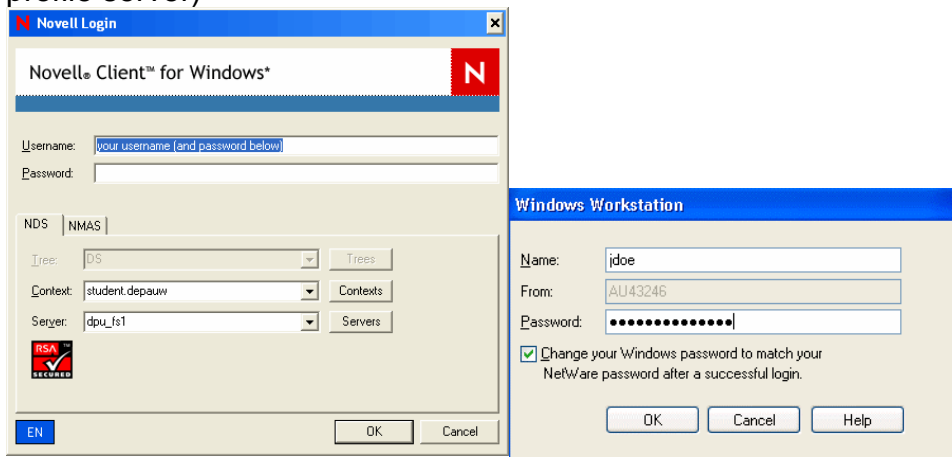


Investigating Users Home Directories

Introduction and Background

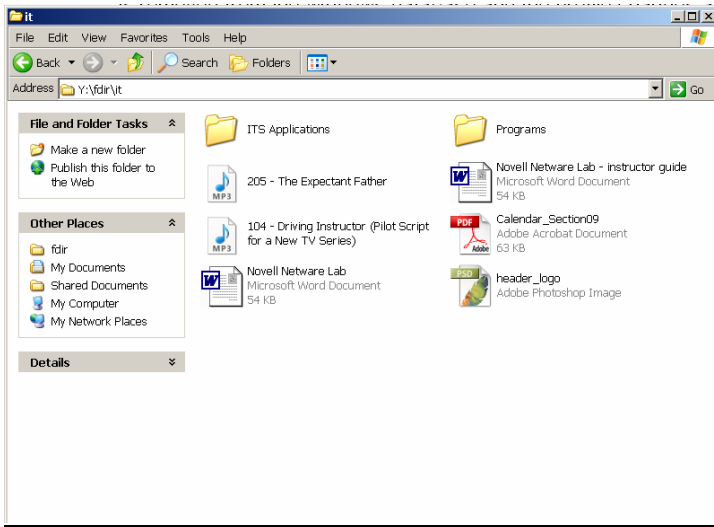
As mentioned in the investigating user's desktops section there are two types of Netware environments, the first environment is the straight Netware without the use of zenworks. In this environment the users are authenticated to the network however the local profiles or the database of users that is on the workstation is totally independent of the Novell server, so the users face two distinct authentication modes and share one single profile with every user on the computer.

(Bellow two login boxes illustrating the Netware login routine without a zenworks profile server)

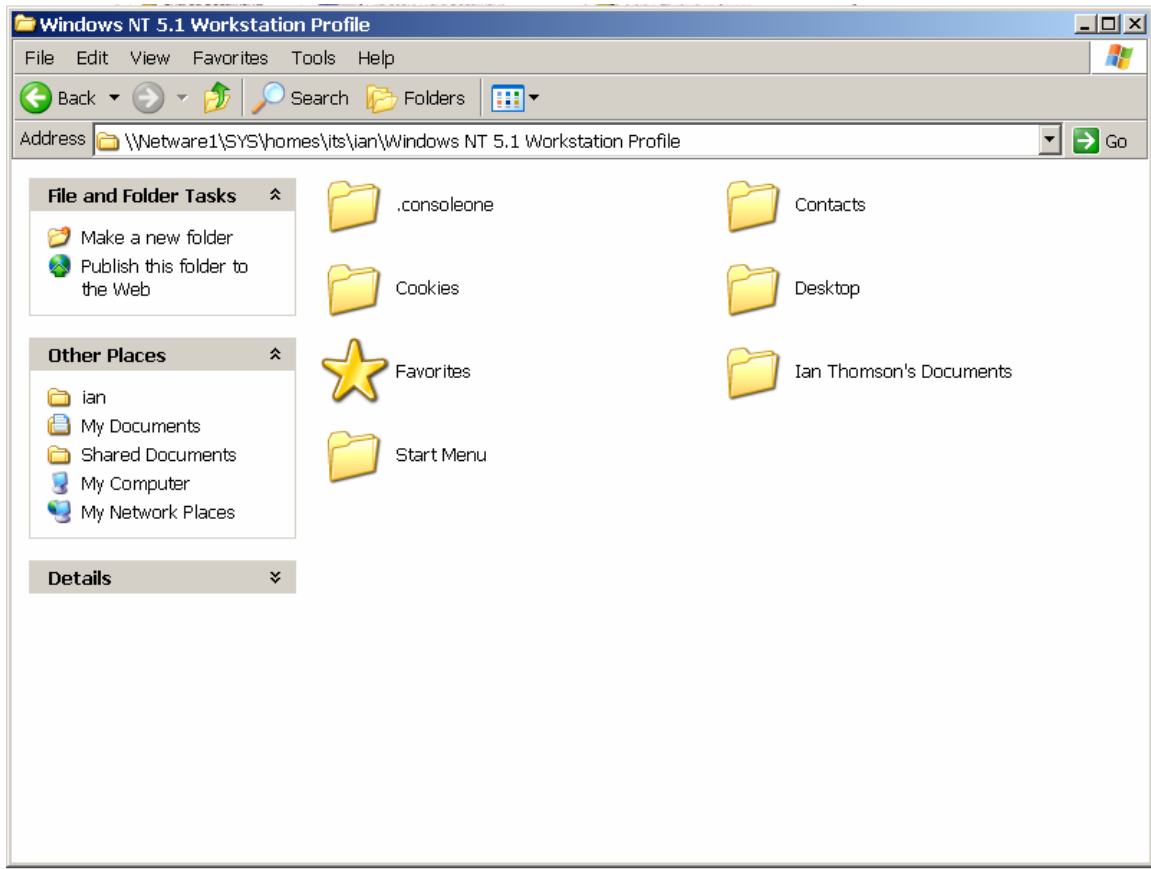
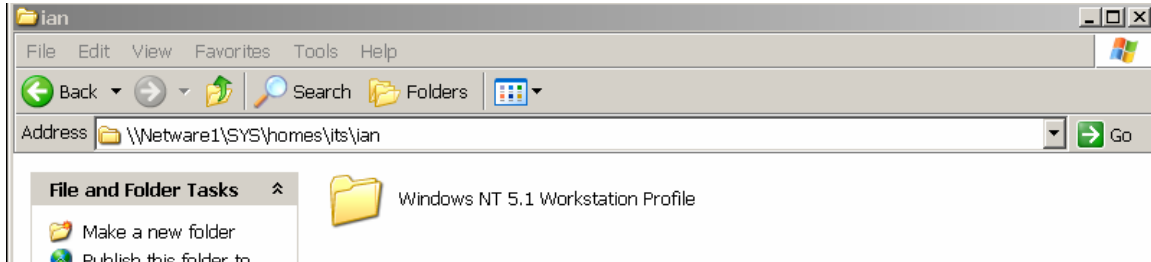


The second type of environment is Netware with Zenworks (4, 6.5, and 7) built in. This environment is vastly superior especially in the area of windows workstations as it creates a dynamic local user (an account with matching credentials inputted into the windows user database) which the user uses for the duration of there session. When the user logs off the workstation then the profile is removed from the windows database and the profile changes are written to the users home directory, whereas with the non zenworks environment, profile changes (favorites, desktop icons, user settings, my documents folder) are usually either lost or stored on that local computer for the next user that uses that workstation.

These two major differences offer a very different scope as to what a home directory is, the first (being the non zenworks environment) offers users a blank network folder mapped to a network drive in which users store files (pictured bellow), the changes are written to the server automatically and none of the users profile settings are changed on the server



The second version of the Novell home directory (the zenworks variant) is much more in-depth, from the root of the folder it contains a series of profile folders, each with a OS depending on how the Policy is setup with Zenworks, inside the folders it appears exactly as a windows 'Documents and Settings Profile' appears on a standard windows workstation or a active directory domain

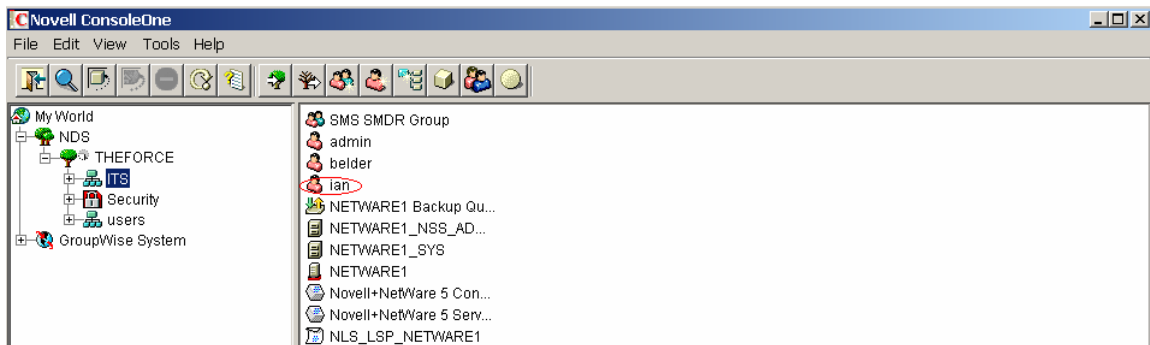


Locating Home Directories on Novell Network

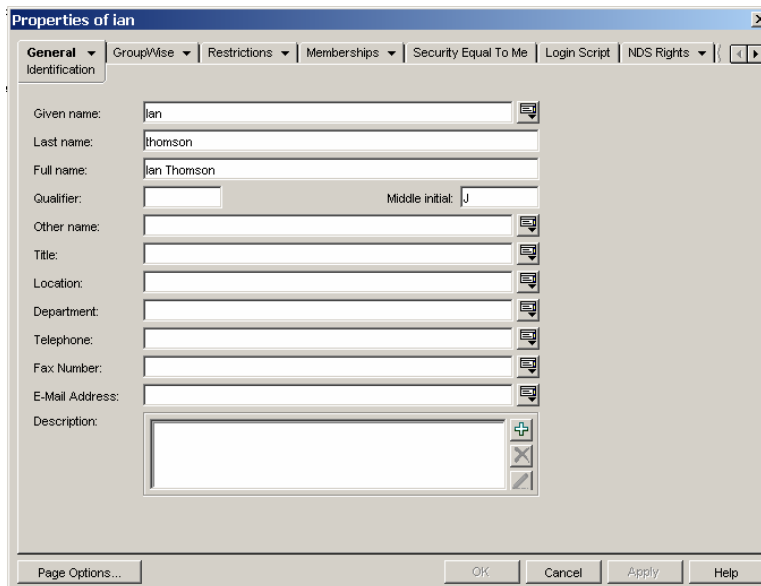
Before investigating the home directory we must first learn the location on the network. 70 to 80% of all Novell networks contain more than one server so a simple search of the server is a very inefficient way of locating the items needed, for this task we will use the Administrators program Novell Console1, or if you are operating a Netware 3 or 4 server the older NWADMIN32 program will work effectively as well.

Note: It is necessary to complete this task to have admin access or security equal to admin.

- Launch the Console1 Program and locate the user you wish to investigate.



- Double click on the users icon to load there settings page



- On the general tab click the drop down arrow and click the environment link to load the environment page


The screenshot shows a configuration window with the following fields and values:

- Language: ENGLISH
- Network address: IP: 172.16.1.11
- Default server: (empty)
- Home Directory:
 - Volume: NETWARE1_SYS.ITS
 - Path: \homes\its\ian

Note the location of the home directory on the network.

The second piece of information we need to locate is if this user is associated with a zenworks profile policy to do this we will again use the console1 property page.

Note: The workstation you are running console1 from must have Zen works snapin's installed in order to view Zen works information.

Double click the policy packages as denoted by the following icon in the console1 view  User Package

Click the associations tab:

If the user you are investigating is listed in the following page then the user has a zenworks profile.

The screenshot shows the 'Properties of User Package' dialog box with the 'Associations' tab selected. The 'Associations' list contains the following entries:

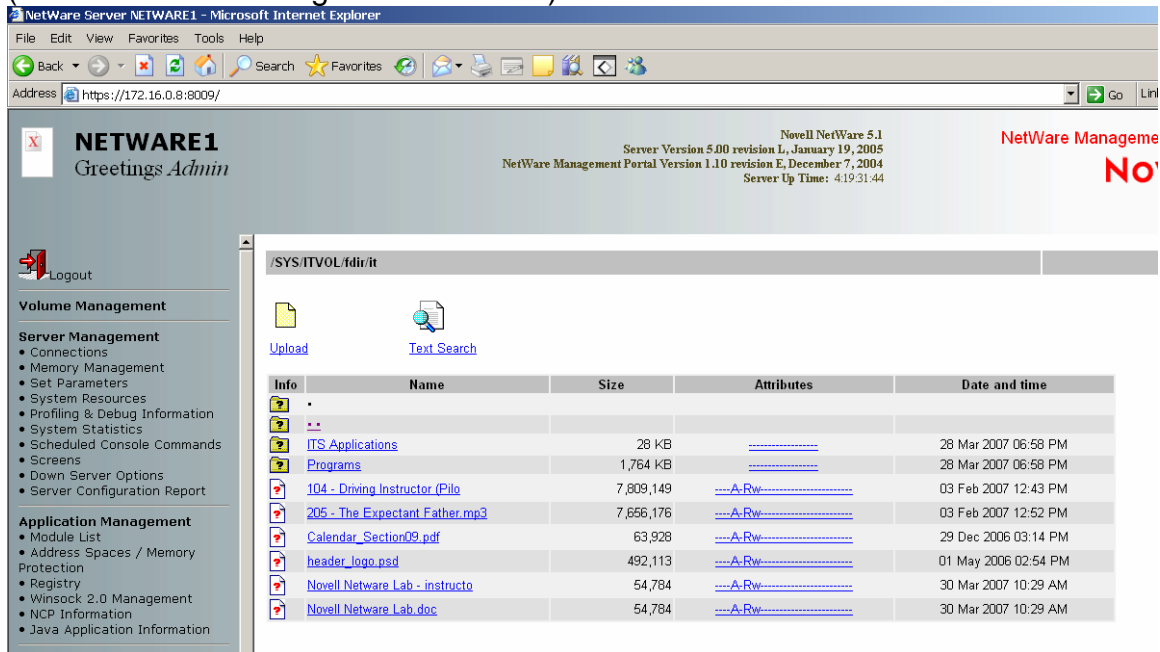
- admin.ITS
- belder.ITS
- ian.ITS

Investigating non-zenworks directories

A Basic rule when dealing with Novell at the admin level especially with non zenworks profiles is “what you see is what you get”. This is true for simple home directories as well, the users files are shown in the folder, and there is no way to hide data from the admin user. Therefore it is a simple matter of applying general forensics to the home directory and investigating the documents.

Although stated above there is no way to hide information from a admin user there is however ways to hide data from the windows console the admin user is using, be advised of traditional windows explorer style data hiding tactics and if possible use a more direct console interface such as the file browser at the servers GUI or the Novell imanager folder viewer

(Browser based imanager folder viewer)



The screenshot shows a Microsoft Internet Explorer browser window displaying the NetWare Management Portal. The address bar shows <https://172.16.0.8:8009/>. The page header includes "NETWARE1 Greetings Admin" and "Novell NetWare 5.1 Server Version 5.00 revision L, January 19, 2005". The main content area displays a file browser view for the directory `/SYS/ITVOL/udir/it`. The browser shows a table of files with columns for Name, Size, Attributes, and Date and time.



Info	Name	Size	Attributes	Date and time
?	.			
?	..			
?	ITS Applications	28 KB	-----	28 Mar 2007 06:58 PM
?	Programs	1,764 KB	-----	28 Mar 2007 06:58 PM
?	104 - Driving Instructor (Pilo	7,809,149	---A-Rw-----	03 Feb 2007 12:43 PM
?	205 - The Expectant Father.mp3	7,666,176	---A-Rw-----	03 Feb 2007 12:52 PM
?	Calendar_Section09.pdf	63,928	---A-Rw-----	29 Dec 2006 03:14 PM
?	header_logo.psd	492,113	---A-Rw-----	01 May 2006 02:54 PM
?	Novell Netware Lab - instructo	54,784	---A-Rw-----	30 Mar 2007 10:29 AM
?	Novell Netware Lab.doc	54,784	---A-Rw-----	30 Mar 2007 10:29 AM









Investigating Zenworks Home Directories

As with the non zenworks home directories the same principles about file hiding apply, there is no way to hide files from a admin user, however there are still ways to hide them from the explorer, so therefore it is advisable to do all work from the manager program.

To investigate the users home directories in this context all that is required is to use the same principles as with a general windows home directory, as zenworks is really nothing more then windows management features for a Novell environment

/SYS/homes/its/ian/Windows NT 5.1 Workstation Profile

 [Upload](#)  [Text Search](#)

Info	Name	Size	Attributes	Date and time
	.			
	..			
	.consoleone	4 KB	-----	28 Mar 2007 08:02 PM
	Contacts	1,660 KB	-----	28 Mar 2007 08:02 PM
	Desktop	16 KB	-----	28 Mar 2007 08:02 PM
	Favorites	4 KB	-----Dj---	28 Mar 2007 08:02 PM
	My Documents	2,428 KB	-----Dj---	28 Mar 2007 08:02 PM
	Start Menu	24 KB	-----Dj---	28 Mar 2007 08:02 PM

(Zenworks Home Directory as shown in imanager)