

# VISUAL message center

## NFS Sharing

How to Access Files Shared via NFS on a UNIX Server  
from a Windows Computer  
For Internal Use

8.0

VMC-Mxx

**tango04**  
Computing Group

Solutions for Advancing People

## NFS Sharing - How to access files shared via NFS on a UNIX Server from a Windows Computer

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

### Copyright Notice

Copyright © 2013 Tango/04 All rights reserved.

Document date: August 2012

Document version: 1.0

Product version: 8.0

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Tango/04.

### Trademarks

Any references to trademarked product names are owned by their respective companies.

### Technical Support

For technical support visit our web site at [www.tango04.com](http://www.tango04.com).

Tango/04 Computing Group S.L.

Avda. Meridiana 358, 5 A-B

Barcelona, 08027

Spain

Tel: +34 93 274 0051

# Table of Contents

Table of Contents .....	iii
-------------------------	-----

## Chapter 1

---

Introduction .....	1
1.1. Objectives .....	1
1.2. Audience .....	1
1.3. Notations .....	1
1.4. Additional Resources .....	1

## Chapter 2

---

Configuring the UNIX Server .....	2
2.1. About NFS .....	2
2.2. Installation and Configuration .....	3
2.2.1. Shared Folders and Access .....	3
2.2.2. Starting NFS.....	6

## Chapter 3

---

Windows NFS Client configuration .....	8
3.1. Installation of Windows Services for UNIX.....	8
3.1.1. Windows XP Professional and 2003 Server .....	8
3.1.2. Windows Vista.....	12
3.2. Configuration of the NFS Client .....	12
3.2.1. NFS Administration Console .....	12

3.2.2. User-Mapping Configuration ..... 13

## Chapter 4

---

Configuration of Applications Agent ..... 18

4.1. Linux Server Configuration ..... 18

4.2. Windows Configuration: Applications Agent ..... 18

---

About Tango/04 Computing Group ..... 21

Legal Notice ..... 22

### 1.1 Objectives

The objective of this document is to explain how to set up a network access from a Windows server to a Linux File System via Network File System (NFS). Such a configuration can be used to monitor remote files thanks to Applications Agent.

### 1.2 Audience

This document has been designed for technical readers with a knowledge of UNIX and Windows file systems and file-sharing protocols.

### 1.3 Notations

In this document, references to UNIX may also apply to Linux and other IX operating systems.

### 1.4 Additional Resources

For more details about installation, configuration and optimization of NFS on Linux hosts, you may read the How-To called Linux-NFS-HOWTO by Christopher Smith, available at <http://nfs.sourceforge.net/nfs-howto/index.html>.

Most of the examples and explanations in this document are taken from this How-To.

In this chapter, we will explain how to configure the Unix machine to act as an NFS file server.

## 2.1 About NFS

Extract from Wikipedia's article on Network File System:

**Network File System** (NFS) is a network file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.

...

Assuming a Unix-style scenario in which one machine (the client) requires access to data stored on another machine (the NFS server):

1. The server implements NFS daemon processes (running by default as `nfsd`) in order to make its data generically available to clients.
2. The server administrator determines what to make available, exporting the names and parameters of directories (typically using the `/etc/exports` configuration file and the `exportfs` command).
3. The server security-administration ensures that it can recognize and approve validated clients.
4. The server network configuration ensures that appropriate clients can negotiate with it through any firewall system.
5. The client machine requests access to exported data, typically by issuing a `mount` command.
6. If all goes well, users on the client machine can then view and interact with mounted filesystems on the server within the parameters permitted.

Note that automation of the NFS mounting process may take place — perhaps using `/etc/fstab` and/or automounting facilities.

## 2.2 Installation and Configuration

This paragraph explains briefly how to set up and configure NFS on a Linux host in order to make files available to certain users on the network.

More information can be found at this address:

<http://nfs.sourceforge.net/nfs-howto/>

Setting up NFS involves 2 steps:

- Configuration of the shared folders as well as the authorizations
- Launching the NFS daemon that will wait for incoming client connections.

These operations can be done thanks to the Terminal. Modern distributions also allow configuration via a graphical interface.

### 2.2.1 Shared Folders and Access

#### File-based configuration

The list of folders to be shared and the permissions to access them are listed in a plain-text file located in `/etc/exports`. It can also be modified via a GUI on modern distributions.

It should contain something like:

```
directory machine1(option11,option12)
machine2(option21,option22)
```

with:

- **Directory**: the directory that you want to share. It may be an entire volume though it need not be. If you share a directory, then all directories under it within the same file system will be shared as well.
- **machine1** and **machine2**: client machines that will have access to the directory. The machines may be listed by their DNS address or their IP address (e.g., `machine.company.com` or `192.168.0.8`). Using IP addresses is more reliable and more secure. If you need to use DNS addresses, and they do not seem to be resolving to the right machine, *see Section 7 - Troubleshooting of Christopher Smith's online guide: <http://nfs.sourceforge.net/nfs-howto/index.html>*.
- **Optionxx**: the option listing for each machine will describe what kind of access that machine will have. Important options are:
  - **ro**: The directory is shared read only; the client machine will not be able to write it. This is the default.
  - **rw**: The client machine will have read and write access to the directory.
  - **no\_root\_squash**: By default, any file request made by user `root` on the client machine is treated as if it is made by user `nobody` on the server. (Exactly which UID the request is mapped to depends on the UID of user “nobody” on the server, not the client.) If `no_root_squash` is selected, then `root` on the client machine will have the same level of access to the files on the system as `root` on the server. This can have serious security implications, although it may be necessary if you want to perform any administrative work on the client machine that involves the exported directories. You should not specify this option without a good reason.

- `no_subtree_check`: If only part of a volume is exported, a routine called subtree checking verifies that a file that is requested from the client is in the appropriate part of the volume. If the entire volume is exported, disabling this check will speed up transfers.
- `sync`: By default, all but the most recent version (version 1.11) of the `exportfs` command will use `async` behavior, telling a client machine that a file write is complete - that is, has been written to stable storage - when NFS has finished handing the write over to the filesystem. This behavior may cause data corruption if the server reboots, and the `sync` option prevents this. See [Section 5 - Optimizing NFS Performance of Christopher Smith's online guide: http://nfs.sourceforge.net/nfs-howto/index.html](http://nfs.sourceforge.net/nfs-howto/index.html) for a complete discussion of `sync` and `async` behavior.

The machine part can also include Net Masks, to allow a certain range of IP addresses to connect.

For instance, to give read-only access to my folder `/home/tibo/shared` to people with IP addresses `192.168.0.XXX`, I could add the line:

```
/home/tibo/shared 192.168.0.0/255.255.255.0(ro)
```

Usual options include security measures. A safer way would be:

```
/home/tibo/my_shared 192.168.0.0/255.255.255.0  
(ro,root_squash,sync,no_subtree_check)
```

You can add some more advanced security checks modifying the files `/etc/hosts.allow` and `/etc/hosts.deny` that explicitly states which hosts can and cannot connect to the server's network services. We will not cover this in detail.

At this point, you can try to restart the NFS Daemon.

## Using the GUI

On distributions like OpenSUSE the configuration can be done through a GUI. Here are some screen shots about how to proceed.

**Step 1.** You may first need to install an NFS Server. On modern distributions, you can use the Software packet manager to install it

**Step 2.** To configure the NFS Server, open the YaST2 administration panel in OpenSUSE

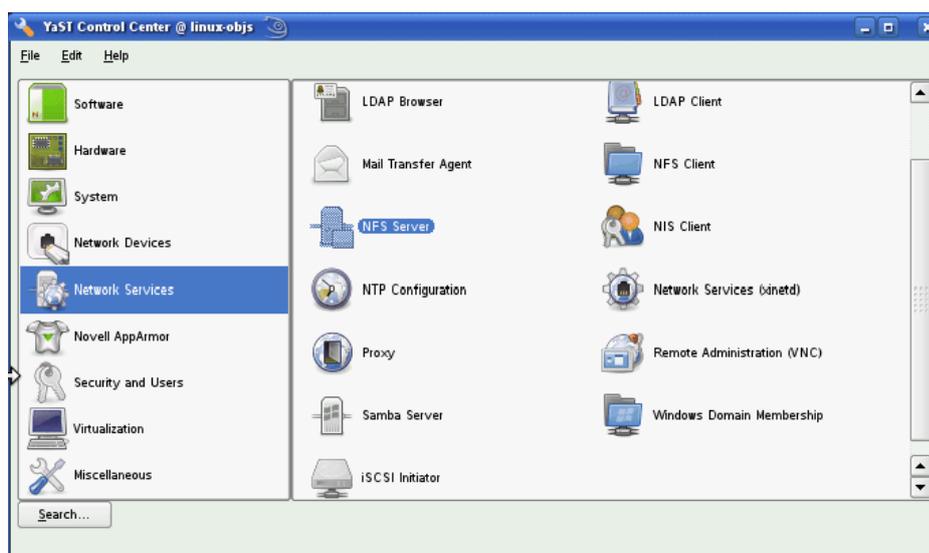


Figure 1 – YaST2 administration panel

**Step 3.** Click the **NFS Server** icon to open the configuration window, you will be able to configure general parameters, and start or restart it.

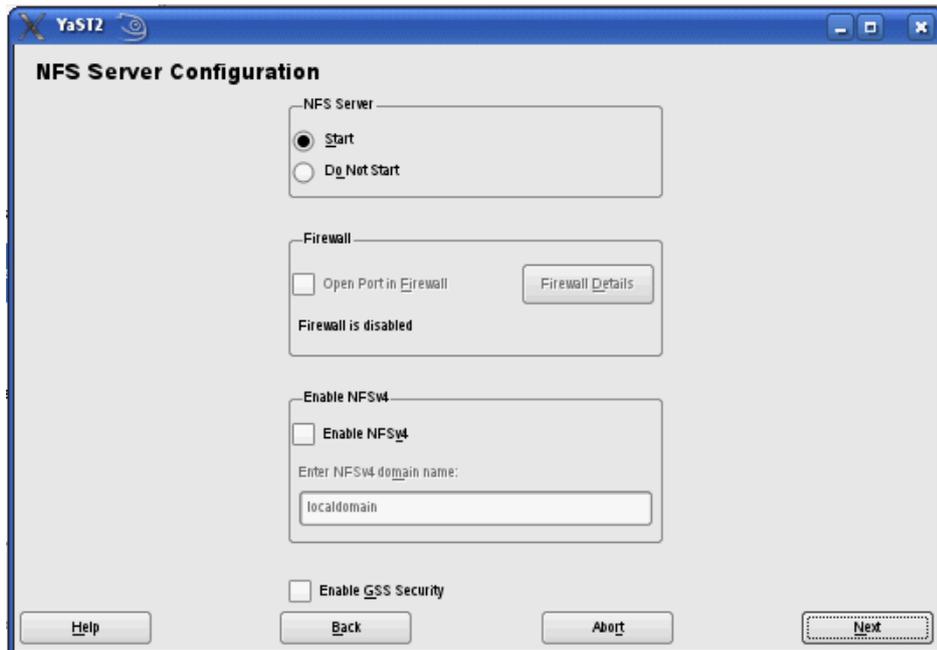


Figure 2 – NFS Server configuration

**Step 4.** Configure the folders that are published, and the access options for these folders. You can add folders, and for each folder you can add permissions to hosts.

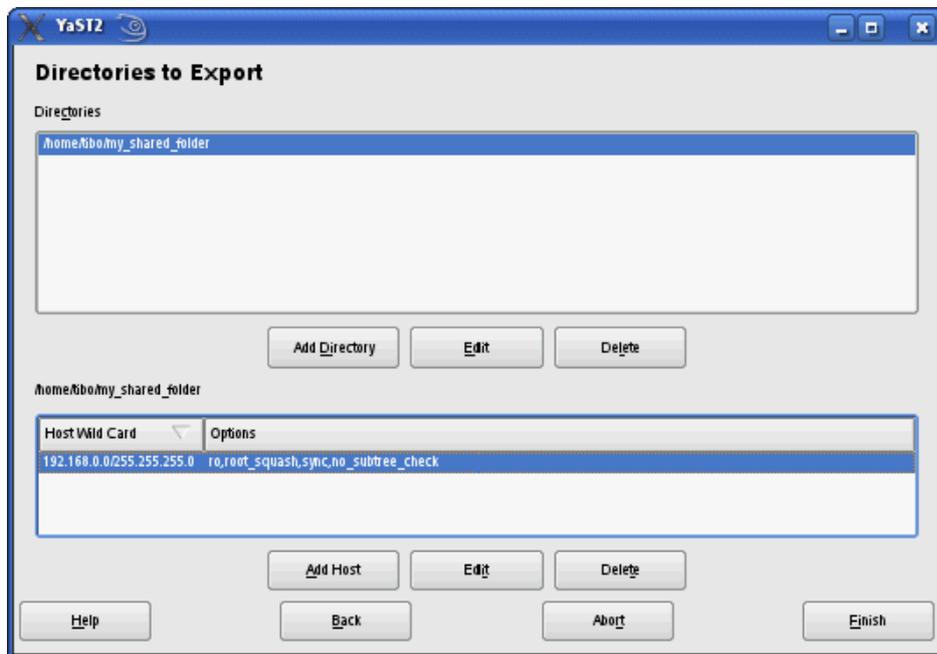


Figure 3 – Add the directories to export

**Step 5.** Click **Finish** to apply the changes and restart the NFS Server to take the changes into account.

## 2.2.2 Starting NFS

### The portmapper daemon

NFS depends on the **portmapper** daemon, either called `portmap` or `rpc.portmap`. It will need to be started first. It should be located in `/sbin` but is sometimes in `/usr/sbin`. Most recent Linux distributions start this daemon in the boot scripts, but it is worth making sure that it is running before you begin working with NFS (just type `ps aux | grep portmap`).

### NFS daemons

NFS serving is taken care of by five daemons:

- `rpc.nfsd`, which does most of the work;
- `rpc.lockd` and
- `rpc.statd`, which handle file locking;
- `rpc.mountd`, which handles the initial mount requests, and
- `rpc.rquotad`, which handles user file quotas on exported volumes.

Starting with 2.2.18, `lockd` is called by `nfsd` upon demand, so you do not need to worry about starting it yourself. `statd` will need to be started separately. Most recent Linux distributions will have startup scripts for these daemons.

The daemons are all part of the `nfs-utils` package, and may be either in the `/sbin` directory or the `/usr/sbin` directory.

If your distribution does not include them in the startup scripts, then you should add them, configured to start in the following order:

```
rpc.portmap
rpc.mountd, rpc.nfsd
rpc.statd, rpc.lockd (if necessary), and
rpc.rquotad
```

The `nfs-utils` package has sample startup scripts for RedHat and Debian. If you are using a different distribution, in general you can just copy the RedHat script, but you will probably have to take out the line that says:

```
.. /init.d/functions
```

to avoid getting error messages.

### Checking that NFS is running

To do this, query the portmapper with the command `rpcinfo -p` to find out what services it is providing. You should get something like this:

```
tibo@linux-objs:~> /usr/sbin/rpcinfo -p
program vers proto  port
100000    2    tcp    111  portmapper
100000    2    udp    111  portmapper
100005    1    udp    47072 mountd
100005    1    tcp    55372 mountd
```

## Configuring the UNIX Server

```
100005  2  udp  47072  mountd
100005  2  tcp  55372  mountd
100005  3  udp  47072  mountd
100005  3  tcp  55372  mountd
100024  1  udp  52396  status
100024  1  tcp  60582  status
100003  2  udp   2049  nfs
100003  3  udp   2049  nfs
100003  4  udp   2049  nfs
100021  1  udp  37857  nlockmgr
100021  3  udp  37857  nlockmgr
100021  4  udp  37857  nlockmgr
100003  2  tcp   2049  nfs
100003  3  tcp   2049  nfs
100003  4  tcp   2049  nfs
100021  1  tcp  48031  nlockmgr
100021  3  tcp  48031  nlockmgr
100021  4  tcp  48031  nlockmgr
```

You should see that nfs is running as well as portmapper.

At this point, NFS should be running, publishing the folders you have defined.

## Windows NFS Client configuration

The previous chapter explained how to set up NFS to share folders on a network. This part will explain how to configure a client on a Windows computer so that those files can be easily accessed.

### 3.1 Installation of Windows Services for UNIX

NFS is not a native Windows protocol, Therefore, it is necessary to install additional packages to make it communicate with NFS-shared folders.

#### 3.1.1 Windows XP Professional and 2003 Server

For versions **previous to Windows Vista**, the package that allows access to NFS-shared folder is called Windows Services for UNIX (218 MB), and can be downloaded from Microsoft's web page:

<http://www.microsoft.com/downloads/details.aspx?familyid=896c9688-601b-44f1-81a4-02878ff11778&displaylang=en>

The latest version is 3.5 at time of the writing.

- Step 1.** Download this package from the above link.
- Step 2.** Launch it and extract its content in the folder of your choice

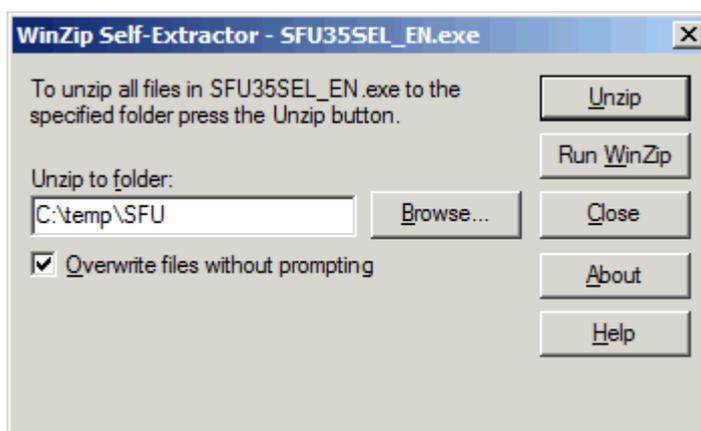


Figure 4 – Select the folder to unzip the files to.

- Step 3.** After the extraction, run `SfuSetup.msi` from the folder where you extracted the files.
- Step 4.** After accepting the license, select **Custom Installation**, in order to install only the required components

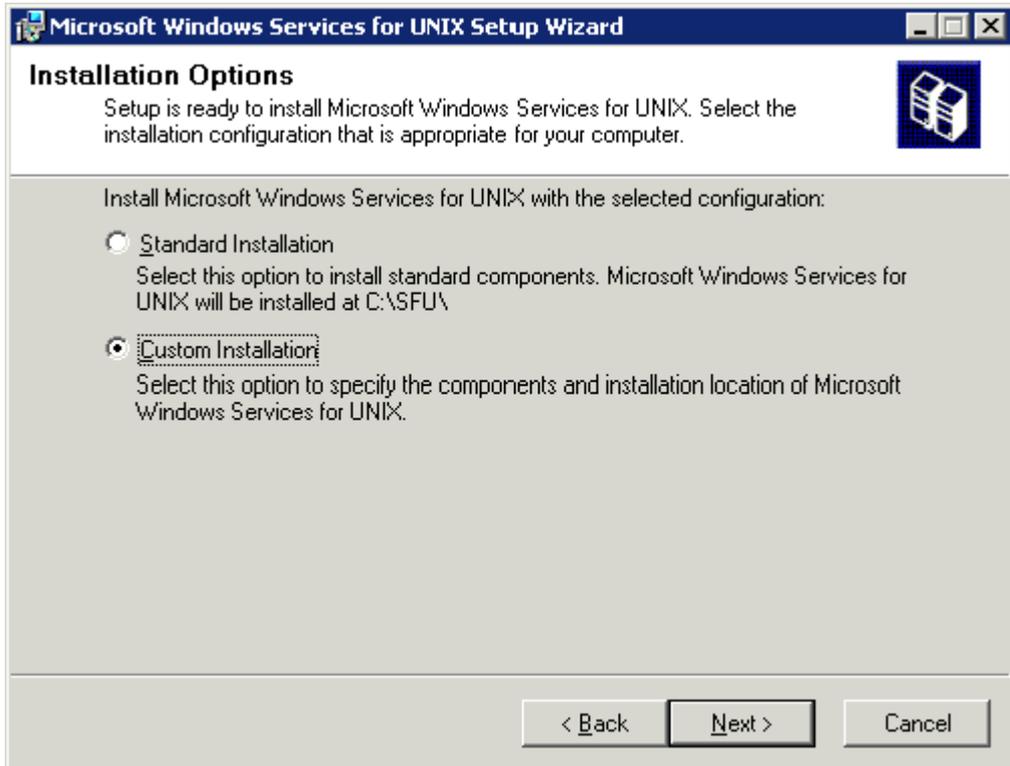


Figure 5 – Select Custom Installation

**Step 5.** De-select all components except **Client for NFS**

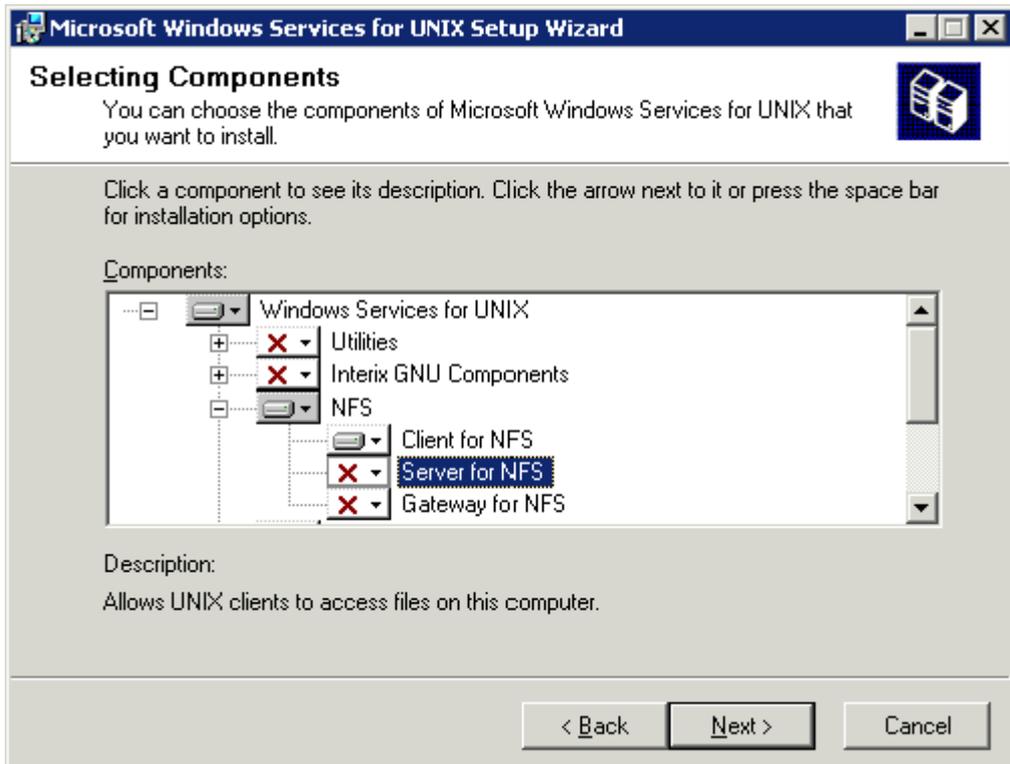


Figure 6 – De-select all components except Client for NFS

**Step 6.** Click **Next**

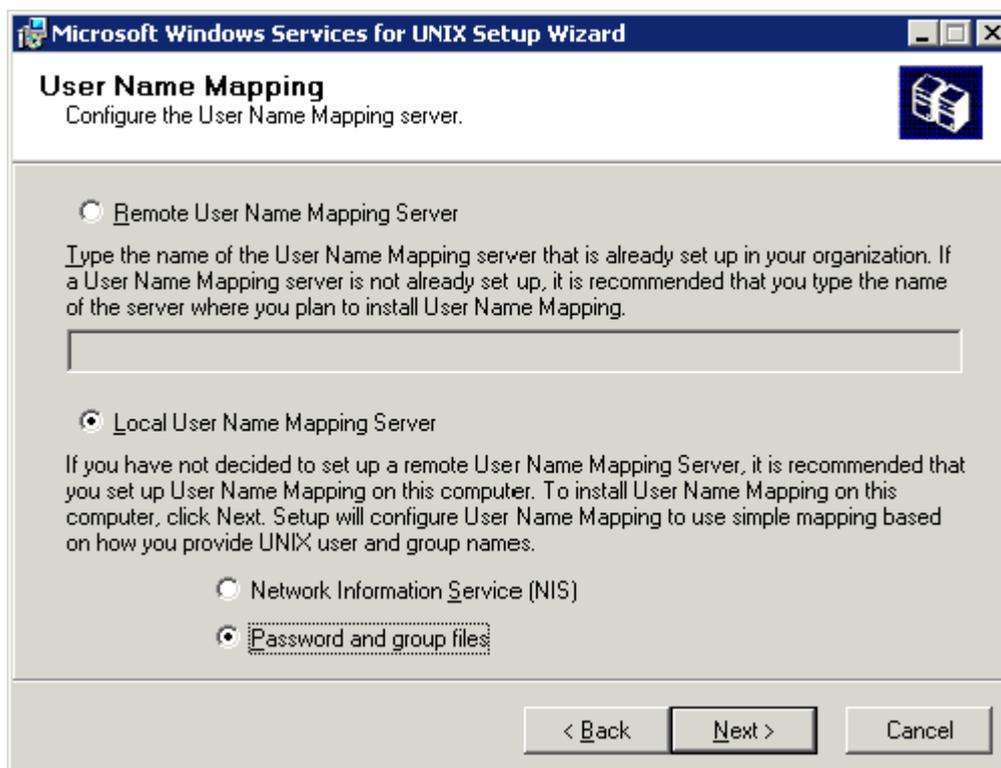


Figure 7 – User Name Mapping

In our case, we will select **Local User Name Mapping**, and **Password and groups files**. If you already have a User Name Mapping Server or a NIS, you may chose these options. In the following we will assume you selected Password and Group files.

**Step 7.** In order to know which Linux user should be used to connect for a given Windows User we must define **User Name Mapping**. The Windows computer where we install NFS Client needs to know which users and groups exist on the Linux Server (and their associated User IDs and Group IDs). To do that, **you should copy 2 files from the Linux Server: /etc/passwd and /etc/group** which list users and groups, and **put them in a folder on your Windows machine**. Then type in the path to those files. Note that this can also be set and changed later.



**Note**

The `passwd` file does not contain the users' passwords, but only there names and User IDs.

You should also choose where the list of Windows users must be extracted from. It can be extracted locally (from the computer list) or from the domain. The available domains and servers should appear in the drop-down list box, and you can select the one you want.

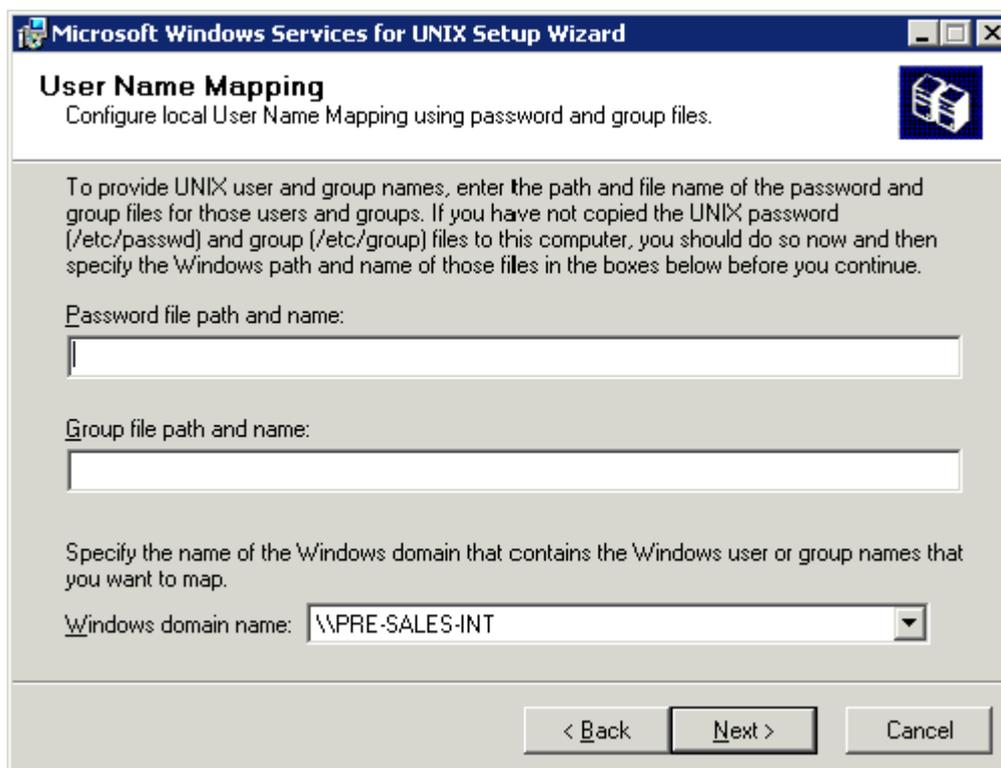


Figure 8 – Select the Windows domain name

- Step 8.** Press **Next** to select the path where the NFS Client should be installed, and click **Next** again to complete the installation

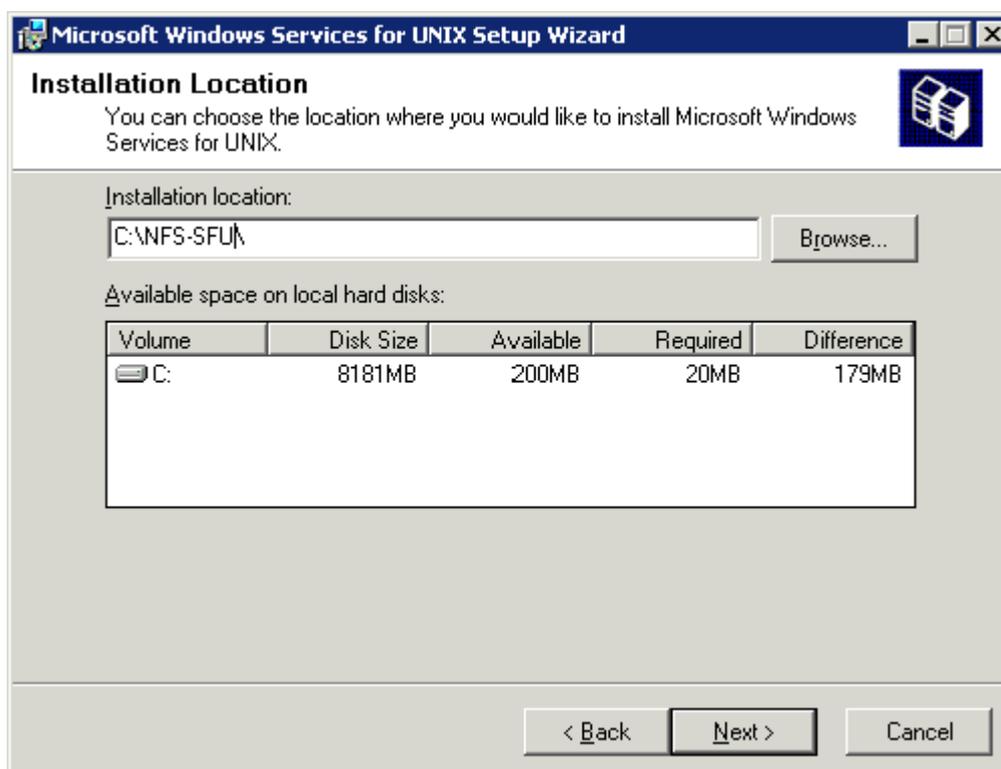


Figure 9 – Select the path where the NFS Client should be installed

- Step 9.** If the installation is successful you will see a new entry in the Windows **Start Menu > Programs** called **Windows Services For UNIX**. You may now proceed to the next chapter.

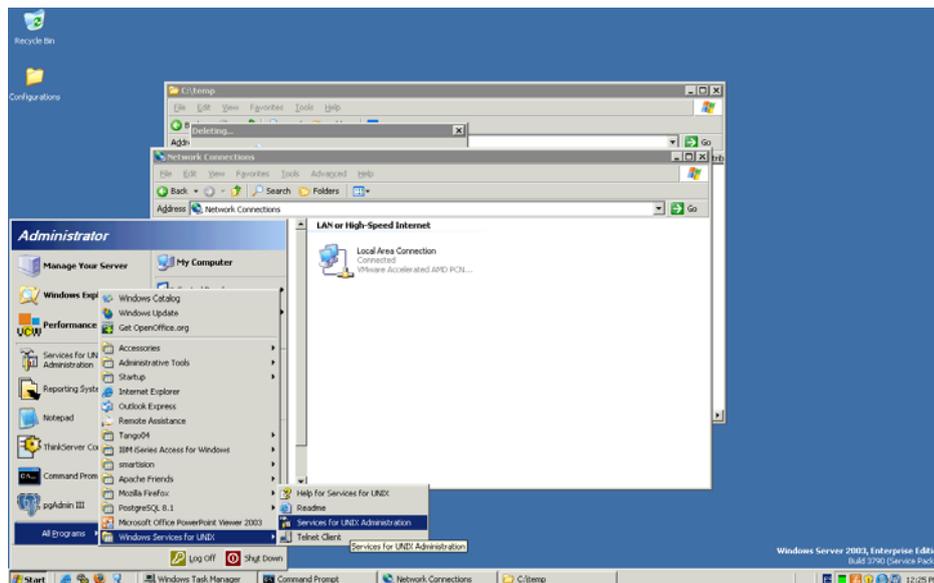


Figure 10 – Windows Services for UNIX in the Programs menu

### 3.1.2 Windows Vista

For **Windows Vista-based operating systems**, you need to enable some Windows Components. Note that they are available only for the Ultimate and Enterprise editions.

## 3.2 Configuration of the NFS Client

At this point, you should have successfully installed the Windows NFS Client. We will now proceed to its configuration.

### 3.2.1 NFS Administration Console

Configuration of the NFS Client is done through the **Services for UNIX Administration** console, located in the **Windows Start Menu**.

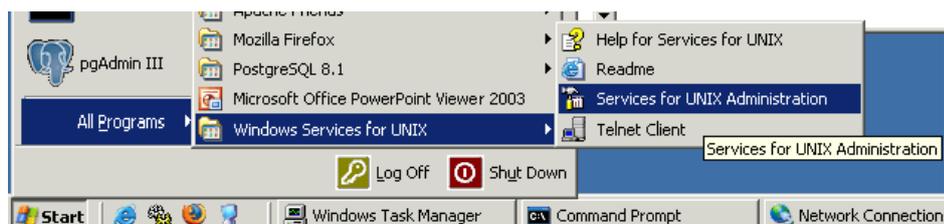


Figure 11 – Select Services for UNIX Administration from the Windows Start menu

Launching it opens a window that allows you to configure some parts of the NFS Client.

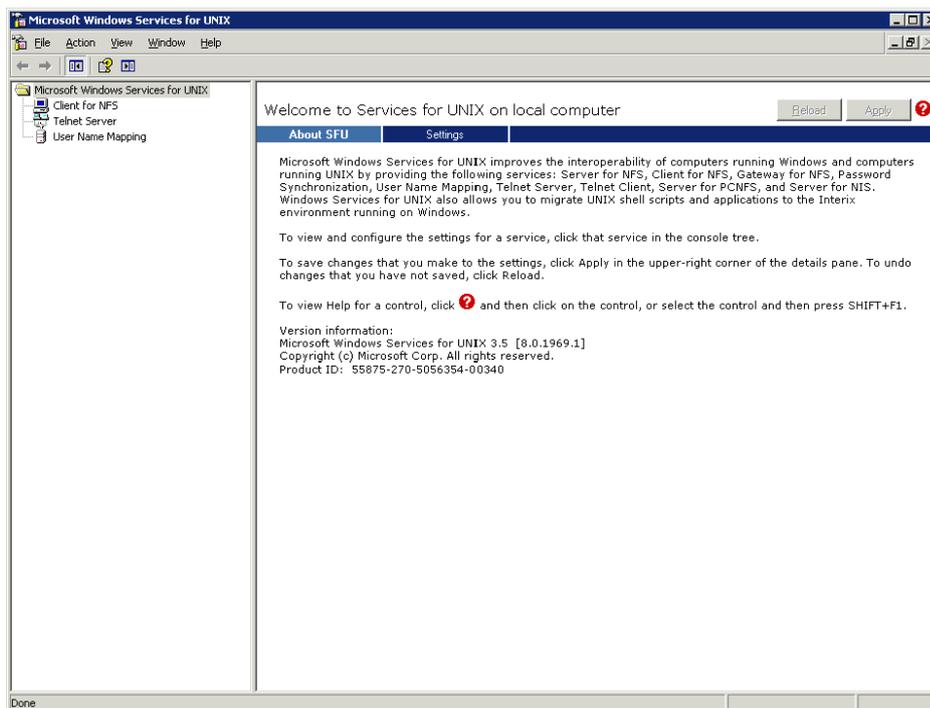


Figure 12 – Microsoft Windows Services for UNIX

There are 3 entries in the left menu:

- **Client for NFS:** allows to define general settings for NFS such as the default permissions for files created in NFS shared folders, but also tuning of the communication protocol between client and server. We won't go into detail for that part.
- **Telnet Server:** this is not useful for us right now
- **User Name Mapping:** in that part, you define mappings between Windows and Linux users. This is the most important part of the configuration, and we will see how to configure it in next part.

## 3.2.2 User-Mapping Configuration

### About User Mapping

In the NFS file-sharing protocol, a client trying to connect to a NFS Server must provide information about its identity, so that the NFS Server knows which permissions the user should be granted. This information is provided as a User ID and Group ID, which are unique identifiers representing users and groups on a given Linux server. As these notions don't exist on Windows platforms, **User-mapping** must be defined in the client side, to associate a Linux User and Group ID to Windows users trying to connect to the NFS server. This is what we will configure in this part.

### Configuring local File-based user-mapping

**Step 1.** Click **User Name Mapping**, to open the following screen:

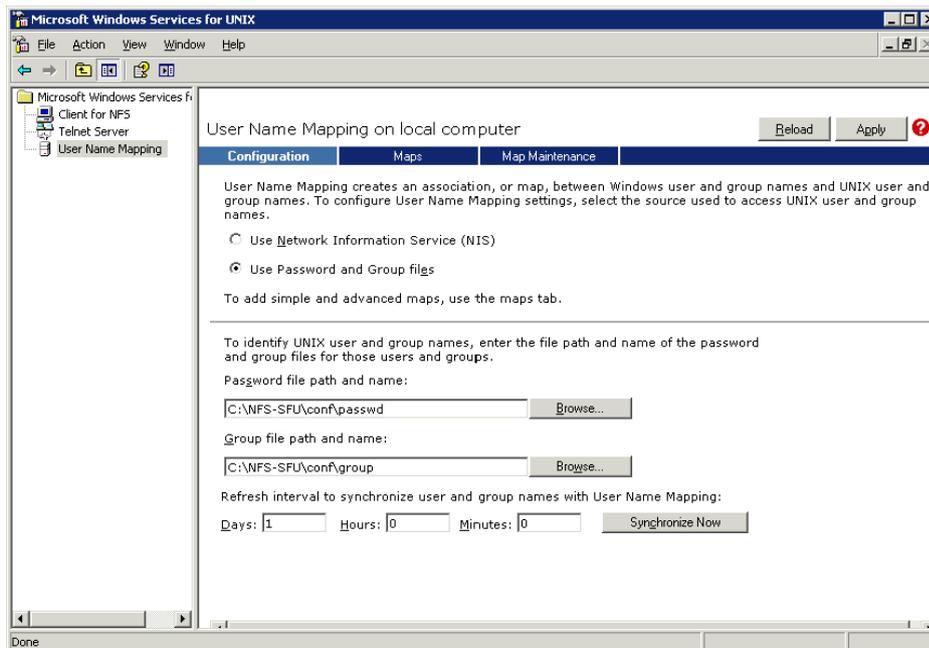


Figure 13 – The password and group files you copied from Linux should appear

**Step 2.** According to what you configured in the installation wizard, the password and group files you copied from Linux should appear. If not, you can still do it now, and select the path where you copied them. Thanks to those files, the NFS client can know which users exist on the Linux Server.

**Step 3.** You can now click the **Maps** tab to configure the Windows-Linux user mapping.

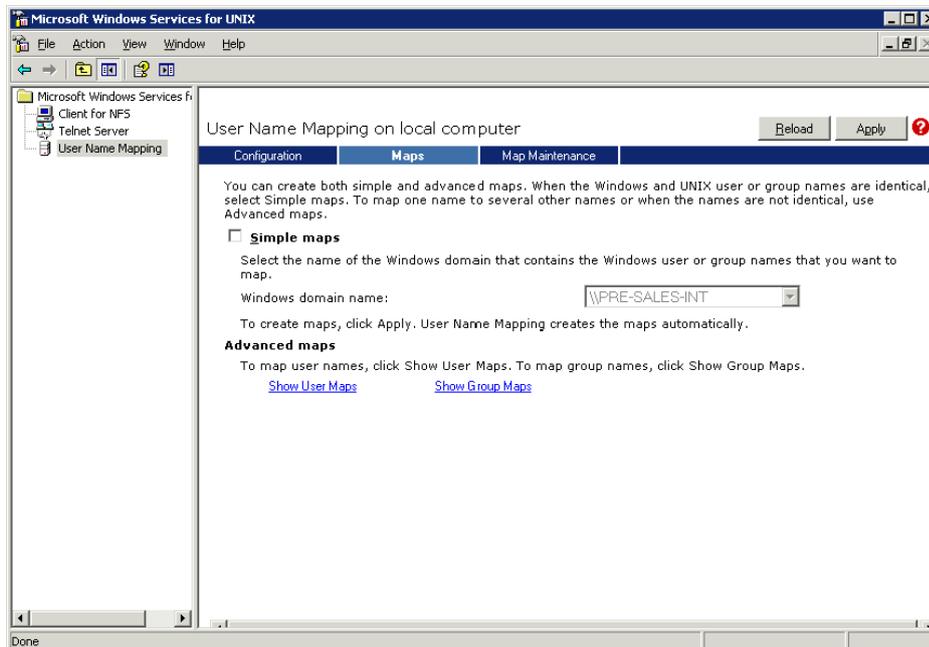


Figure 14 – Maps tab

**Step 4.** If your Windows and Linux users have the same names, you can select the **Simple maps** check box. If not, it is necessary to configure the mapping for each user. This can be done by clicking **Show User Maps**.

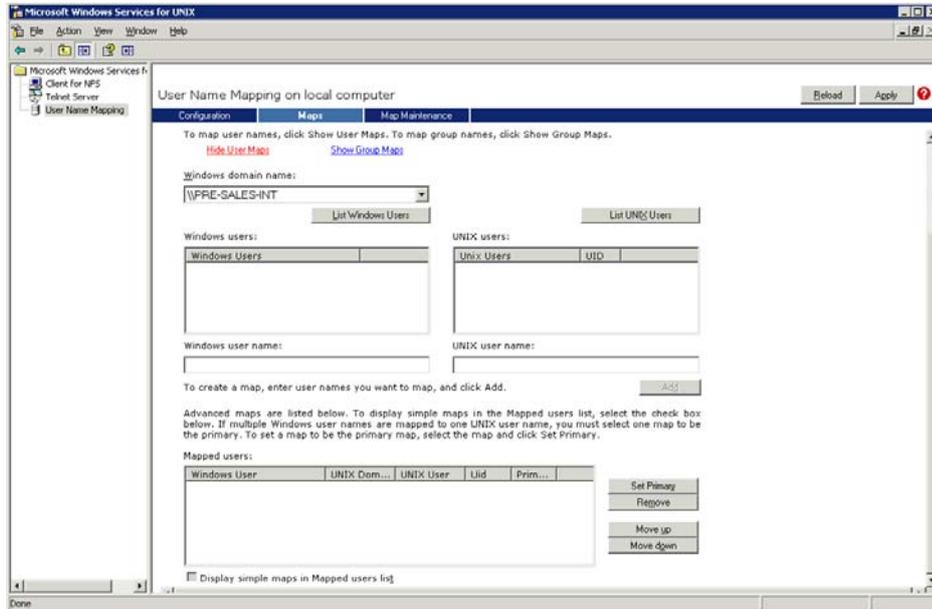


Figure 15 – Configure the mapping for each user

**Step 5.** Select where you want to load Windows groups and users from. It can be a domain or your local machine. Then click **List Windows Users**.

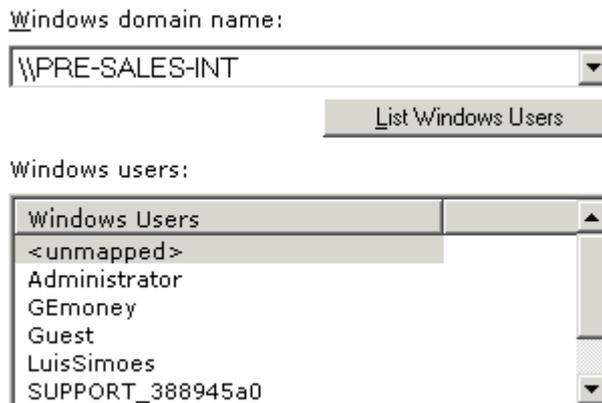


Figure 16 – Select where you want to load Windows groups and users from

**Step 6.** To list the UNIX Users click **List UNIX users**

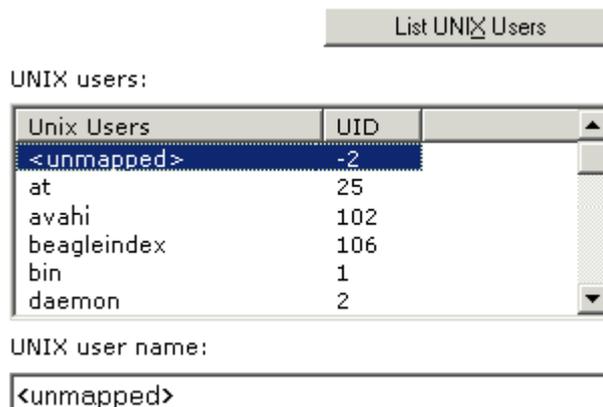


Figure 17 – List UNIX users

- Step 7.** You must now associate Windows users with their Linux equivalent users. To do this, select a user in the Windows list, and a user in the Linux List, and press the **Add** button.

Windows user name:  UNIX user name:

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\PRE-SALES-INT\nfs-user	PCNFS	nobody	65534	*

Figure 18 – Associate Windows users with their Linux equivalent users

- Step 8.** Repeat this operation for each mapping you want to set. You may do similar things with the Group Maps.
- Step 9.** When you are done, click **Apply** to save the settings

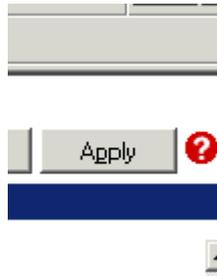


Figure 19 – Click **Apply**

The user-mapping should now be set up. You may now test it.

### Testing the NFS Access

- Step 1.** Log on your computer using the Windows user you used in the mapping configuration.
- Step 2.** Try to connect to the Linux Server, from the Windows explorer, typing `\\IP_Address\.`. The shared folders should appear:

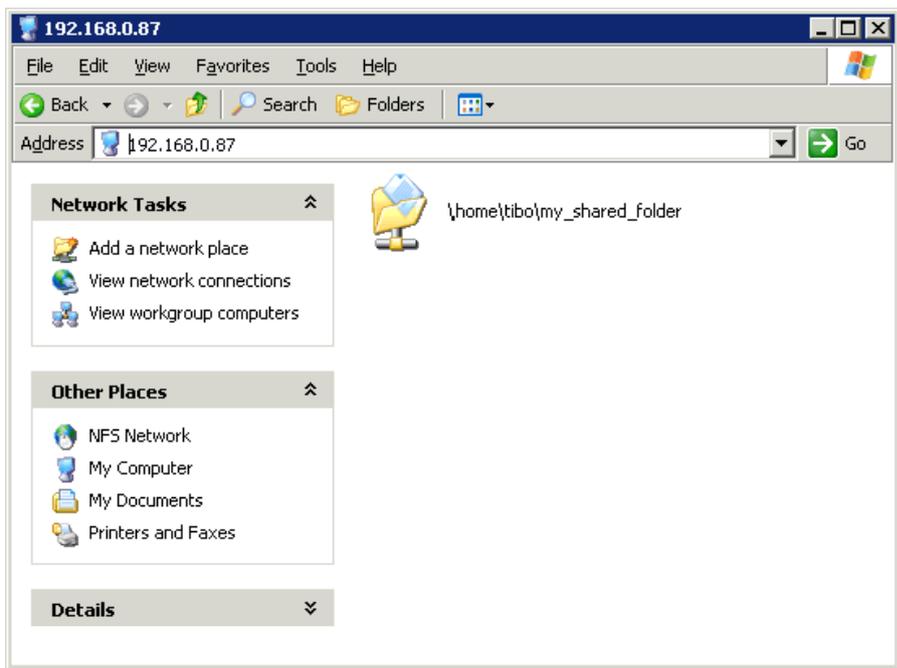


Figure 20 – The shared folders

**Step 3.** Check that you can open the folder to see its content. If you can't, the user mapping may not be properly configured, or the mapped UNIX user doesn't have permissions to access it.

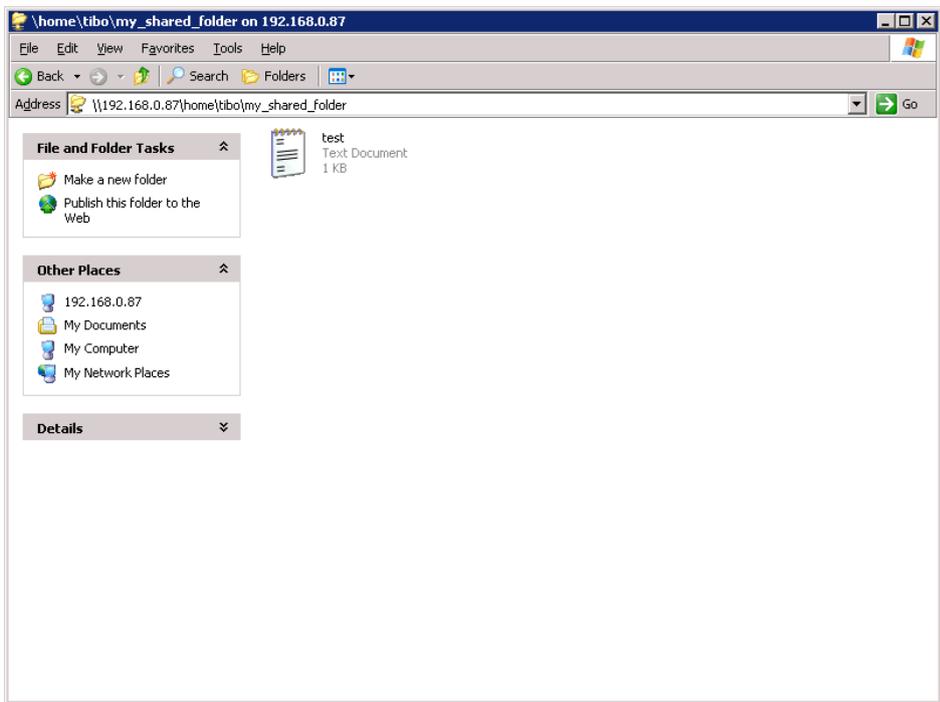


Figure 21 – Check the folder contents

If you can access the folder and its contents, it means you have successfully configured the NFS Server and the NFS Client.

## Configuration of Applications Agent

### 4.1 Linux Server Configuration

For security matters, it is good practice to limit the access to the shared files:

- Allow only access from the server where Applications Agent is running
- Give read-only access as Applications Agent does not need to modify the files it reads
- Use a limited power user for the NFS Access.

This means that the exports configuration file should look like this:

```
/home/tibo/my_shared_folder    192.168.0.158(ro,root_squash)
```

If your files are in the folder `/home/tibo/my_shared_folder` and Applications Agent is running on `192.168.0.158`.

**Note**

Some more advanced configuration options allow to set a user to use for NFS access (anonuid and anonguid). We won't go into details for that part.

### 4.2 Windows Configuration: Applications Agent

At this point, we consider that you have already defined User mappings for at least one Windows user. We will use this user's profile to connect to the NFS shared folder.

- Step 1.** Launch Applications Agent if it is not started already (as a service on a production environment)
- Step 2.** It is important to make it execute with a user profile that is properly mapped in the User Mapping configuration.

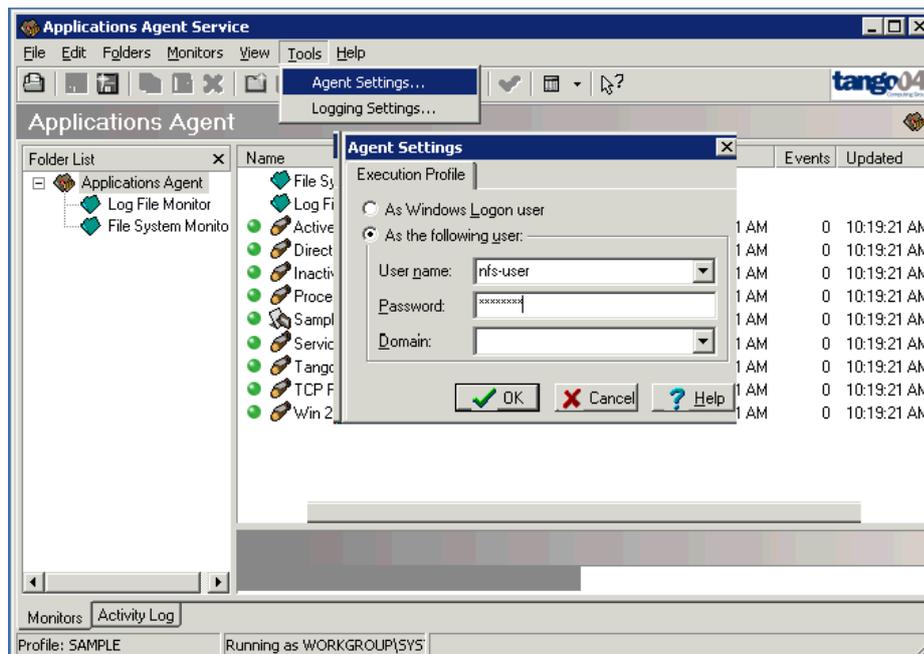


Figure 22 – Agent settings

**Step 3.** Next, save the *Applications Agent Profile*,

**Step 4.** Create a file monitor, putting the path to the file you wish to monitor, in the same form you type it in Windows Explorer.

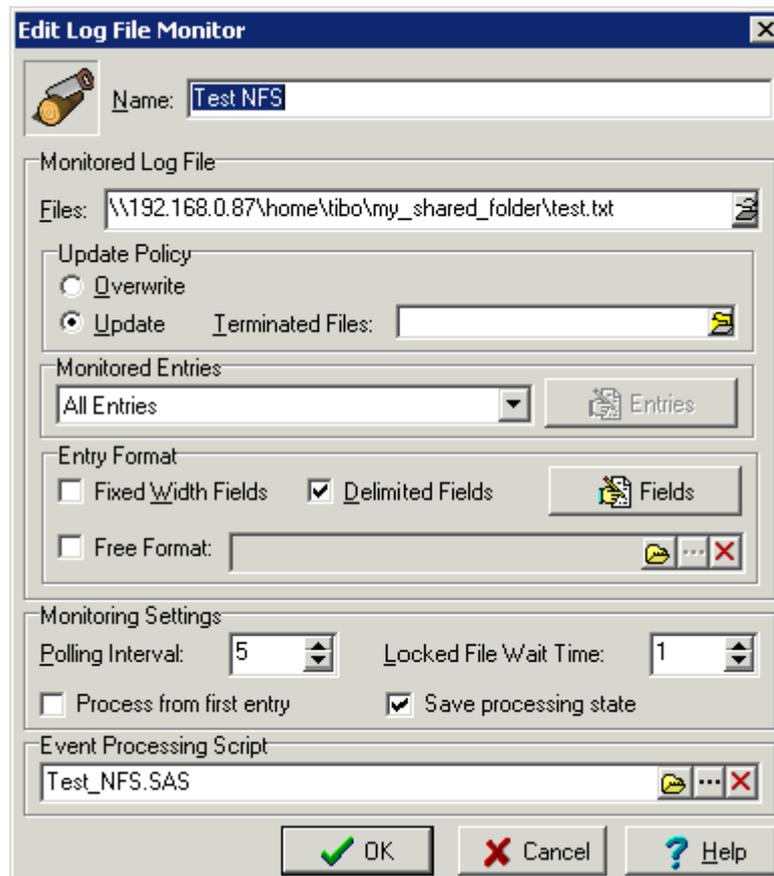


Figure 23 – Edit Log File Monitor

**Step 5.** Select the options you wish. You will be prompted to edit the script. We will keep the default settings.

**Step 6.** Start the monitor, and try to add some lines in the file. Check that some events are generated by Applications Agent.



Figure 24 – Events generated by Applications Agent

**Step 7.** Don't forget to save the Applications profile to avoid losing the changes.

**Step 8.** You can go on configuring your monitor to fit your needs.

## About Tango/04 Computing Group

Tango/04 Computing Group is one of the leading developers of systems management and automation software. Tango/04 software helps companies maintain the operating health of all their business processes, improve service levels, increase productivity, and reduce costs through intelligent management of their IT infrastructure.

Founded in 1991 in Barcelona, Spain, Tango/04 is an IBM Business Partner and a key member of IBM's Autonomic Computing initiative. Tango/04 has more than a thousand customers who are served by over 35 authorized Business Partners around the world.

### Alliances



### Partnerships

- IBM Business Partner
- IBM Autonomic Computing Business Partner
- IBM PartnerWorld for Developers Advanced Membership
- IBM ISV Advantage Agreement
- IBM Early code release
- IBM Direct Technical Liaison
- Microsoft Developer Network
- Microsoft Early Code Release

### Awards



The information in this document was created using certain specific equipment and environments, and it is limited in application to those specific hardware and software products and version and releases levels.

Any references in this document regarding Tango/04 Computing Group products, software or services do not mean that Tango/04 Computing Group intends to make these available in all countries in which Tango/04 Computing Group operates. Any reference to a Tango/04 Computing Group product, software, or service may be used. Any functionally equivalent product that does not infringe any of Tango/04 Computing Group's intellectual property rights may be used instead of the Tango/04 Computing Group product, software or service

Tango/04 Computing Group may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

The information contained in this document has not been submitted to any formal Tango/04 Computing Group test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility, and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. Despite the fact that Tango/04 Computing Group could have reviewed each item for accurateness in a specific situation, there is no guarantee that the same or similar results will be obtained somewhere else. Customers attempting to adapt these techniques to their own environments do so at their own risk. Tango/04 Computing Group shall not be liable for any damages arising out of your use of the techniques depicted on this document, even if they have been advised of the possibility of such damages. This document could contain technical inaccuracies or typographical errors.

Any pointers in this publication to external web sites are provided for your convenience only and do not, in any manner, serve as an endorsement of these web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: iSeries, iSeriese, iSeries, i5, DB2, e (logo)@Server IBM ®, Operating System/400, OS/400, i5/OS.

Microsoft, SQL Server, Windows, Windows NT, Windows XP and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries. UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group. Oracle is a registered trade mark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of other companies.