Native File Access **Wanted**

[Client Software Need Not Apply]

by Cheryl Walton

As a NetWare administrator, you no doubt appreciate NetWare's legendary stability and reliability. In fact, you probably wish that all of the servers on your company's network were as reliable as the NetWare servers. Of course, you probably already take advantage of NetWare's reliability by storing on your trusty NetWare systems the application data produced by other, less reliable systems.

For example, you may store data from Windows-based applications such as Excel on NetWare servers. After all, in your experience, NetWare has proven to be more reliable than Windows—and you're not the only one to have arrived at this conclusion. The author of a recent *ZDNet* article explains, "Between reboots, I've run NT for weeks, Windows 2000, Linux, and UNIX servers for months, and NetWare 3.1x/4.x for years." ("NetWare Still a Top-Notch NOS," *ZDNet*, Sept. 10, 2001. You can download this article from http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2811500,00.html.)

The upside of using the reliable NetWare platform to store and manage your company's critical data far outweighs the downside of using NetWare for this purpose. Nevertheless, a downside exists: You may need to install and manage client software so that users can access data on NetWare servers.

Admittedly, running client software on Macintosh, Windows, and UNIX clients to enable access to files on NetWare servers has advantages. However, this approach doesn't make sense for everyone. Therefore, Novell now provides an arguably more sensible way for Macintosh, Windows, and UNIX users to access files on NetWare servers: With Novell Native File Access Pack, these users can access files on NetWare servers without having to run Novell or third-party client software.

A PACK OF COMPONENTS

Native File Access Pack is server-based software that includes the following components:

- Native File Access for Macintosh
- Native File Access for Windows
- Native File Access for UNIX

You can install one or more of these components on NetWare 6 servers and on NetWare 5.1 servers that are running Service Pack 3 and above. (You can download the latest service pack for NetWare 5.1 at http://support.novell.com/misc/patlst.htm. For more information about installing Native File Access Pack, see "Installing Native File Access Pack Components" on p. 14.)

Native File Access Pack components ship with NetWare 6. NetWare 5.1 maintenance and upgrade customers can download Native File Access Pack components free from Novell's web site. (You can also purchase Native File Access Pack for U.S. $299 per server. For more information, visit www.novell.com/products/nfa.)

As the names of these components suggest, Native File Access Pack components enable computers running Mac OS, Windows, and UNIX-based operating systems to access and manage files on NetWare 6 and 5.1 servers using native file protocols. That is, computers running Mac OS 8.1 or above and Mac OS X can use the Apple Filing Protocol (AFP) to copy, delete, move, open, and save files on NetWare 6 and 5.1 servers.

Similarly, computers that are running Windows 2000, ME, NT 4, 98, and 95 can use the Common Internet File System (CIFS) protocol to perform these tasks. Computers running UNIX-based operating systems such as Linux, on the other hand, can use the Network File System (NFS) protocol to perform these tasks. (See Figure 1 on p. 12.)

Because these server-based components enable users to access NetWare servers with no client-side software strings attached, using Native File Access Pack components can simplify network administration. You don't have to install, update, and manage Novell client software on these operating systems. In fact, in many cases you can take a Macintosh, Windows, or UNIX-based computer out of its box, plug it into the network, configure it to use TCP/IP, and start using that computer to access files on a NetWare server without further ado.

Native File Access Pack components also help secure your company's data because these components use Novell eDirectory to ensure that only users with appropriate rights have access to files on NetWare servers. In other words, like most of the software that Novell has created over the past two years, Native File Access Pack components are Net services software. As you probably

Illustration: Paul Zwolak

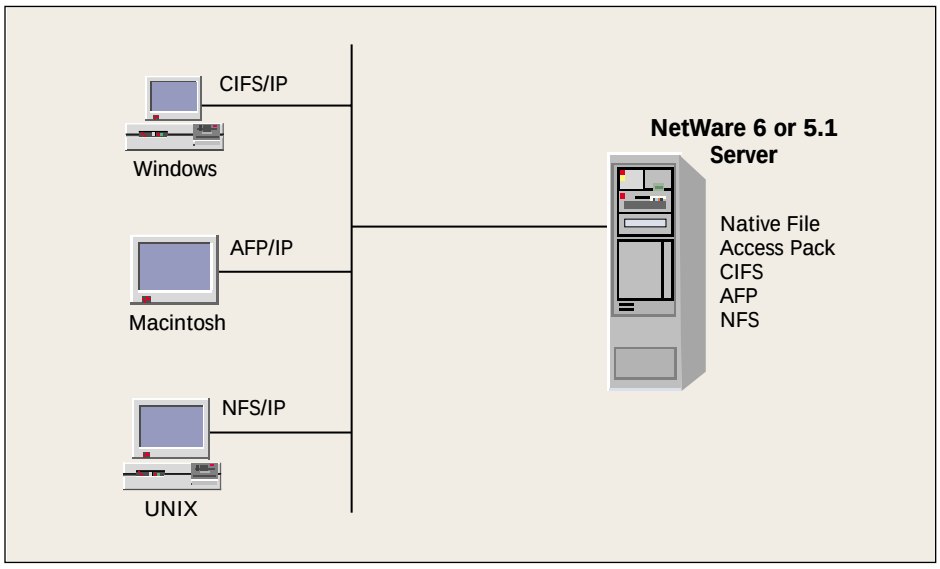

Figure 1. Native File Access Pack components for Macintosh, Windows, and UNIX emulate Macintosh, Windows, and UNIX servers. Users can access files on NetWare from Macintosh, Windows, and UNIX client computers using native file protocols.

FOLDER RIGHTS MAPPING FROM MAC TO NETWARE

Macintosh	NetWare Mapping
Read-Only	File Scan, Read
Write Only (Drop Box)	Create
Read/Write	File Scan, Read, Create, Write, Erase, Modify
No rights	No rights

FOLDER RIGHTS MAPPING FROM NETWARE TO MAC

NetWare Rights	Macintosh Mapping
File scan or read	Read-Only
Create	Write Only (drop box)
(File scan or read) and (create or write or erase or modify)	Read/Write
No rights	No rights or just write or erase or modify

Figure 2. Mapping NetWare's six rights to Macintosh's four rights can be confusing for Macintosh users. For example, suppose a Macintosh user has file scan, read, create, and write access to a folder on NetWare. Native File Access for Macintosh would display these rights on a Macintosh computer as read-write rights. On an AppleShare network, read-write rights would enable users to delete folders. Because erase and modify rights have not been assigned on NetWare, however, this user would not be able to delete this folder.

know, Net services software works across all major operating systems to simplify the complexities of network management, secure network resources against unauthorized access, and accelerate your company's transition to e-business.

THEY'RE THE SAME, ONLY DIFFERENT

Native File Access Pack components have several key features in common. For example, all three components use native file protocols over TCP/IP, and all three components use eDirectory to control users' access to NetWare volumes.

In addition, all three Native File Access Pack components support Novell Cluster Services. Native File Access Pack components for NetWare 5.1 support Novell Cluster Services 1.01, which runs on NetWare 5.1. Native File Access Pack components for NetWare 6 support Novell Cluster Services 1.6, which runs on NetWare 6. (For more information about Novell Cluster Services, see "Novell Cluster Services 1.6: Keep the Server Side Up and the SAN Side Simple," *Novell Connection*, June 2001. You can download this article from www.ncmag.com/past.)

Another point of similarity is that you can manage all three Native File Access Pack components via ConsoleOne. For example, you use ConsoleOne (running on an administrator workstation) to manage simple passwords for Native File Access for Macintosh and Windows components. (For more information about simple passwords, see "Keep It Simple" on p. 22.) Similarly, you use ConsoleOne to configure and manage Native File Access for UNIX. (You can also configure and manage Native File Access for UNIX through configuration files using a standard text editor.)

Finally, the Native File Access for Macintosh and Windows components enable you to use context search files that, in turn, enable users to log in using only a username and password. Without these context search files, Windows and Macintosh users must log in using their entire eDirectory context. (For more information about context search files, see "Putting Things Into Context" on p. 16.)

Native File Access for UNIX also provides this service, but does so differently. In the UNIX case, you configure a Search Root, which is the eDirectory context from which you want Native File Access for UNIX to begin its search for UNIX users and groups.

Although Native File Access components have many features in common, each component interacts with a different operating system's file access protocol. Consequently, each component functions uniquely. As Novell product manager Matt French explains, "For each platform, Novell Native File Access Pack has a different story."

TCP/IP SUPPORT PUTS A LOT OF POLISH ON THE OLD APPLE

Although all three Native File Access Pack components use TCP/IP, TCP/IP support in Native File Access for Macintosh is particularly noteworthy. If your company needs to provide Macintosh users with access to NetWare servers, you know that previous options for performing this task do not use AFP over TCP/IP.

NetWare Client for MacOS uses either NetWare Core Protocol (NCP) over IPX or NetWare/IP, depending on which protocol configuration you select. NetWare 5 Services for AppleShare, on the other hand, uses AFP over AppleTalk, which is a proprietary transport protocol for AppleShare networks. (NetWare 5 Services for

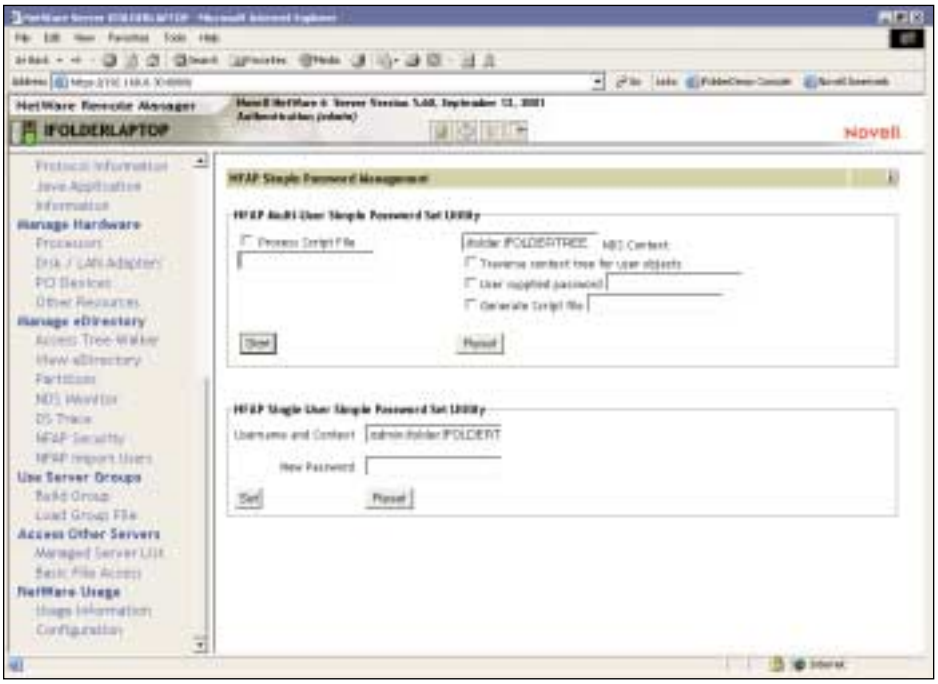

Figure 3. The Native File Access Pack Simple Password Management utility gives you several options for setting users' simple passwords in eDirectory.

AppleShare from Prosoft Engineering is server-based file-sharing software that runs on NetWare servers. For more information, visit www.prosofteng.com.) Using these previous options prevents you from migrating your company's NetWare network to TCP/IP only.

Because you must use TCP/IP to do business over the Internet, companies that want to engage in e-business may be particularly anxious to migrate their networks to IP only. In fact, as Douglas Phillips, a senior software engineer for Novell, explains, the ability to migrate your company's network to IP only may be only one of the primary reasons to deploy Native File Access for Macintosh.

Of course, whether or not your company wants to move its network to IP only, with Native File Access for Macintosh, dyed-in-the-wool Macintosh users won't need to learn how to use NetWare client software. Instead, these users can create, delete, and manage files just as they would if they were connected to an AppleShare network.

Like AppleShare, But Not Exactly

With Native File Access for Macintosh, Macintosh users can share folders on their Macintosh workstations. In contrast, using NetWare Client for MacOS and NetWare 5 Services for AppleShare, users must ask you, the network administrator, to share folders for them.

However, these users' ability to share folders isn't exactly like sharing folders on an AppleShare network. As Phillips explains, eDirectory has "a much richer set of access controls than AFP" allows. (See Figure 2 on p. 12.) Therefore, mapping the limited set of access controls available through AFP to the larger set of access controls available through eDirectory can confuse Macintosh users. After all, these users are accustomed to sharing folders on an AppleShare network.

The information that Native File Access for Macintosh users see when they access information about shared folders is a fraction of the information that actually exists. For example, suppose a Macintosh user who is accustomed to sharing folders through AppleShare is the owner of a particular folder. Also suppose that this user wants to make that folder available to the Teachers group. Furthermore, suppose this same folder is currently available to the Administrators group.

AFP supports only one user or group per shared folder. Therefore, if this user makes the folder available to the Teachers group, she expects to simultaneously make the folder unavailable to the Administrators group. As you know, however, Native File Access for Macintosh uses eDirectory to control access rights, and eDirectory supports a virtually unlimited number of users and groups per folder.

Consequently, when this user makes the folder available to the Teachers group, she is actually making this folder available to an additional group, rather than reassigning access rights from the Administrators group to the Teachers group. Unfortunately, the user's Macintosh client can display access rights for only one of these two groups.

The group the user's Macintosh client displays when that user requests information about the folder depends upon which group has the greatest access rights. When users request information about access rights, Native File Access for Macintosh favors group access rights over user access rights and greater access rights over lesser access rights.

If the Administrators group in this example had greater access rights than the Teachers group, the user's Macintosh client would display the Administrators group's ownership to this folder. The user would therefore think that her attempt to give the Teachers group access rights to this folder had failed.

In addition, Macintosh computers support inherited rights or explicit rights, but not both, as eDirectory does. Furthermore, Macintosh computers do not display inherited rights in the Get Info/Sharing

Installing Native File Access Pack Components

Native File Access Pack components run on NetWare 6 servers and on NetWare 5.1 servers with Service Pack 3 or later. If you install Native File Access Pack components on NetWare 5.1 before Service Pack 4 is available, you must also install the following two patches: Winsock Update for NetWare 5.0/5.1 and NSS NLMs post SP3. (You can download these patches from the Novell Support Knowledgebase. To find the most current version of these patches, search the Support Knowledgebase—http://support.novell.com/search/kb_index.jsp—for each patch by name.)

These patches will be included with NetWare 5.1 Service Pack 4 and are included with Native File Access Pack components for NetWare 6, which ship with NetWare 6.

Putting Things Into Context

Using context search files, you can simplify access to files on NetWare servers that are running Native File Access for Macintosh and Native File Access for Windows. A context search file is a text file wherein you list eDirectory contexts for Macintosh and Windows users. When users don't provide a context at login, Native File Access for Macintosh and Native File Access for Windows search these listed contexts. By entering these users' contexts in context search files, you enable Macintosh and Windows users to log in without having to provide their contexts.

By default, Native File Access for Macintosh and Native File Access for Windows look for context search files in the SYS:\ETC directory on the server where these components are running. Specifically, Native File Access for Macintosh looks in the SYS:\ETC directory for a context search file named CTXS.CFG; Native File Access for Windows searches in the SYS:\ETC directory for a file named CIFSCTXS.CFG.

The Native File Access for Windows installation program asks you to provide eDirectory contexts for all Windows users who need to access this server. The installation program then stores these contexts in the CIFSCTXS.CFG file. After installation, you can use a standard text editor (such as Notepad) to add or delete contexts in the CIFSCTXS.CFG file.

The Native File Access for Macintosh installation program does not ask you to provide user contexts. Instead, you use a text editor to create the CTXS.CFG file after the installation program has completed its task. You then add contexts for Macintosh users.

For example, suppose your company's eDirectory tree is called *catchall,* and you want to provide NetWare file access to Macintosh users in your company's graphics, sales, and administrative departments. These departments are represented in eDirectory by graphics, sales, and administrative container objects. Using a text editor, you would enter the following contexts in the CTXS.CFG file:

- graphics.catchall
- sales.catchall
- administrative.catchall

Suppose Sara, a Macintosh user in the administrative department, tries to log in to the NetWare 6 server by typing only her username and password (instead of typing her username with a context such as sara.administrative). Because Sara does not provide a context with her username, Native File Access for Macintosh searches through the contexts listed in the CTXS.CFG file, starting with the first context in the file—the graphics.catchall context.

If a different user named *Sara* exists in the graphics context, Native File Access for Macintosh will assume that this different Sara is the same Sara who is attempting to log in. That is, Native File Access for Macintosh will try to log in sara.graphics using sara.administrative's credentials.

Of course, this login attempt would fail. Sara would then need to log in using her name and context (sara.administrative).

Like Native File Access fosr Macintosh, Native File Access for Windows searches the first context in the context search file, followed by the second context, and so on. However, if the contexts in the example above are located in the CIFSCTXS.CFG file rather than the CTXS.CFG file, and Sara is a Windows user rather than a Macintosh user, Native File Access for Windows does not attempt to log in sara.graphics using sara.administrative's credentials.

Instead, Native File Access for Windows compares sara.administrative's login credentials with sara.graphic's credentials. When these credentials don't match, Native File Access for Windows continues searching the contexts in the CIFSCTXS.CFG file until it finds a match for Sara's login credentials in the administrative context. Native File Access for Windows then logs Sara in to the NetWare server.

dialog box, where Macintosh users are accustomed to seeing file-sharing information. As a result, Macintosh users cannot see the inherited rights that eDirectory is enforcing at the server.

Herein lies the potential for confusing Macintosh users.

ConsoleOne: The Know-It-All Do-It-All Utility

Because Macintosh computers don't include code for displaying the full array of NetWare access rights, Novell cannot remedy this potential confusion for Macintosh users. However, as a network administrator, you can't afford to be confused about access rights. Because managing access rights is part of your job, you must be able to see all of these rights. Fortunately, you can use ConsoleOne to see and manage these rights.

You also have a web-based option for seeing and managing file attributes: Novell Remote Manager enables you to use a web browser to manage NetWare 6 and 5.1 servers remotely. (For more information about Novell Remote Manager, see "Novell Remote Manager: Remote Control for NetWare Servers," *Novell Connection*, Sept. 2001. You can download this article from www.ncmag.com/past.)

In addition to managing access rights, you use ConsoleOne to create User objects for Macintosh users. Because Native File Access Pack components use eDirectory to store access rights, you must create User objects for all Macintosh (and Windows and UNIX) users who do not already have an eDirectory User object.

You may also want to create a Guest User object for Macintosh users. On AppleShare networks, users who do not have a username and password can log in as Guest. (See "The Ideal Guest" on p. 26 for step-by-step instructions for creating a Guest account in eDirectory.)

As you know, you can also use ConsoleOne to assign simple passwords for Macintosh users. (For more information, see "Keep It Simple" on p. 22.) After you've assigned simple passwords, Macintosh users can access volumes on the NetWare server just as if it were an AppleShare server.

TWO WAYS TO OPEN WINDOWS

With Native File Access for Macintosh, users must use simple passwords to authenticate to eDirectory. In contrast, with Native File Access for Windows, you have another option: Users can authenticate to a Windows domain.

When you install Native File Access for Windows, the installation program asks you if you want the Local option or the Domain option. The Local option enables users to use a simple password to authenticate locally to eDirectory. By redirecting requests for authentication to a Windows

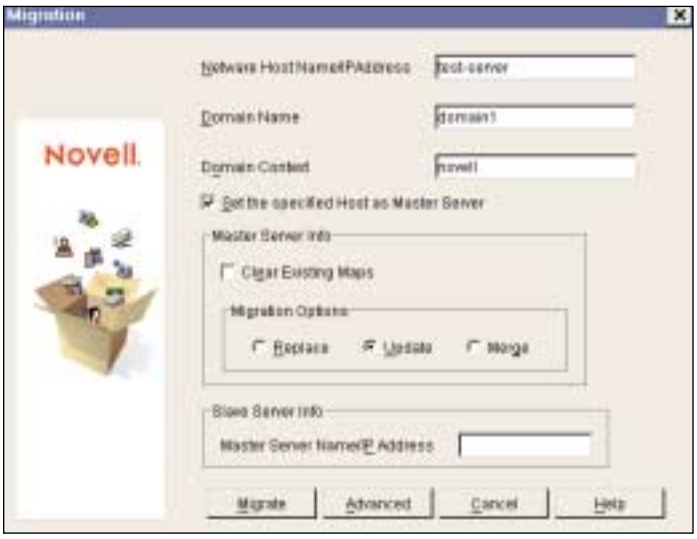

Figure 4. Native File Access for UNIX includes a migration utility to help you migrate users, groups, and NIS maps from an NIS server running on UNIX to Novell eDirectory. The Native File Access for UNIX NIS server then uses the information stored in eDirectory to provide NIS services for UNIX users.

domain controller, the Domain option enables users to authenticate using a domain controller password.

As you may expect, each option has advantages and disadvantages. For example, one disadvantage of the Local option is that Windows users need a simple password. (See "Keep It Simple" on p. 22.) With the Domain option, in contrast, you don't need to provide simple passwords.

However, the Domain option has its own disadvantages. For example, when you select the Domain option, users cannot use the Windows Change Password feature, as they can when you select the Local option. To change domain passwords for these users, you must use Windows domain management utilities, such as the User Manager for Domains utility for Windows NT 4.0.

Of course, the Domain option has some advantages. For example, when you select the Domain option, you do not have to manually create user accounts in eDirectory for Windows users who do not have an existing account. Instead, you can use the Native File Access Pack Import Users utility to import accounts for these users from a Windows domain. (This utility is hereafter called the *Import Users utility*.)

The Native File Access for Windows installation program installs the Import Users utility in Novell Remote Manager. To access this utility, you launch a web browser and type the URL for the Novell Remote Manager running on the same server as Native File Access for Windows. You then select the NFAP Import Users link that appears on the Novell Remote Manager main page.

To use the Import Users utility, you must provide an eDirectory context. The Import Users utility locates user and group accounts in the Windows domain that you specify when you select the Domain option. This utility then creates eDirectory accounts for these users and groups in the context that you provide. After the Native File Access Pack Import Users utility has created these user and group accounts, you must use ConsoleOne to set access rights for these users and groups in eDirectory.

The Right Option for Your Network

As you may expect, your company's present network will probably determine which of these options is most advantageous. For example, if your company has a large NetWare network, selecting the Local option is probably best. On an existing NetWare network, selecting the Local option enables you to add Windows computers to that network without having to install and manage Novell client software on those computers. (You do need to run the Client for Microsoft Networks on these computers. For more information see "Networking a la Windows.")

In contrast, the Domain option is probably the best choice if your company already has a large Windows network in place. The Domain option is a particularly good choice if Windows users are already authenticating to your company's network through domain controllers. This option conveniently enables these users to use their existing login credentials to access NetWare servers.

Furthermore, these users probably won't even know they are using NetWare servers. After all, when you use Native File Access for Windows, NetWare and Windows servers look the same to users.

In other words, if you have a Windows shop, Novell consulting software engineer Scott Isaacson explains, you can strengthen your network's backend without disrupting users at all. That is, you can buy a Novell server for the backend, and users can then access that server in precisely the same way they access Windows servers, Isaacson adds.

The impact on you is also minimal: You do not have to manage Novell client software, and you do not have to teach users a new way of accessing data.

In addition, you can use eDirectory to manage user accounts by deploying Novell Account Management. By integrating with Windows 2000, NT, Sun Solaris, and Linux, Novell Account Management enables you to manage all network users through eDirectory. (For more information, visit www.novell.com/products/nds/accountmanagement/details.html.)

With Novell Account Management, you can create user accounts in eDirectory and then use these eDirectory accounts to populate user accounts in Windows domains. Because managing users in eDirectory is easier than managing users in domains, Novell Account Management further simplifies your life.

Networking a la Windows

With Native File Access for Windows, Windows users can access NetWare servers without running Novell client software on their Windows client computers. However, these users still need networking software on their computers. These users must run Microsoft's Client for Microsoft Networks, which is a standard component of the Windows operating system. To install Client for Microsoft Networks, complete the following steps:

1. On a Windows client computer, select Control Panel from the Windows Explorer menu.
2. Select Network.
3. Click the Add bar.
4. Select Client and click Add.

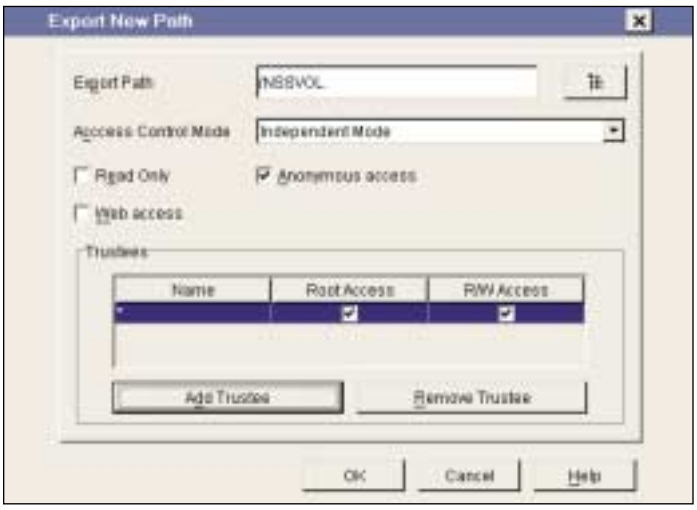

Figure 5. When you export a volume or directory for UNIX users, you specify trustees—UNIX client machines—for which you want to allow access. An asterisk indicates that all UNIX computers running on the network are trustees.

No Regrets

If you select either the Local or Domain option and later decide that you have selected unwisely, don't worry about it. You can change your selection without having to reinstall Native File Access for Windows by taking the following steps:

1. Using a standard text editor, open the CIFS.CFG file on the NetWare server running Native File Access for Windows. (The Native File Access for Windows installation program creates this file in the SYS:\ETC directory.)
2. Locate the -AUTHENT entry.
3. Change the -AUTHENT entry from AUTHENT DOMAIN to AUTHENT LOCAL, or vice versa.

Share and Share Alike

The Native File Access for Windows installation program also enables you to specify NetWare volumes and folders that you want to make available to Windows users as share points. (*Share point* is Microsoft's term for shared directories, folders, and files in a Windows environment.)

Users that are using Windows 2000, NT, and 98 can share files running on their local computers with other users. That is, these users can engage in peer-to-peer file-sharing. Similarly, you can designate files on a Windows NT or 2000 server as share points.

Of course, you don't have to specify share points. If you don't, Native File Access for Windows displays all mounted volumes on the NetWare server. That is, all NetWare volumes become sharable. If you do specify share points, only the share points you specify are sharable.

By enabling share points on your company's NetWare server, Native File Access for Windows is "making this NetWare server play in that Windows environment," Isaacson explains. Thus, Native File Access for Windows is ensuring that users who are accustomed to a Windows environment won't notice when you add a NetWare server to that environment.

Windows users can see and access these share points when they select the NetWare server through Windows' Network Neighborhood just as they can see and access share points on a Windows server. To add and delete share points after you install Native File Access for Windows, you edit the CIFS.CFG file. Alternatively, you can type the following command at the NetWare server console to add a share point:

CIFS SHARE ADD [*local path*] [*share name*] [*connection limit*] [*comment*]

To remove a share point, type the following command at the server console:

CIFS SHARE REMOVE [*share name*]

NATIVE FILE ACCESS FOR UNIX: DEJA VU ALL OVER AGAIN?

If your company already provides UNIX users with access to files on NetWare servers, the following discussion may sound somewhat familiar to you. After all, Native File Access for UNIX is a version of another Novell product that provides access to NetWare for UNIX users: NetWare NFS services. Native File Access for UNIX includes two components from NetWare NFS Services: the Network Information Services (NIS) server component and NFS server component.

NIS is a yellow-pages–style directory that many UNIX implementations use. UNIX-based computers use NIS to find information about the local network. These client computers can also use remote procedure calls (RPCs) to obtain information from NIS servers running on remote networks.

Although Native File Access for UNIX includes NIS and NFS server components, it does not include a third component that is included with NetWare NFS Services—the NFS Gateway component. This component enables client computers running Novell client

Setting UNIX Passwords

Although the Native File Access for UNIX migration utility can migrate users from UNIX Network Information Services (NIS) servers to eDirectory, this utility cannot migrate these users' UNIX passwords. Therefore, you must manually set UNIX passwords in eDirectory.

Before you can perform this task, you must configure the UNIX NIS server from which you migrated user accounts to act as a UNIX client computer. To do so, you perform the following steps:

1. Launch ConsoleOne running on the Native File Access for UNIX server and log in. (The Native File Access for UNIX snap-in module must be installed in ConsoleOne.)
2. Right-click the server running Native File Access for UNIX in ConsoleOne's main menu, and then select Properties.
3. Select the Directory Access tab.
4. Click the checkbox to enable the NIS client access to this server.

You can then log in to the server running Native File Access for UNIX from this UNIX client computer.

To set a user's UNIX password in eDirectory, log in either as the user for whom you want to set the password or as a user with Root access. (In UNIX-based systems, users with Root access are users who have supervisor rights.) You then run the native UNIX password set utility—yppaswd—to set the user's password.

Keep It Simple

Native File Access for Macintosh and Native File Access for Windows require users to use simple passwords. Like traditional NetWare passwords, simple passwords are stored in User objects in Novell eDirectory. However, NetWare passwords are stored using a one-way hash algorithm, and simple passwords are stored securely in a retrievable format using Novell Secret Store technology.

Simple passwords are necessary because Macintosh and Windows client computers cannot use hashed passwords natively. To use these hashed passwords, these client computers must run Novell client software.

You can use ConsoleOne to create simple passwords for each user separately. You simply complete the following steps:

1. Right-click a User object in ConsoleOne.
2. Click Properties, and then click Login Methods.
3. Check the Assign Simple Password check box, and enter a password in the provided field.

A UTILITY FOR MANAGING SIMPLE PASSWORDS

You can also use the Native File Access Pack Simple Password Management utility to create simple passwords for each user separately. (This utility is hereafter called the *Simple Password Management utility*.) The installation programs for the Native File Access for Macintosh and Native File Access for Windows automatically install this utility in Novell Remote Manager. You can access the Simple Password Management utility by selecting NFAP Security under the Manage eDirectory option in Novell Remote Manager.

The Simple Password Management Utility is actually two utilities in one: the Single-User Simple Password Set utility and the Multi-User Simple Password Set utility. As its name suggests, the Single-User Simple Password Set utility can help you assign simple passwords to individual users. You can use this utility to perform this task in one of the following ways:

- You can specify the user's username and context in the Simple Password Set utility's Username.Context field and then click Set. The Single-User Simple Password Set utility then creates a password for the user named in this field. (See Figure 3 on p. 14.)
- You can specify a username and context in the Username.Context field and then type a new password into the utility's New Password field. When you click Set, the Single-User Simple Password Set Utility then sets this simple password for the user. (See Figure 3 on p. 14.)

Also as its name suggests, you can use the Multi-User Simple Password Set utility to set simple passwords for multiple users. This utility includes the following options for setting simple passwords:

- NDS Context. When you type an eDirectory context in the NDS Context field and click the Start button, the Multi-User Simple Password Set utility creates a simple password for each eDirectory User object in the specified context. (See Figure 3 on p. 14.)
- Traverse Entire Tree for User Objects. When you check the Traverse Entire Tree checkbox, and then click the Start button, the Multi-User Simple Password Set utility creates a simple password for each eDirectory User object in the eDirectory tree.
- User Supplied Password. When you check the User Supplied Password checkbox and then enter a simple password in the field provided, the Multi-User Simple Password Set utility sets this password for the users you have selected. (See Figure 3 on p. 14.) You use the NDS Context or Traverse Entire Tree for User Objects options to select users.
- Process Script File and Generate Script File. These options enable you to create a script that assigns simple passwords according to your company's particular password policy.

ONE PASSWORD IS SIMPLER THAN TWO

Although simple passwords are technically different from NetWare passwords, "it actually works out better if these passwords are the same," Douglas Phillips, a senior software engineer for Novell, explains. That is, it works better for both you and users if users' NetWare password and simple password are the same password.

When these two passwords are the same, Native File Access for Macintosh and Native File Access for Windows support the native password-change features on Macintosh and Windows computers for both simple passwords and NetWare passwords. That is, these Native File Access components keep simple passwords and NetWare passwords in sync.

When these passwords are not the same, on the other hand, Macintosh users cannot use the Macintosh password-change feature to change either password. Furthermore, Windows users can change only their simple password using Windows native password-change features. To change their NetWare password, Windows users must use a computer that is running Novell client software.

Synchronizing simple passwords and NetWare passwords simplifies life for you and users because users need to remember only one password rather than two. Users are less likely to forget that password and are, therefore, less likely to call you for help.

SIMPLE PASSWORD SYNCHRONIZATION FOR MACINTOSH USERS

If you want to set simple passwords that are the same as NetWare passwords for Macintosh users, you have two options:

- You can set each user's password individually using ConsoleOne or the Single-User Simple Password Set utility.
- You can use the CLEARTEXT option to enable users to set their own simple passwords.

The CLEARTEXT option is a Native File Access for Macintosh feature that enables you to send clear text passwords across the network. Using this option, Native File Access for Macintosh prompts Macintosh users to provide their NetWare login credentials when they log in to the network. After the NetWare password is verified in eDirectory, Native File Access for Macintosh automatically stores that password as a simple password.

Obviously, the CLEARTEXT option isn't an option if you are concerned about someone capturing Macintosh users' passwords over the network. Even if you feel certain that users' passwords won't be compromised, however, Novell recommends that you use the CLEARTEXT option for the shortest period of time possible. As soon as all of the Macintosh users on your company's network have created simple passwords by logging in using the CLEARTEXT option, you should disable that option.

continued on page 23

continued from page 22

To enable the CLEARTEXT option on a server running Native File Access for Macintosh, type the following command at the server console: LOAD AFPTCP.NLM CLEARTEXT. To disable the CLEARTEXT option, unload the AFPTCP.NLM, and reload the AFPTCP.NLM without the CLEARTEXT option.

SIMPLE AND SECURE

After you set simple passwords, Macintosh and Windows users can use their simple password and NetWare username to authenticate to a NetWare server using native Macintosh and Windows security methods. For example, when Macintosh users use these credentials to authenticate to a NetWare server running Native File Access for Macintosh, their Macintosh client computers use Apple's native random number exchange algorithm to transmit these credentials securely to the NetWare server. Windows client computers, as mentioned above, use Windows' native RC4 encryption.

Native File Access for Macintosh and Native File Access for Windows then use Novell Modular Authentication Service (NMAS) to verify those credentials in eDirectory. (NMAS integrates with eDirectory to provide network access using a variety of authentication methods.) NMAS 2.0 is automatically installed when you install Native File Access Pack components. If the server upon which you are installing Native File Access Pack components is already running a previous version of NMAS, the Native File Access installation program automatically updates that previous version to NMAS 2.0. (For more information about NMAS, see "NMAS: It's What Spy Movies Are Made Of," *Novell Connection,* Feb. 2000. You can download this article from www.ncmag.com/past.)

software to access files on UNIX servers and, therefore, isn't a good fit for Native File Access for UNIX. The raison d'etre for Native File Access for UNIX (and other Native File Access Pack components) is, after all, to enable users to access NetWare servers without having to use Novell client software.

The Native File Access for UNIX NIS server component enables NetWare to emulate NIS services running on UNIX-based computers. Also, in Native File Access for UNIX, the NIS server and NFS server components work together, as they do in NetWare NFS services. These components work together to enable UNIX-based client computers to natively access files on NetWare.

As you know, Native File Access for UNIX enables these computers to access files on NetWare 6 and NetWare 5.1 servers. NetWare NFS Services enables this access for NetWare 5.1 and earlier versions of NetWare. (NetWare NFS Services 3.0 Support Pack 2—the latest version of NetWare NFS Services—runs on NetWare 5.1 with Support Pack 3 or the International release of NetWare 5.1. NetWare NFS Services 2.4 and 2.3 run on NetWare 5.0 and NetWare 4.x, respectively. For more information about NetWare NFS Services, visit Novell's web site at www.novell.com/products/nfs/details.html.)

Like NetWare NFS Services 3.0 Support Pack 2, Native File Access for UNIX supports any UNIX implementation that supports NFS protocol versions 2 or 3. Specifically, when used with the traditional NetWare file system, Native File Access for UNIX supports only NFS 2 because this file system supports only NFS 2. When used with NSS, on the other hand, Native File Access for UNIX supports NFS 2 and 3 because NSS supports NFS 2 and 3.

Novell has tested Native File Access for UNIX with Linux, Solaris Intel, SPARC, UnixWare, FreeBSD, and AIX. However, Novell software engineering manager Annapurna Lolla points out that because Native File Access for UNIX contains no platform-specific code, Native File Access for UNIX "should ideally work with any flavor of UNIX."

Native File Access for UNIX Gives eDirectory Its Full Support

You set up and manage the Native File Access for UNIX NIS server and Native

The Ideal Guest

As you may know, Macintosh users can access AppleShare networks without having to provide login credentials. They simply log in as Guest. To ensure that Macintosh users can log in as Guest when accessing a Novell Native File Access for Macintosh server, you must create a Guest account. To do so, complete the following steps:

1. Using ConsoleOne on the administrator workstation, create a User object named *Guest*. (An administrator workstation is a Windows 2000, 98, 95, or NT 4 workstation that is running Novell client software for Windows, ConsoleOne, and Novell International Cryptographic Infrastructure (NICI) 1.5.7 or above. ConsoleOne uses NICI to provide password administration for Native File Access for Macintosh and Native File Access for Windows.)
2. Double-click the Guest object, and then select Rights to Files and Folders.
3. Assign rights to the files and folders that you want to make available to users who log in as Guest.
4. Click Restrictions, and uncheck the Allow User to Change Password box.
5. Using a text editor (such as Notepad), add the complete eDirectory context of the Guest User object to the CTXS.CFT file, which is located in the NetWare server's SYS:\ETC directory. (The CTXS.CFG file is a context search file that you create in this directory. For more information about context search files, see "Putting Things in Context" on p. 16.) Any Macintosh user can then log in using the Guest username without a password to access the files to which you have assigned the Guest user rights.
6. Load the Native File Access for Macintosh NetWare Loadable Module (NLM) with the Guest option enabled. To load this NLM, you type the following command at the server console:

```
LOAD AFPTCP GUEST
```

File Access for UNIX NFS server components separately through the Native File Access for UNIX snap-in module for ConsoleOne. (You can also set up and manage these components by using a text editor to edit Native File Access for UNIX configuration files). Setting up and managing these components is relatively simple in part because Native File Access for UNIX extends the eDirectory schema.

To be more specific, Native File Access for UNIX (like NetWare NFS Services 3.0 and above) extends the eDirectory schema to include NIS objects and attributes. For example, Native File Access for UNIX extends User objects to include NIS user attributes, such as the UNIX user identification (UID) number that uniquely identifies UNIX users. (The UID also identifies ownership of files and directories on UNIX-based systems.)

Native File Access for UNIX and NetWare NFS Services 3.0 and above also extend Group objects to include NIS group information—such as the UNIX group identification (GID) number. Because UNIX user and group profiles are stored in eDirectory User and Group objects, you can manage UNIX users and groups in only one directory rather than in two. You then manage those users and groups in eDirectory using the Native File Access for UNIX snap-in module for ConsoleOne.

In contrast, with NetWare NFS Services 2.3 and 2.4, you have to create User and Group objects in eDirectory and separate user and group objects in NIS. You then have to map these two sets of objects so that users can access NIS information on NetWare servers using UNIX-based client computers.

Move It, Don't Lose It!

As you know, eDirectory runs on several UNIX-based servers, including Linux. You can therefore use eDirectory to create user accounts on these servers, rather than using NIS. Using eDirectory to manage Linux users is arguably the most practical solution, particularly if your company's Linux users are accessing NetWare servers.

However, suppose your company's network already includes NIS domains running on Linux servers. If you want the Native File Access for UNIX NIS server to provide the NIS services that are currently running on these Linux servers, you can use the Native File Access for UNIX migration utility. (See Figure 4 on p. 18.)

This migration utility creates an eDirectory container object for each NIS domain that you want to migrate to a Native File Access for UNIX NIS server. (NIS domains are administrative segments that exist in a local networking environment.)

Within these Domain objects, the migration utility creates two related container objects: domainname_U and domainname_G. Domainname_U contains UNIX users, and domainname_G contains UNIX groups.

For example, suppose your company's network has a network segment—the administrative domain—that includes the users on the top floor of your company's headquarters. Further suppose that information about this domain is contained in the following two NIS maps:

- The Passwd map
- The Group map

The Passwd map is an NIS map that contains details (such as users' UID, username, and UNIX password) about UNIX users in the administrative domain. Similarly, the Group map contains information about groups in the administrative domain. (NIS maps are text files that contain information about a particular NIS domain.)

In this example, the migration utility would create a Domain container object in eDirectory for the administrative domain. Within that Domain object, Native File Access for UNIX would then create a domainname_U and a domainname_G container object.

During the migration process, the migration utility would search eDirectory for User objects that correspond to users in the administrative domain. The migration utility would read these administrative domain users from the Passwd map. If the migration utility found eDirectory users who corresponded to these administrative domain users, it would update those users' eDirectory User objects with UNIX information (such as the users' UID). If the migration utility did not find corresponding eDirectory users, it would create eDirectory User objects for these users in the domainname_U container.

Similarly, the migration utility would search for eDirectory Group objects that

corresponded to administrative domain groups listed in the Groups map. The migration utility would then either update the existing Group objects in eDirectory or create Group objects in eDirectory within the domainname_G container.

The migration utility would also create a User object called *Nobody* in the domainname_U container and a Group object called *Nogroup* in the domainname_G container. These objects enable anonymous file access for UNIX users.

Everything But the UNIX Passwords

Although the migration utility migrates UNIX user accounts in NIS to eDirectory, this utility does not migrate the UNIX passwords from those accounts. Before you migrate UNIX users to eDirectory, you should use a text editor to remove the password field from user entries in the NIS Passwd map.

In fact, if you are migrating these users to NetWare 5.1, you must perform this task. If you do not remove passwords from the Passwd map with Native File Access for UNIX on NetWare 5.1, the UNIX Password attribute in eDirectory will not be valid, and UNIX users will not be able to log in. This limitation does not apply to Native File Access for UNIX on NetWare 6 servers.

After the migration utility creates (or updates) user accounts in eDirectory, you can then use yppaswd—the NIS client password utility—to set UNIX passwords for these users. (For information about how to perform this task, see "Setting UNIX Passwords" on p. 20.) UNIX users can then use these passwords to access directories and files on NetWare. Before those users can access these directories and files, however, you must make those directories and files available to UNIX users by exporting the directories and files. To export these directories and files, you use the Native File Access for UNIX snap-in module for ConsoleOne. (See Figure 5 on p. 20. For more information about how you can export directories and files for UNIX users, read "Exporting 101" on the *Novell Connection* web site www.ncmag.com.)

CONCLUSION

Because you have experienced NetWare's reliability firsthand, you probably aren't surprised that NetWare draws praises from the IT community. For example, NetWare garnered praises in the 2001 VAR Business Annual Report Card Awards. NetWare is the overall winner of the Enterprise Operating Platform category, taking top marks in product quality, among other things. (For more information about the 2001 VAR Business Annual Report Card awards, visit www.varbusiness.com/arc.)

On top of this reliability, NetWare now offers the ability to store and secure data for all of the users on your company's heterogeneous network without having to bother with Novell client software. With Native File Access Pack components, users can have their client computer cake in any of three flavors—Macintosh, Windows, and UNIX—and your company can feed on a steady diet of well-done NetWare stability and reliability.

Cheryl Walton works for Niche Associates, which is located in Sandy, Utah.