

## Investigating Novell Workstations

### Understanding workstation management

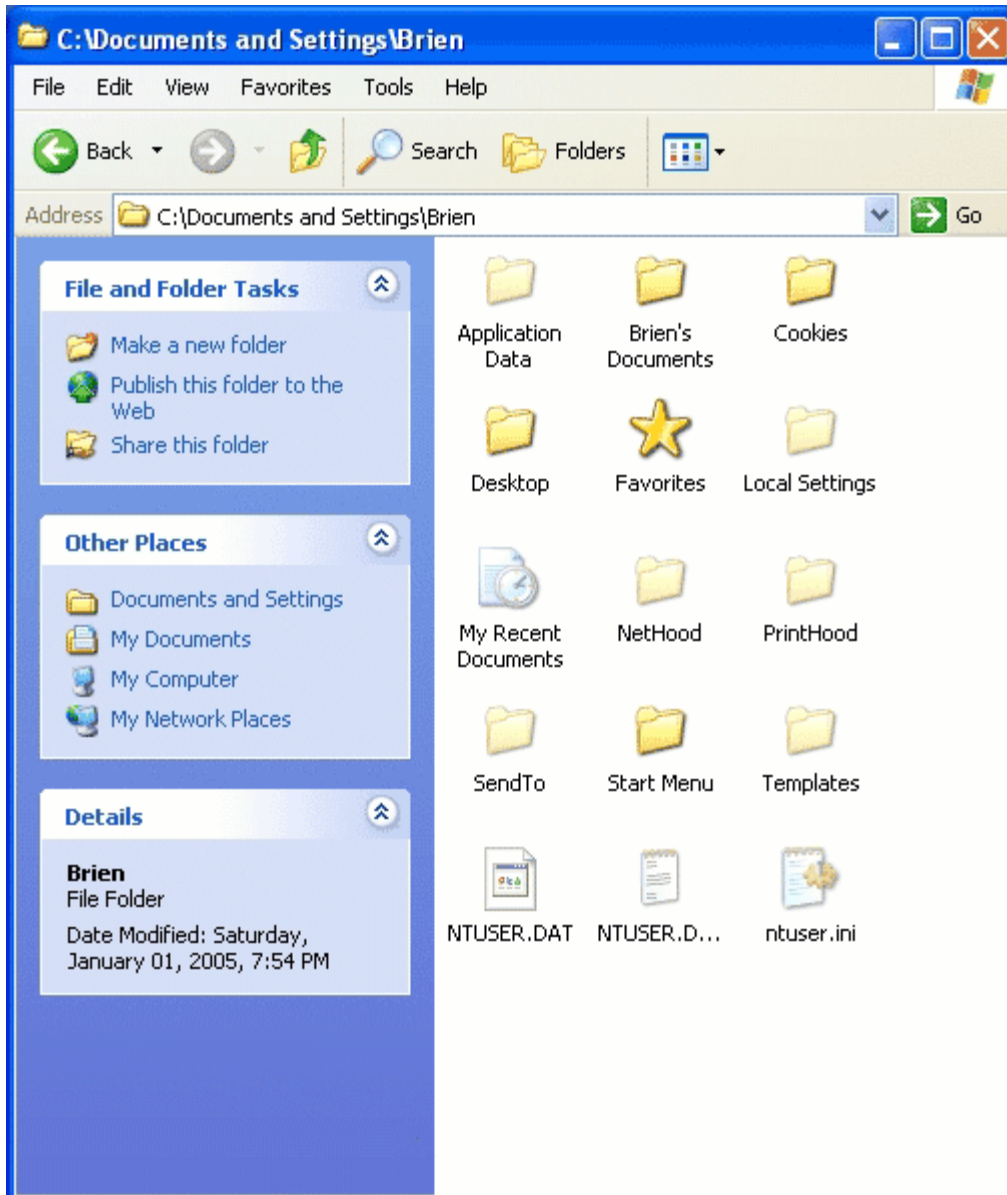
Novell workstation management exists on a two tier scale the first being the simple Novell network OS and connected clients, this implementation offers very little to work with as far as workstation management is concerned, clients login and logout most times writing documents to there automatically mapped home directories and unless a program like farfonics deepfreeze is installed all changes are written to the hard drive as if they were using the computer without a network operating system, in straight Netware environments (otherwise known as non zenworks environments) desktop investigation follows the same principles as with a stand alone computer.

The other tier of Novell desktop management (the more popular implementation) is the Zenworks desktop management suite (versions 4, 6.5 and 7) this allows administrators to mimic the popular active directory style of workstation management and makes forensics slightly more complicated. With Zenworks (the name zenworks meaning Zero Effort Networks) administrators can install group policy controls and manage user's home directories, all without a additional windows server. Zenworks is a very robust management tool that allows administrators increased controls over there networks. From a security perspective zenworks is a necessary addition to any reliable secure Novell network.

In addition to windows desktop management Novell has also developed a Zenworks Linux management and a Linux client for Novell, at this point however the actual management of the users experience with zenworks is non relevant to the Linux implementations as the zenworks Linux platform does very little to enhance or secure the users desktop, the main application of Zenworks Linux management is application deployment and desktop inventory management. And as with non zenworks environment when investigating user's desktops on the Linux Novell client proceed as normal when investigating a Linux desktop.

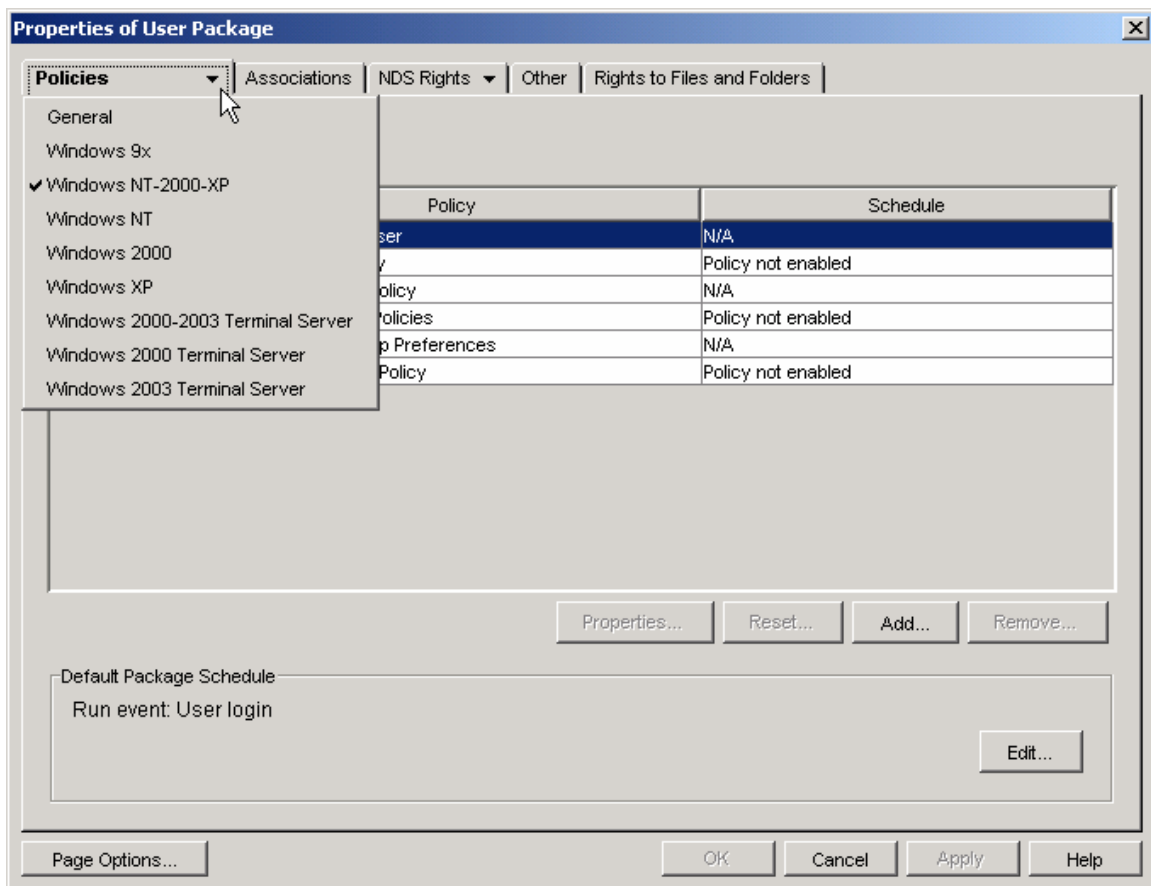
## Investigating a Desktop

Like its windows counterpart when a workstation is managed with Zenworks the users personal settings are stored in a roaming profiles are stored in the users home directory this allows us a detailed view of how the users workspace looks and feels not only from a evidence point of view is this data valuable it can also give you a interesting look at the suspects psychological mindset



Above is a typical users roaming profile, depending on the data this collection of folders can be anywhere between 1mb and several gigabytes of data and can be examined at length via a administrators console while not running the risk of

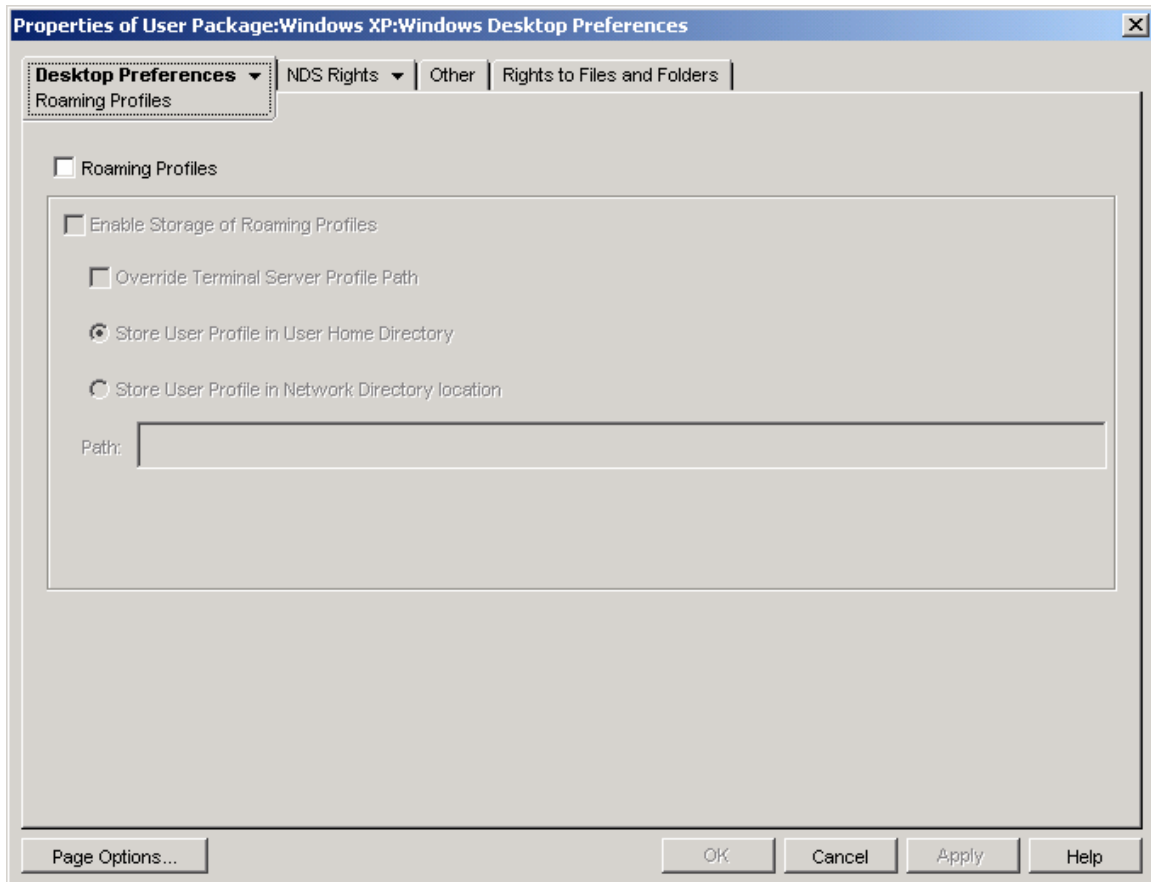
using the suspects computer directly. (For more information about investigating the roaming profiles directory see the investigating users home directories article). This information is invaluable to someone investigating a user's desktop because unlike windows zenworks will allow for separate user profiles for each version of windows. Although this feature is usually disabled in favor of a common roaming profile for all Windows NT series operating systems however a user wishing to hide data may effectively do so by turning on this feature and using a non standard company OS, this would be very effective as by default Novell networks do not require a administrator password to join the tree, so anyone can plug any OS into the network, install the Netware client and connect to the network.



in the example above the administrator is configuring policies for Windows NT-2000 and XP however if the administrator were to configure separate policys for each of the three OS's then separate roaming profiles would exist for each OS

## Storage Locations:

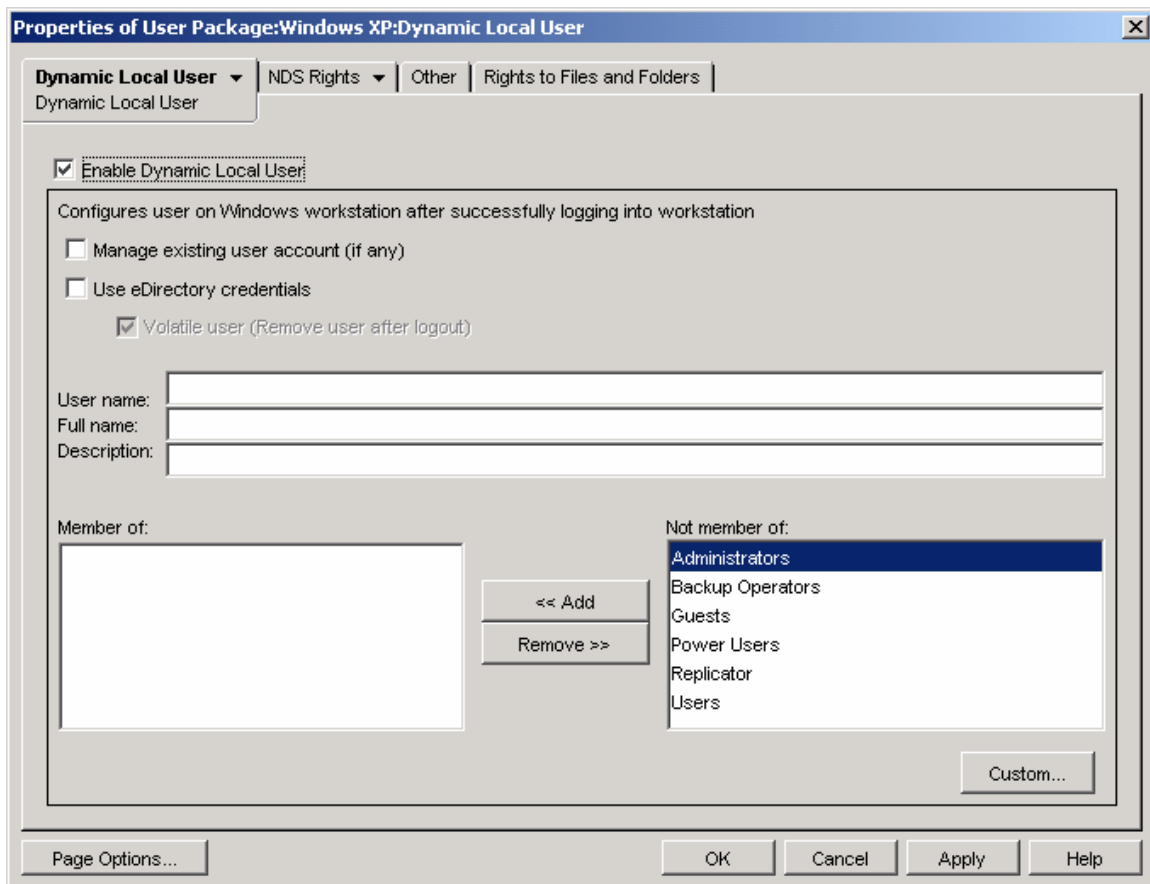
Using the most taught and most logical implementation strategy for Novell zenworks roaming profiles it is best to store the profiles in the users home directory, however this can be overridden and the profile can be stored on any network volume for investigative purposes it is important to note the location of the roaming profiles through the console1 program with the Zenworks snapins included as pictured in the bellow screenshot



## Local Users and Groups

As Novell Netware is not a windows based application and the client program is a windows add in there are some difficulties that could make forensics work complicated, the most notable when it comes to desktop management is the GINA or login routine when it comes to profiles. As windows must authenticate everyone through its local database or a active directory database Novell users are often faced with the problem of having to create built in “users” accounts on the windows machines and also authenticating through the edirectory, this process of having everyone share a windows profile is tiresome and incredibly insecure (unless a product like deepfreeze is used) so to combat the problem Novell introduced a feature called Dynamic local user with Zenworks. This feature creates a windows user based on the e-directory credentials and input it into the working local windows user database with the option to add groups, remove the user at log out or manage a existing user if necessary.

This feature is enabled in console1 through the zenworks snap-ins (see below)



Name	Full Name	Description
__vmware_user__	__vmware_user__	VMware User
ACTUser	Application Center Test Account	Account used to launch the Application Center Test Broker and...
Administrator		Built-in account for administering the computer/domain
ASPNET	ASP.NET Machine Account	Account used for running the ASP.NET worker process (aspnet...
Guest		Built-in account for guest access to the computer/domain
HelpAssistant	Remote Desktop Help Assistant Account	Account for Providing Remote Assistance
ian	Ian Thomson	Account created by Novell's Workstation Manager
SQLDebugger	SQLDebugger	This user account is used by the Visual Studio .NET Debugger
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C...	This is a vendor's account for the Help and Support Service

When successfully completed the users are added into the windows users database as illustrated above.

From a forensics point of view this is often a stumbling block of most investigations as when investigating the desktops from a logged off state it appears as if the user was never on the computer begin with, therefore it is important to remember to check the roaming profile when investigating zenworks environments and to perform a standard windows check anyway.

Dynamic local users do however have there advantages, because of the migration between Edirectory account and Windows account the users password hash is copied into the windows database (also removed at logout) however if it is necessary to find out the users password instead of simply changing it running a program like LC3 on the users machine will revile the password.

As depicted bellow the user managed by Zenworks account “ian” is entered into the database.

User Name	LM Password	<G	NTLM Password	Audit Time
ACTUser				
Administrator				
ASPNET				
Guest	* empty *	x	* empty *	
HelpAssistant				
ian				
SQLDebugger	* empty *	x		
SUPPORT_388945a0	* empty *	x		

**DICTIONARY STATUS**

words total: 3704  
words done: 235007  
% done: 1.576%

**BRUTE FORCE**

time elapsed: 0d 0h 0m 0s  
time left: 0d 0h 0m 0s  
% done: 0%  
current test: 0  
keyrate: 0

User Info Check  
 Dictionary  
 Hybrid  
 Brute Force

LC3  
Security Software Technologies, Inc.  
securitysoftwaretech.com

Audit paused. NUM

## **Conclusions and Summery**

This article has outlined the steps of how Novell zenworks interacts with the windows clients it manages and how data is exchanged between the zenworks application and the windows server. It is meant to inform users of how to properly investigate users operating with zenworks. However as zenworks is not made by Microsoft it is not perfect and much of the cached data that is usually found on windows workstations is not removed on logout by zenworks, therefore it is very critical to investigate the user with the procedures described above and standard forensics practices used to investigate windows computers.