Global Information Assurance Certification Paper

Implementing a Strong Password Filter in a NetWare Environment

Damien Dinh

Practical version 1.3
March 11, 2002

Abstract

Weak passwords create a large hole in any "defense in depth" policy. Implementing a password filter in the NetWare environment is challenging because there is no strong password filter in Novell Directory Services (NDS). This paper discusses two client-based solutions, and documents a process to implement a strong password filter in the NetWare environment.

Introduction

The practice of combining many security tools, including router ACLs, VPNs, firewalls, host and network based intrusion detection systems, encryption, OS hardening methods and strong passwords, describes "defense in depth." The use of a password is the most fundamental layer of protection. To authenticate to our network, users must first input their user name and password into the Novell Client32 logon screen. At this point, the use of a weak password provides a hole in our security in depth policy.

Through the SANS Security Essentials training I have developed a great understanding and an urgency in implementing the use of a strong password in our organization. It has proven to be a difficult task to centrally implement a password filter in our NetWare environment because Novell did not build a strong password filter into the Novell Directory Services (NDS).

The purpose of this paper is to document the process I used to implement a strong password filter in the NetWare environment. There are four basic steps in this process:

1) Create a "bare bone" image for each version of Windows.
2) Use ZENworks to create an Application Object.
3) Use ConsoleOne to configure an Application Object in NDS.
4) Deploy the Application Object to implement the strong password filter.

Strong Password Filter Tools

During our preliminary research, our security group identified two client-based solutions, but found no tool that is fully integrated into NDS. Before selecting either filter we consulted a Novell system engineer, who verified that Novell does not offer an NDS-based password filter. He also explained that the reason a server-based solution is not feasible is that Client32, which runs on Windows workstations, hashes the password before passing the hash to the server.

There is no way for the server to reverse the one-way hash to validate any characters. Therefore, it cannot have a mechanism or tool that resides in NDS to validate any strong password rule, such as differentiating between an upper or a lower case alphabetic character, or a special character or a numeric character, etc. The white paper with technical support is provided in the bibliography (**1**). As a result of this finding, we evaluated the two client-based solutions: dirXperts and Connectotel.

Both dirXperts and Connectotel are approved by Novell. And both products operate on the client side, meaning a piece of the product is installed on the user's workstation. However, Connectotel (**2**) is more developed than dirXperts in two ways.

One, it has an administration software that can be integrated into NWADMIN32 or ConsoleOne as a snap-in. As you may already know, NWADMIN32 and ConsoleOne are Novell tools used to centrally administrate the NDS database which contains all network resources (**3**). ConsoleOne is the latest version in the form of a JAVA applet. As a result, you can set the strong password parameters centrally. DirXperts does not have this snapin.

Two, it integrates the password filtering client into the Novell Client32 installation which resides on the user's operating system. This allows the Connectotel client to pass the user's password to the administration software before the password is hashed by Client32. Therefore, a strong password character rule defined in the administration software on the NDS side can differentiate between an upper or a lower case alphabetic character, or a special character, or a numeric character, etc. DirXperts is not integrated into Client32.

Connectotel seems to be the solution we were seeking to centrally manage a strong password filter. So why did we choose dirXperts over Connectotel? The obvious reason is dirXperts is free. Licensing Connectotel would cost thousands of dollars for our enterprise network. In addition, I have found a way to deploy dirXperts easily with ZENworks 3.0. Even though cost is a big factor in our choice, the ease of deployment helped cement our decision.

Deploying DirXperts

DirXperts is a collection of tools, which includes LDAP Contextless Login, Message of the Day, NDS Explorer, and Password Restrictions (**4**).

In this paper, I will only use the Password Restrictions tool. This tool uses LgnPwW32.DLL to validate a password rule beyond the rule set defined in the Novell Directory Services. NDS can require a password, minimum length, force periodic changes, and require unique passwords, but does not enforce types of characters because it only sees hash differences (**5**).

LgnPwW32.DLL rule set are as follows (**6**):

- **Minimum numeric characters**: specified number of digits ([0-9])
- **Minimum alphabetic characters:** the password must contain at least a specified number of alphabetic characters ([a-z, A-Z])
- **Minimum uppercase characters:** the password must contain at least a specified number of uppercase characters ([A-Z])
- **Minimum lowercase characters:** the password must contain at least a specified number of lowercase characters ([a-z])
- **Minimum special characters:** the password must contain at least a specified number of characters that are neither alphabetic nor numeric ([!, @, #, $, ...])
- **Maximum consecutive characters:** the password may not contain the same character more than a specified number of times in a row.
- **Maximum repeated characters:** the password may not contain the same character more than a specified number of times in the entire password.
- **Maximum sequential characters:** the password may not contain a series of sequential characters longer than a specified length.
- **Maximum characters:** the password may not be longer than a specified length.

I have developed four basic steps to deploy dirXperts throughout our network:

Step1

Create a "bare bone" image for each version of Windows

- Install Windows on a test pc with only the video and network interface card installed. Please follow the minimum hardware requirements for each version of Windows (**7**).
- Do not install fixes or service packs.
- Keep it off the network until use.
- Load only basic drivers for the NIC and video card (VGA is sufficient).
- Install the latest Novell Client32 on the OS. You can use any current version for each respective Windows version. 3.32 for 9.x, 4.8x for NT/2000/XP. Please go to this link for the downloads (**8**):
- Defrag the file structure. Go to this link for documentations on all version of windows (**9**):

- Create a binary image of each OS for backup. I used Symantec Ghost (**10**). You can use any disk imaging tool of your choice. If you are not familiar with these types of tools, basically it allows you to save a binary image of an operating system from the whole hard disk or a partition. Then you can use this image to restore the operating system to the condition from the time you made the image.

  This has helped me save time in the past when something goes wrong during the Application Object creation process. I was able to re-image the operating system in five minutes as oppose to rebuilding the operating system from scratch which may take an hour.

- Repeat the Step 1 process for each version of Windows (9.x, NT-2000, and XP).

Step 2

Use ZENworks to create an Application Object

- Download dirXperts (**11**):

- From the test pc, login to your Novell network.

- Copy dirXperts to the test pc.

- From the test pc map a drive to the directory that contains snapshot.exe. It is in the \\server\sys\public\snapshot directory path by default.

- Execute snapshot.exe on the test pc while in Windows.

  (You can run it from a mapped network drive as shown in Figure 1.)

  (Explanation: By executing snapshot at this point, it will reference the current file system, all files, and the registry.)

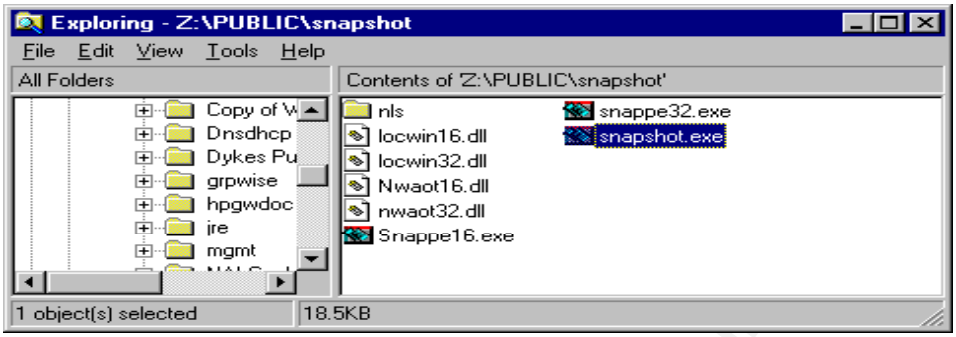

Figure 1

- Choose the "**Custom**" option.
- Keep the "**snAppShot Default Settings**" and click next. See figure 2.

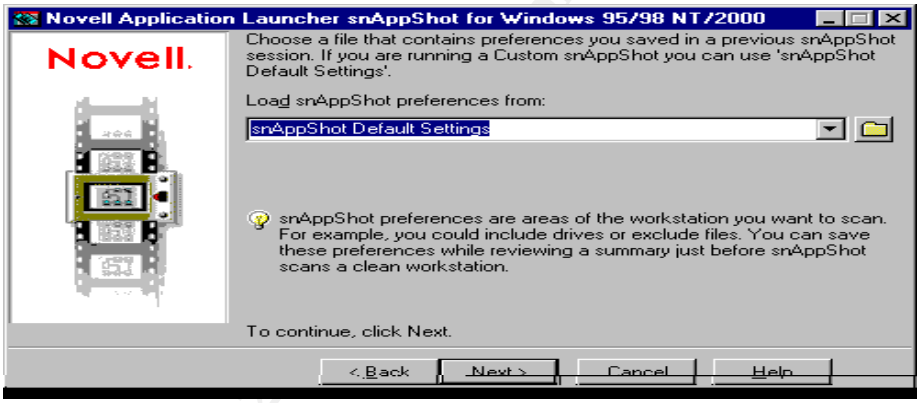

Figure 2

- Give the NDS Application Object a unique name. See figure 3.

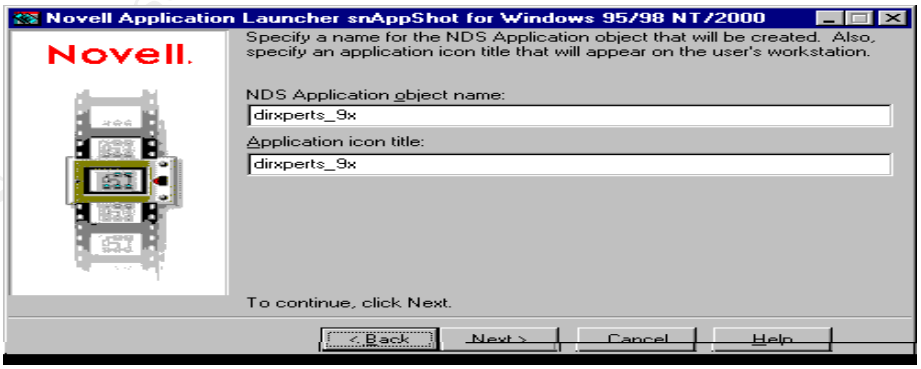

Figure 3

- Type in the UNC path to the server location where the configuration files (.fil and .aot) will be stored. Use the actual server name, volume name, and directory name. The default directory is

\\server\apps\nal_apps.

(Note: If you have NetWare clustering naming convention, do not use that naming scheme. It is not consistent in resolving the name when you run the Application Object. Instead, use the real server name, volume name, and directory.) See figure 4.

Figure 4

- Type in the same UNC path but this time include the ".AOT" file name. See figure 5.

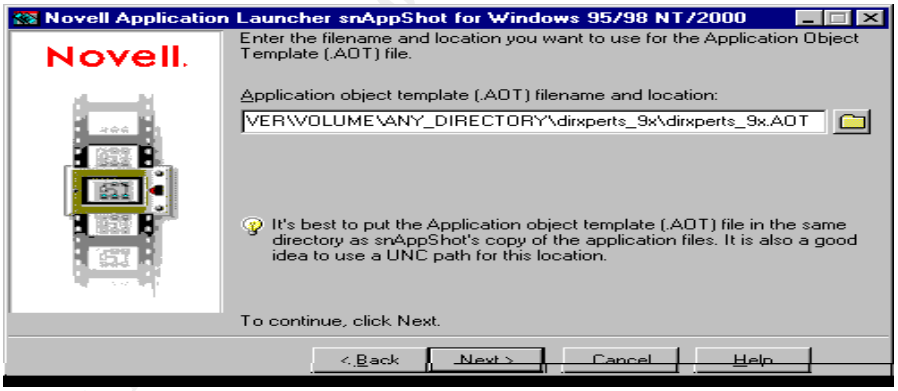

Figure 5

- Select all options except the "**Windows Shortcuts**" options:

This will prevent most users from having easy access to the configuration utility so they can't change or manipulate the password filter. See figure 6.

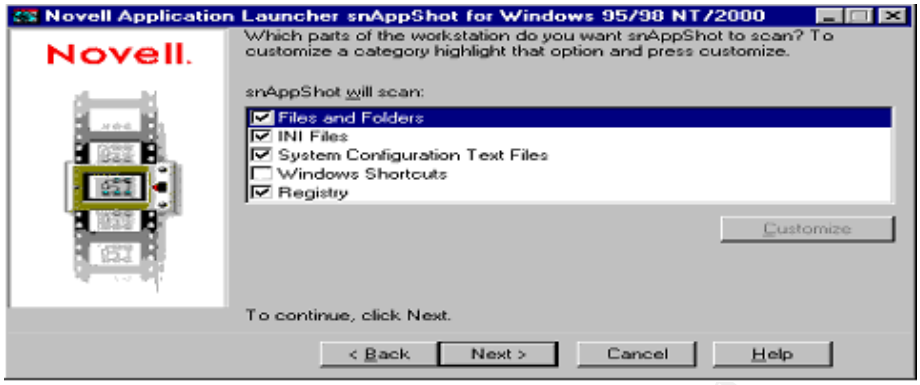

Figure 6

- Click “Next” a couple more times and it will start scanning. When it is done, the window will look like figure 7.

  (Important note: Remember to leave this window open while performing the next step.)

Figure 7

- Install dirXperts when Snapshot finishes.

- Uncheck “**Message of the Day**” and “**LDAP Contextless Login**” if LDAP is not implemented in your Novell Environment. Please see figure 8.

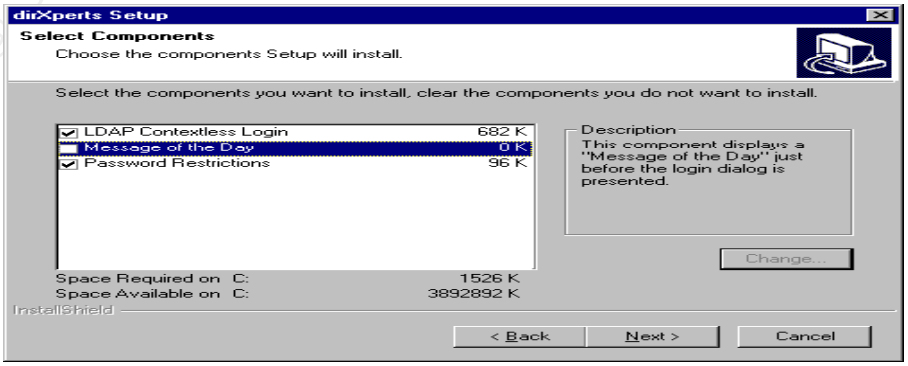

Figure 8

- Configure the password parameters that are to be implemented. The HIPAA standard is six character or more, at least one upper-case, at least one number, and at least one special character (**12**).

  The SANS standard is a little more detailed in that they added password aging, no dictionary words, and no incorporation of user's name (**13**).

- Select the parameters. See figure 9.

  Note: You should choose parameters that are consistent with your organization's password policy.

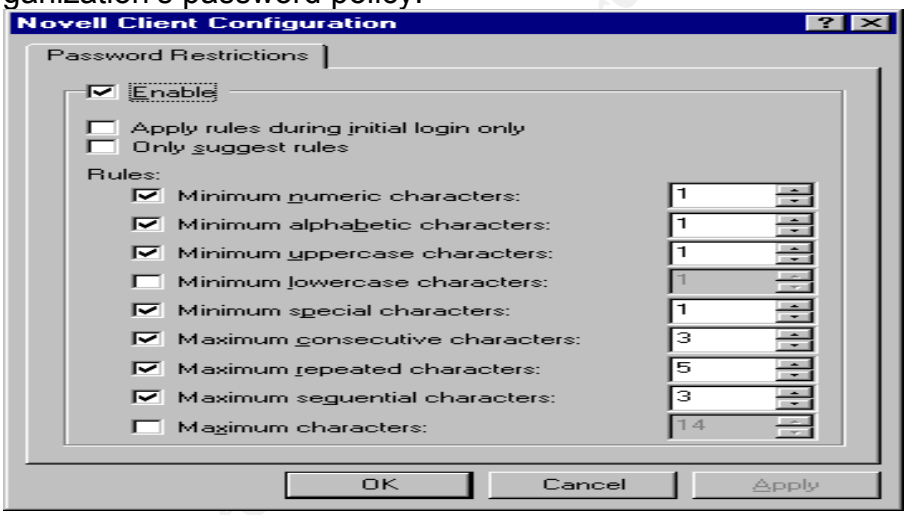

Figure 9

- Clicking "Apply" to commit parameters.

- Delete all dirXperts shortcut out of the Start Menu and empty the Recycle Bin. In windows NT/2000, check all profiles.

- Reboot the test pc with snapshot still running on the desktop.

- After the reboot, snapshot will ask you to resume. Click Yes. See Figure 10.

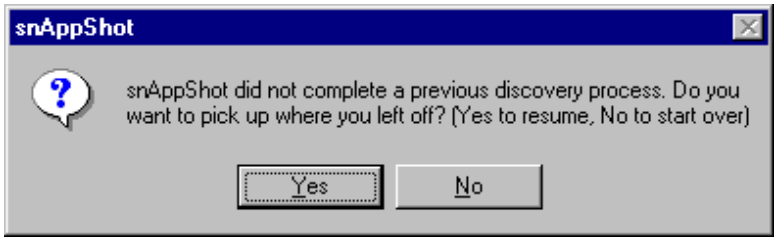

Figure 10

- When snapshot starts up choose the “Copy and create if does not exist” option for all three. Please see figure 11.

  Note: The “Copy or Create if does not exist” option will insure no overwriting any existing registry entries or files when this package is implemented.

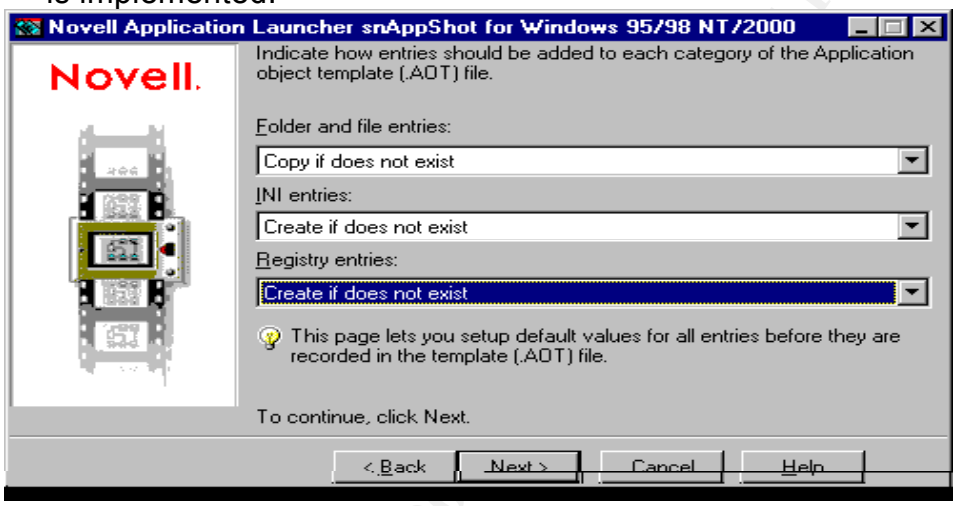

Figure 11

- Click next a couple more times to take the default setting. It will scan the OS for the difference to the “bare bone” snapshot performed earlier.

Step 3

Use ConsoleOne to configure an Application Object in NDS

- Open ConsoleOne from your desk workstation.

- Right click on the container where this Object will reside. Choose **New** and choose from the sub-menu, **Application object**. A wizard will pop up at this time.

- Choose **Using an .aot/.axt file** option. Click next. Please see figure 12.

  Note: If you have ZENworks 3.0, you must use ConsoleOne to perform this task. Using NWAdmin32 will corrupt your Application Object and .aot and .fil files.

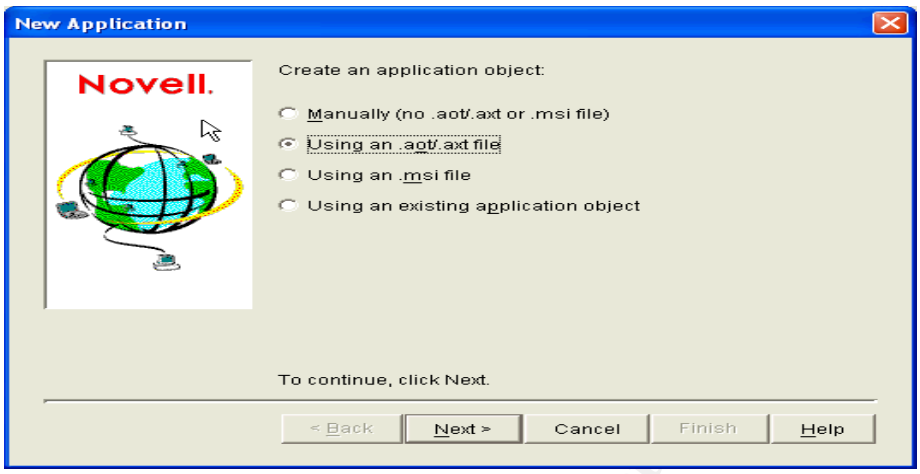

Figure 12

- Type in the UNC path to the .aot files from step 3 and make sure to include the full name of the .aot file and file extension. Please see figure 13.

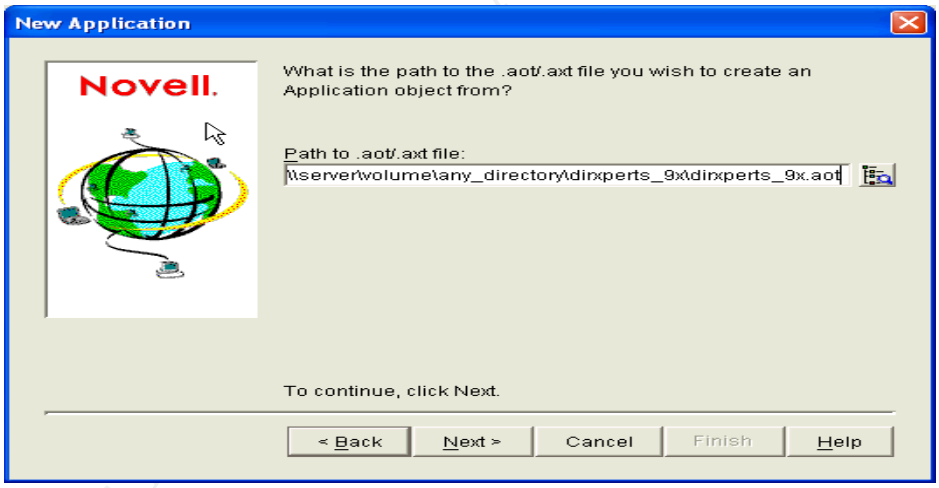

Figure 13

- Click **Next** twice. Then click finish on the summary window of the wizard. The Application Object should populate in the container that you have chosen earlier.

- Locate and go into the properties of the object you just created.

- Go to the “Distribution Options” tab.

- Click the down arrow and choose “Icons/Shortcuts.”

- Delete any shortcuts (This will double check short cut deletion noted in Step 2, pg. 8).

- Click the down arrow on the “Distribution Options” tab again.

- Choose “Registry.”

- To have a clean universal Application Object that you can install on any client PC with the same Windows version, you need to **delete** the following Registry keys:

For Windows 9x

1. All sub keys under HKEY_CURRENT_USER. (if there are any)
2. HKEY_LOCAL_MACHINE\System. (Delete the whole System sub key)
3. HKEY_LOCAL_MACHINE\Software\NetWare (Delete if exist. This entry is cause by the Novell Application Launcher caching after a reboot.)
4. KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion \Uninstall. This will prevent the user from uninstalling dirXperts through the “Add/Remove Programs” in the Control Panel.
5. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Sessio n Manager\Environment]"Path"=

For Windows NT/2K

1. HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVers ion\Uninstall (Important: Prevents the user from uninstalling dirXperts through the “Add/Remove Programs” in the Control Panel.)
2. HKEY_LOCAL_MACHINES\Software\Microsoft\Windows NT (Windows profile cache when rebooted.)
3. HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\Explorer
4. HKEY_LOCAL_MACHINES\Software\Novell\LIBRARY (This is only the user context cache.)
5. HKEY_LOCAL_MACHINES\Software\Novell\NetWareWorkstation (The Client32 will keep a caching of NetWare servers that is talks to during the network link.)
6. HKEY_LOCAL_MACHINES\Software\Novell\Workstation Manager (This entry will cache every time the PC reboots. It only does this if you load Workstation Management option selected during the Client32 installation)
7. HKEY_LOCAL_MACHINES\HARDWARE (This is machine hardware specific when rebooting.)
8. HKEY_LOCAL_MACHINES\NDPS (This entry is cause by the Novell NDPS printing agent that is loaded with the Client32 installation. If you install the client without this option then the registry key will not be created.)

9. HKEY_LOCAL_MACHINES\SYSTEM (This entry is machine specific when reboot occur. Windows is directory caching and DHCP configuration.)

- Click the down arrow on the “Distribution Options” tab again.
- Choose “Application Files.”
- Delete all uninstall.exe and setup.exe files. (This will prevent the user from performing an uninstall)
- Select all executable files (.exe, .com, .dll etc). (You can do this by holding down the CNTRL key when clicking on the files from the list.) (Figure 14)
- After all the executable files are highlighted, choose from the “Selected Item(s) Options” drop down list: “Copy if newer version.” (Figure 14) This will ensure newer executables will not be over written.

Important: If this is not done properly, Windows will have the tendency to crash as a result of this distribution.

- Always perform test pushes before the actual deployment. Naturally, there are always exceptions that a crash will occur. In that case, you can perform a .dll back date which is referenced here:

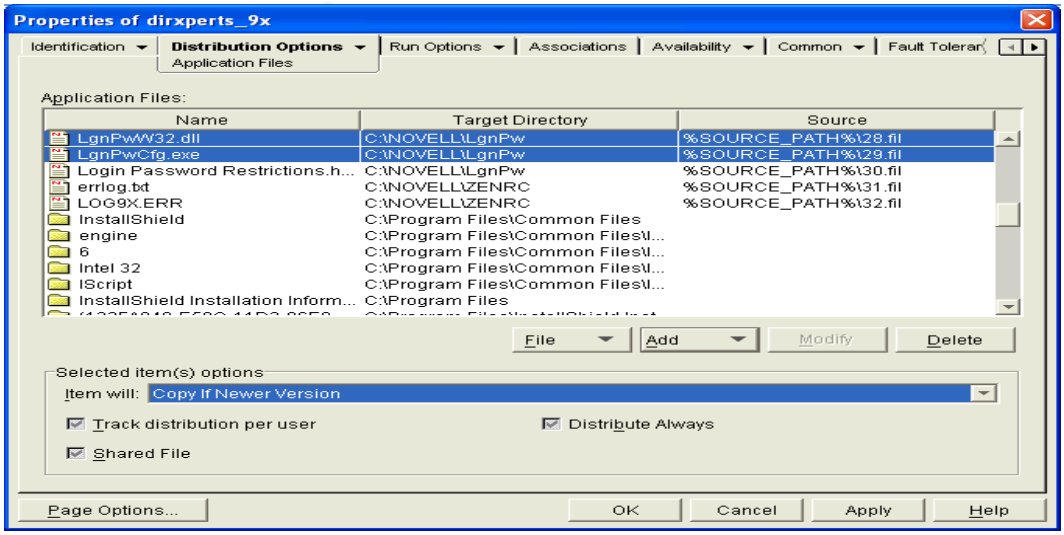

Figure 14

Note: Please remember to create a package for each operating system and follow the same configuration standard described in the above steps for both.

Step 4

Deploy the Application Object to implement the strong password filter

- Open ConsoleOne from your desk workstation.
- Locate and open (viewing the properties) the password filter application Object you created. Figure 15 shows the properties window.
- Click on the **Associations** tab and choose the method of delivery. Then click **Add** to associate the users, group, or container that you want to push this package. The default is **App Launcher**. This option only lets you install manually from the user's PC. The automatic installation technique is **Force Run** which will install every time a user logs into the network.

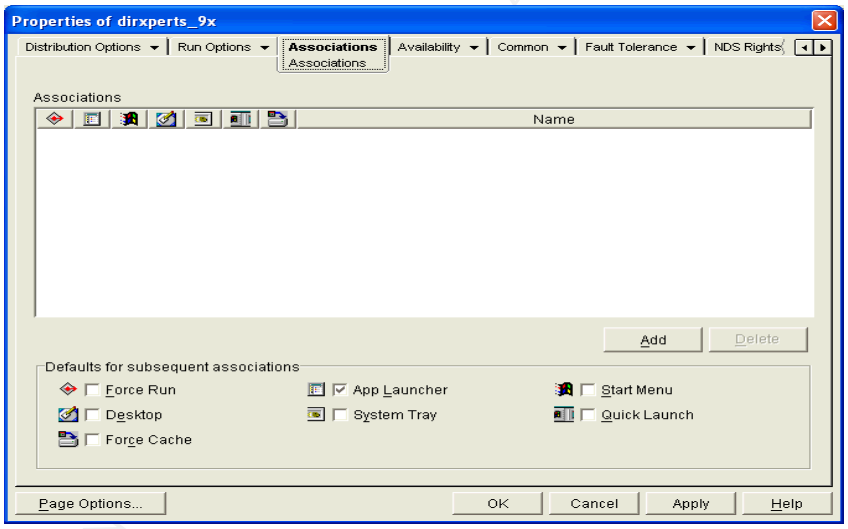

Figure 15

- To prevent this from running every time, you can click to check mark **Run Application Once** under the **Run Options** tab. Please see Figure 16.

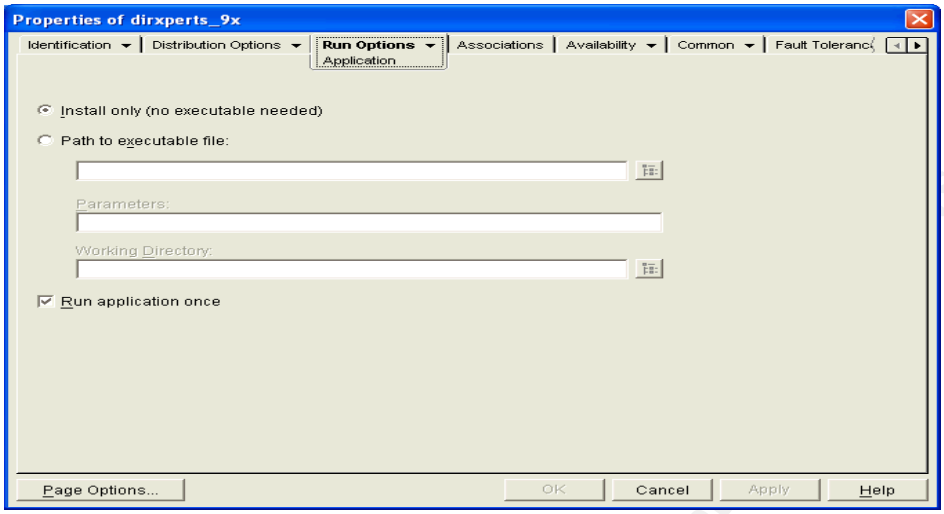

Figure 16

Summary

Deploying dirXperts in a Netware environment via ZENworks is an out of pocket cost-free password filtering solution. Of course, there is another solution, Connectotel, which has great features but it is a high cost solution. We hope Novell will eventually develop a global product that is built into NDS but in the mean time, we need have something in place. That's why I have documented in a step-by-step process on how to put this package together and to ultimately deploy it using ZENworks. I believe, in the premise, that a strong password policy will strengthen the weak link in our network. With that said, I like to end with the following quote which says it all: *"Password - a weak link in the secure digital environment."* (*Source: Ware, Karl, 4/4/01*) (**14**).

References

1) Lee, Rich. "Understanding the Role of Identification and Authentication in NetWare 4." October 1994, URL: http://developer.novell.com/research/appnotes/1994/october/02/index.htm (12 Feb. 2002).

2) http://www.connectotel.com/ppm/ (12 Feb. 2002).

3) Text: Novell, Inc., Netware 5 Administration, course 560. Orem, Utah: Novell, Inc., 1999. Section 1 p.27-29.

4) EINFO@novell.com, "Novell TechNews" July, 2000, URL: http://archives.neohapsis.com/archives/novell-technews/2000-q3/0000.html (15 Feb. 2002).

5) http://www.esu10.k12.ne.us/lanmanage/meetings/sept00/LDAPContextlessLogin.htm (10 Mar. 2002).

6) http://www.novell.com/coolsolutions/zenworks/downloadables.html (17 Mar. 2002).

7) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/support/Default.asp (18 Mar. 2002).

8) http://support.novell.com/filefinder/6385/index.html (22 Mar. 2002).

9) http://www.computerhope.com/software/defrag.htm (22 Mar. 2002).

10) http://enterprisesecurity.symantec.com/products/products.cfm?productID=3 (12 Apr. 2002).

11) http://www.novell.com/coolsolutions/freetools_d_h.html (12 Mar. 2002).

12) Amatayakul, Margret and Walsh, Tom. "HIPAA on the Job: Selecting Strong Passwords," http://www.ahima.org/journal/features/feature.0110.03.htm (18 Feb. 2002).

13) Donovan, Craig. "Strong Passwords," June2, 2002, URL: http://rr.sans.org/policy/password.php (10 April 2002).

14) Ware, Karl. "Testimony and Supporting Documents Hearing by Subcommittee of Oversight and Investigations, Department of Veteran Affairs," 4 April 2001. URL: http://www.house.gov/va/hearings/schedule107/apr01/4-4-01/kware.htm (25 Mar. 2002).

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event