomplished by launching the application object that was installed with ZENworks for the ODBC driver. The name of this application object is ZENworks Reporting – ODBC. Just associate this application object with your login and run the NAL program. When the application appears on the desktop or in the NAL window, double-click it to install the ODBC drivers.

With ODBC drivers, you are required to specify the database to which your queries will be directed. When ZENworks is installed and creates the ODBC driver application object, it places in the object the location of the database that you installed during the install process. If you have multiple databases, then you should have multiple ODBC objects and you will need to launch each one prior to running reports against the desired database.

Once you have installed the ODBC driver, you can launch NWAdmin32 and select reporting from the Tools menu. This launches the reporting dialog box that enables you to select the report you wish to generate. The "canned" reports are categorized into two types — Application Management and Inventory — and are found under the File menu of the reporting tool. The Application Management canned reports display data on application deployment to the desktop, and Inventory reports have information on the hardware and software scan results for each workstation. You can generate any of the following reports:

- Inventory:
  - General Workstation — This gives the list of hardware installed, networking information, and the operating system installed on one or more workstation.
  - Asset Management — This displays a list of the bios information, processor, and operating system on one or more workstations.
  - Hardware — This is a list of the memory information, video, processor, and hard disks installed on one or more workstations.
  - Workstation Based Software — This provides a list of the workstation-specific software installed on one or more workstations, grouped by workstation. The list of software is generated from the software list identified in the policy.
  - Product Based Software — This provides a list of the product software installed on one or more workstations, grouped by workstation. The list of software is generated from the software list identified in the policy.
  - Driver Information — This gives a list of the drivers that are installed on one or more workstations.
  - Networking Information — This provides a list of networking details on one or more workstations.

- Application Management:
  - Application Distribution Successes by Workstation — This provides a list of the successful application distributions that have occurred that were distributed by the ZENworks Application Launcher, grouped by workstation.
  - Application Distribution Failures by Workstation — A list of the failed application distributions that have occurred that were distributed by the ZENworks Application Launcher, grouped by workstation.
  - Application Distribution Successes by Application — This displays a list of successful application distributions that have occurred through the ZENworks Application Launcher, grouped by application.
  - Application Distribution Failures by Application — This displays a list of failed application distributions that have occurred through the ZENworks Application Launcher, grouped by application.
  - Application Distribution Successes by User — This displays a list of successful application distributions that have occurred through the ZENworks Application Launcher, grouped by user.
  - Application Distribution Failures by User — This displays a list of failed application distributions that have occurred through the ZENworks Application Launcher, grouped by user.
  - Application Launch Successes by Workstation — This gives a list of the successful application launches that have occurred, via the ZENworks Application Launcher, grouped by workstation.
  - Application Launch Failures by Workstation — This gives a list of the failed application launches that have occurred, via the ZENworks application launcher, grouped by workstation.
  - Application Launch Successes by Application — This gives a list of the successful application launches that have occurred, via the ZENworks Application Launcher, grouped by application.
  - Application Launch Failures by Application — This gives a list of the failed application launches that have occurred, via the ZENworks application launcher, grouped by application.
  - Application Launch Successes by User — This gives a list of the successful application launches that have occurred, via the ZENworks Application Launcher, grouped by user.

- Application Launch Failures by User — This gives a list of the failed application launches that have occurred, via the ZENworks application launcher, grouped by user.

Once a report is generated, you can either view it online, in the utility that pops up after generating the report, or send it to a printer.