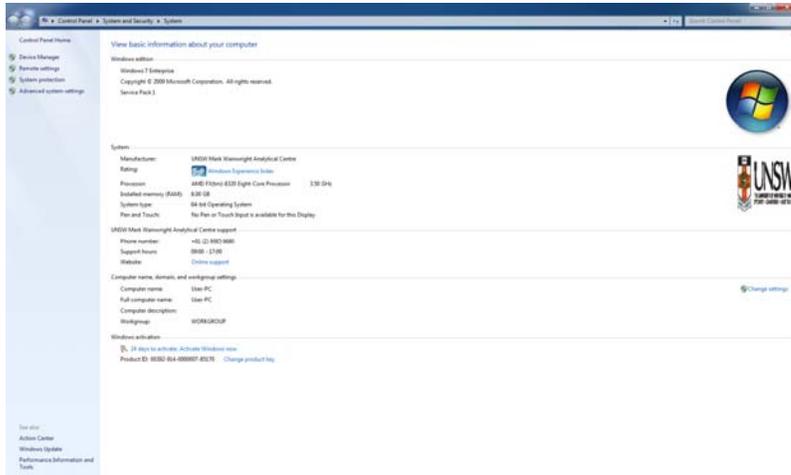


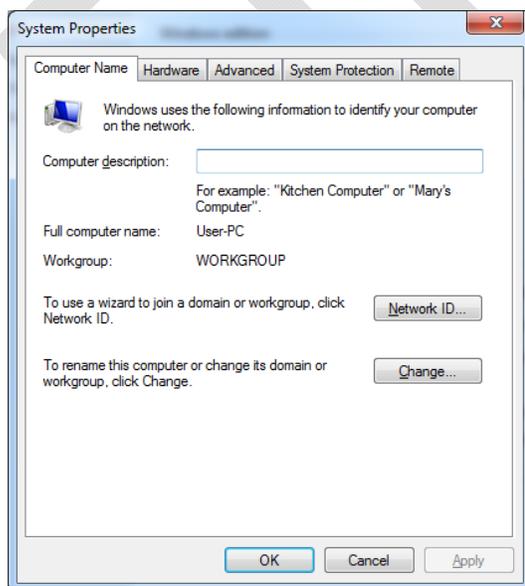
GPFS Installation Notes

1. Install Windows
2. Join domain with the domain administrator account

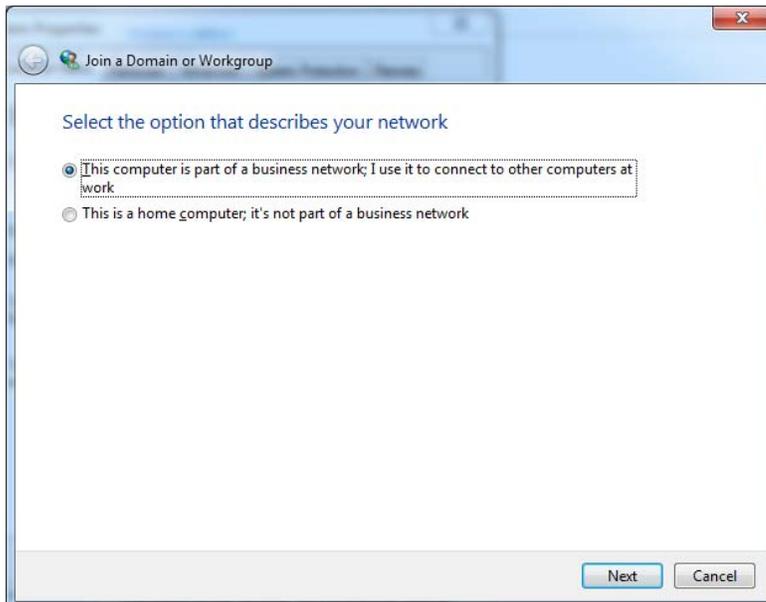
❖ Step 1: go to System



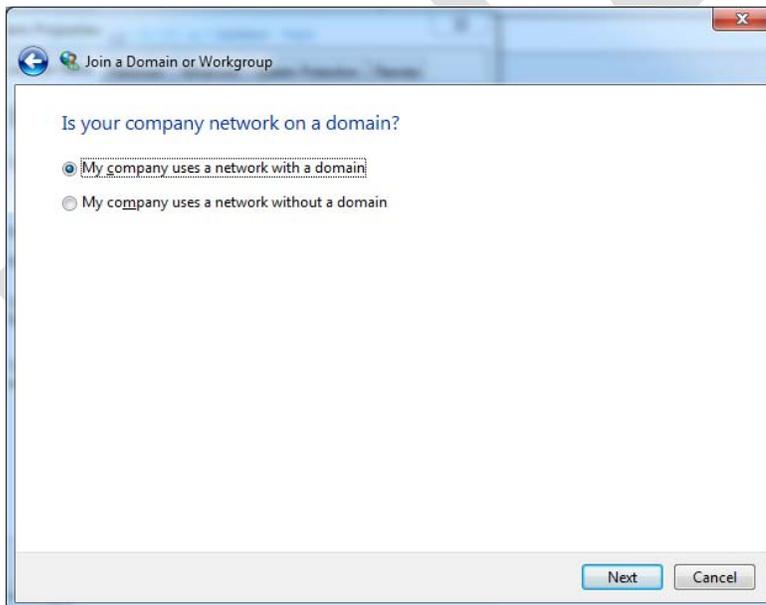
❖ Step 2: Click on Network ID



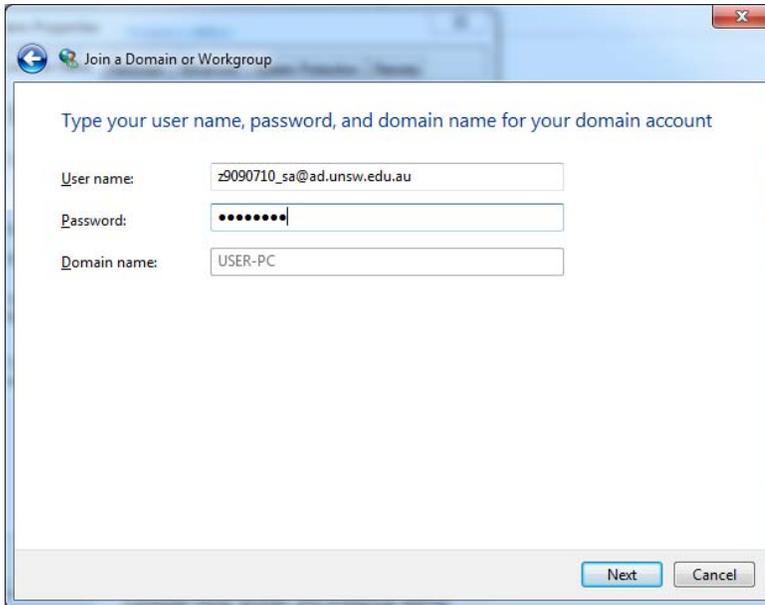
❖ Step 3: Select "This computer is part of business network,....", click next



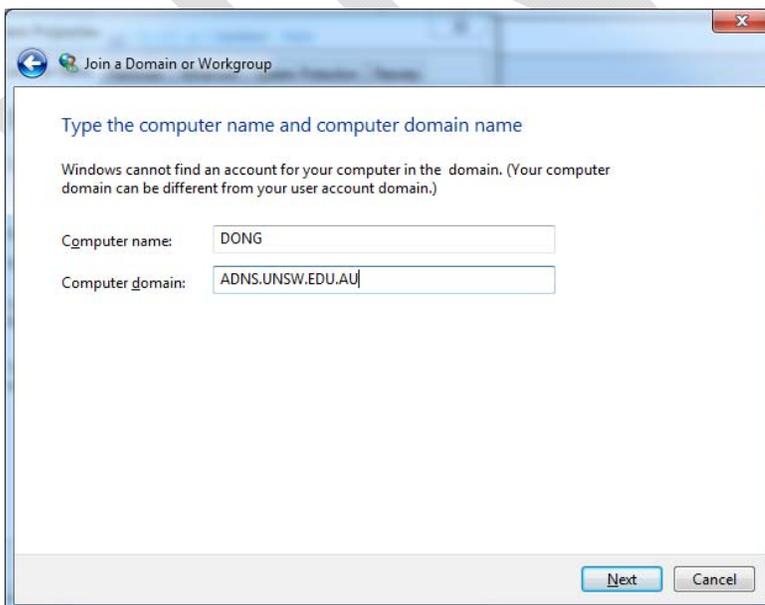
❖ Step 4: Select “My company uses a network with a domain” , click next



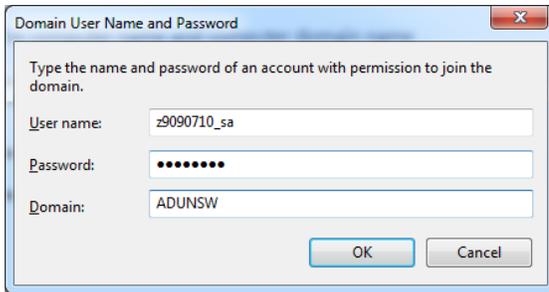
- ❖ Step 5: Enter the User name in the form z123456_sa@ad.unsw.edu.au .. Domain name will then become inactive and should be empty. (enter your password too of course..), click next



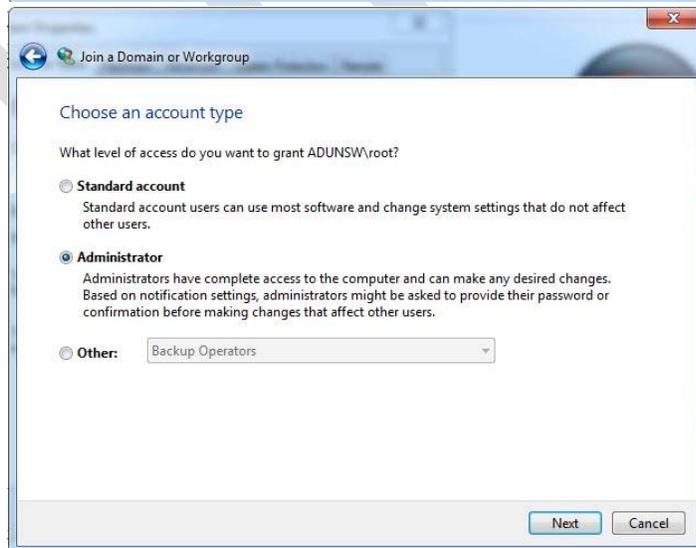
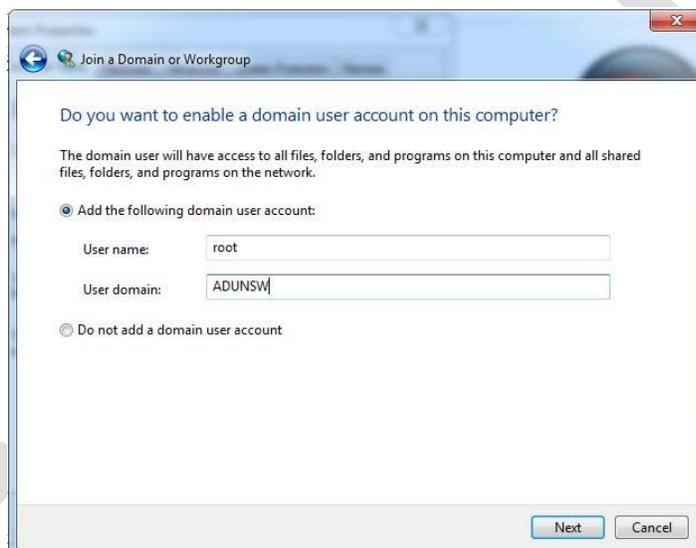
- ❖ Step 6: Computer name: whatever you want to call it, and Computer Domain is ADNS.UNSW.EDU.AU, click Next



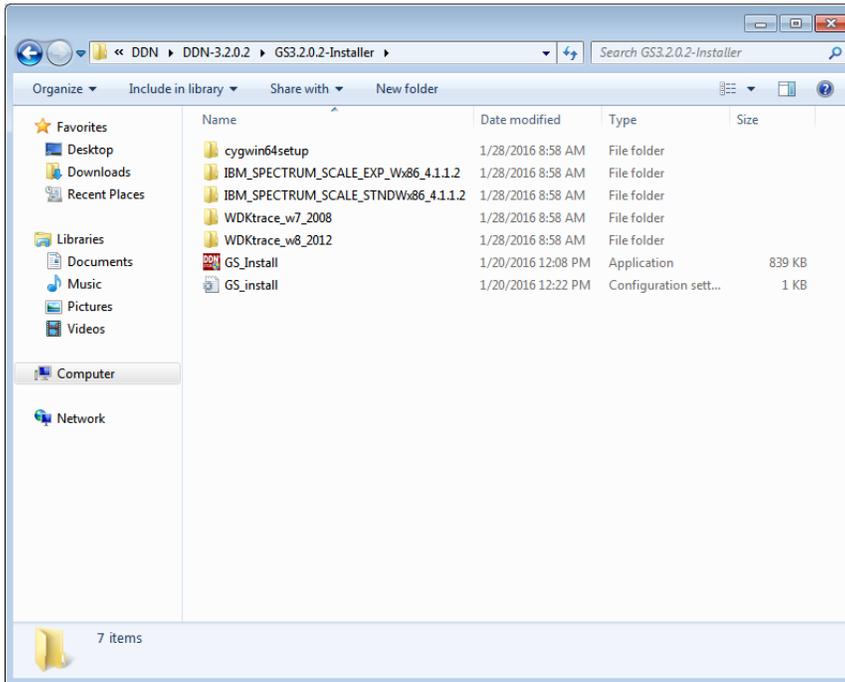
- ❖ Step 7: enter username in the form z123456_sa and Domain ADUNSW, click OK



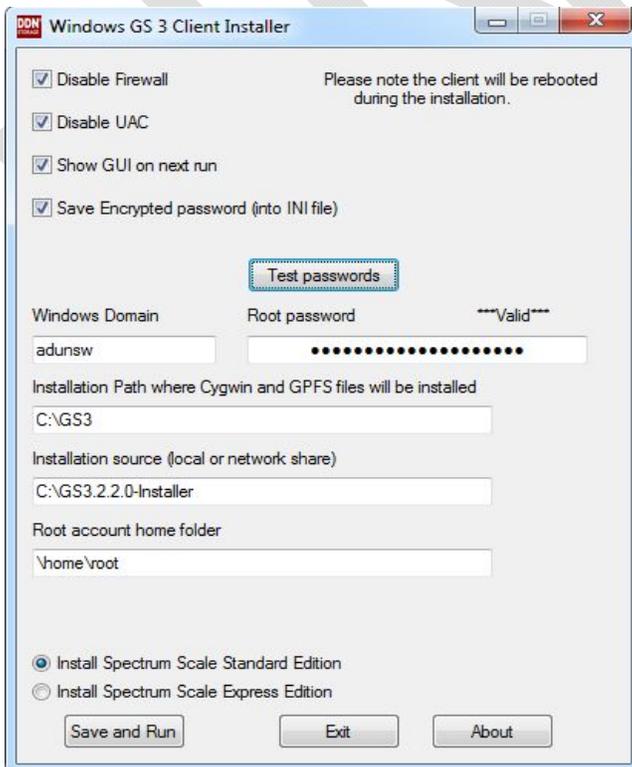
- ❖ Step 8: Add the AD root account put in 'root' for username and "ADUNSW" for domain. the only thing is now when you restart the computer it will try to log you on to the domain (which is where i got a bit confused) and you'll need to put LIFTOUT-PC\liftout as the username in order to log back in to the local admin account.



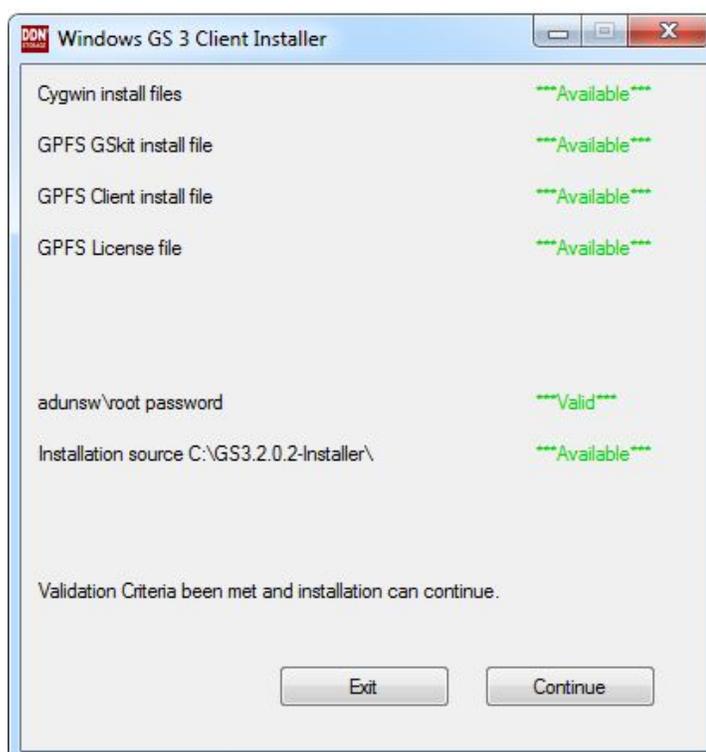
3. While logged in as the local machine admin, run GPFS auto-run installer



4. Enter domain name and root password to continue. Ensure that you use “Test passwords”



5. Click save and run and you should have the following output



6. Installation does two reboot automatically, the process may take up to 5 minutes to complete. DO NOT LOGIN and interrupt. After second reboot, login as domain\root
7. Upon the completion of installation, you see the following desktop, including:



8. Fix for incorrect username follows, this might be fixed in future with a domain alternation. Run the following commands, taking note to substitute the correct root password.
 - 8.1 `mkpasswd -c >> /etc/passwd`
 - 8.2 `sed -i 's/ADUNSW+root/root/' /etc/passwd`
 - 8.3 exit out of the Admin Korn Shell and start it up again
 - 8.4 Stop the ssh server with:
 - 8.5 Remove the ssh server with:
 - 8.6 `ssh-host-config -y -u root -w "ROOT Password HERE"`

```
GPFS Admin Korn Shell
ADUNSW+root@egpfs2-pc:~ $ mkpasswd -c >> /etc/passwd
ADUNSW+root@egpfs2-pc:~ $ sed -i 's/ADUNSW+root/root/' /etc/passwd
ADUNSW+root@egpfs2-pc:~ $ ssh-host-config -y -u root -w " "

*** Info: Generating missing SSH host keys
*** Query: Overwrite existing /etc/ssh_config file? (yes/no) yes
*** Info: Creating default /etc/ssh_config file
*** Query: Overwrite existing /etc/sshd_config file? (yes/no) yes
*** Info: Creating default /etc/sshd_config file

*** Info: StrictModes is set to 'yes' by default.
*** Info: This is the recommended setting, but it requires that the POSIX
*** Info: permissions of the user's home directory, the user's .ssh
*** Info: directory, and the user's ssh key files are tight so that
*** Info: only the user has write permissions.
*** Info: On the other hand, StrictModes don't work well with default
*** Info: Windows permissions of a home directory mounted with the
*** Info: 'noacl' option, and they don't work at all if the home
*** Info: directory is on a FAT or FAT32 partition.
*** Query: Should StrictModes be used? (yes/no) yes

*** Info: Privilege separation is set to 'sandbox' by default since
*** Info: OpenSSH 6.1. This is unsupported by Cygwin and has to be set
*** Info: to 'yes' or 'no'.
*** Info: However, using privilege separation requires a non-privileged account
*** Info: called 'sshd'.
*** Info: For more info on privilege separation read /usr/share/doc/openssh/README.privsep.
*** Query: Should privilege separation be used? (yes/no) yes
*** Info: Updating /etc/sshd_config file

*** Query: Do you want to install sshd as a service?
*** Query: (Say "no" if it is already installed as a service) (yes/no) yes
*** Query: Enter the value of CYGWIN for the daemon: []
*** Info: On Windows Server 2003, Windows Vista, and above, the
*** Info: SYSTEM account cannot be set to other users -- a capability
*** Info: sshd requires. You need to have or to create a privileged
*** Info: account. This script will help you do so.

*** Info: It's not possible to use the LocalSystem account for services
*** Info: that can change the user id without an explicit password
*** Info: (such as passwordless logins [e.g. public key authentication]
*** Info: via sshd) when having to create the user token from scratch.
*** Info: For more information on this requirement, see
*** Info: https://cygwin.com/cygwin-ug-net/ntsec.html#ntsec-nopasswd1

*** Info: If you want to enable that functionality, it's required to create
*** Info: a new account with special privileges (unless such an account
*** Info: already exists). This account is then used to run these special
*** Info: servers.

*** Info: Note that creating a new user requires that the current account
*** Info: have Administrator privileges itself.

*** Info: This script plans to use 'root'.
*** Info: 'root' will only be used by registered services.

*** Info: The sshd service has been installed under the 'root'
*** Info: account. To start the service now, call 'net start sshd' or
*** Info: 'cygrunsrv -S sshd'. Otherwise, it will start automatically
*** Info: after the next reboot.

*** Info: Host configuration finished. Have fun!
ADUNSW+root@egpfs2-pc:~ $
```

8.7 Start the ssh server with: cygrunsrv --start sshd

```

GPFs Admin Korn Shell
*** Info: SYSTEM account cannot setuid to other users -- a capability
*** Info: sshd requires. You need to have or to create a privileged
*** Info: account. This script will help you do so.

*** Info: It's not possible to use the LocalSystem account for services
*** Info: that can change the user id without an explicit password
*** Info: (such as passwordless logins [e.g. public key authentication]
*** Info: via sshd) when having to create the user token from scratch.
*** Info: For more information on this requirement, see
*** Info: https://cygwin.com/cygwin-ug-net/ntsec.html#ntsec-nopasswdl

*** Info: If you want to enable that functionality, it's required to create
*** Info: a new account with special privileges (unless such an account
*** Info: already exists). This account is then used to run these special
*** Info: servers.

*** Info: Note that creating a new user requires that the current account
*** Info: have Administrator privileges itself.

*** Info: This script plans to use 'root'.
*** Info: 'root' will only be used by registered services.

*** Info: The sshd service has been installed under the 'root'
*** Info: account. To start the service now, call 'net start sshd' or
*** Info: 'cygrunsrv -S sshd'. Otherwise, it will start automatically
*** Info: after the next reboot.

*** Info: Host configuration finished. Have fun!
ADUNSW+root@gpfs2-pc:~ $ cygrunsrv --start sshd
ADUNSW+root@gpfs2-pc:~ $ ssh root@129.94.120.62
The authenticity of host '129.94.120.62 (129.94.120.62)' can't be established.
RSA key fingerprint is SHA256:Dbwx3infLUbM8zdM4Wkt+C3hDawcPWROYSubG0Quz10.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '129.94.120.62' (RSA) to the list of known hosts.
root@129.94.120.62's password:
Last login: Wed Aug 31 15:30:58 2016 from gpfs02
[root@ls-vm1 ~]#

```

9. Create a local ssh key with, "ssh-keygen -t rsa", then press enter to get the defaults
10. ssh to DDN VM at 129.94.120.62 as root via GPFs Admin Korn Shell "ssh 129.94.120.62"
11. Edit /etc/hosts and ensure that the ip address of the new client is there

```

GPFs Admin Korn Shell
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1        localhost localhost.localdomain localhost6 localhost6.localdomain6
129.94.120.62    ls-vm1
129.94.120.61    ls-vm2
129.94.120.60    ls-vm3
129.94.120.59    ls-vm4
129.94.120.57    Z7-00079
129.94.165.35    gsclient21
129.94.164.87    gsclient22
129.94.120.38    gs7kc0
129.94.120.39    gs7kc1
129.94.120.27    master mwacddn
129.94.165.33    lecia01
129.94.165.36    gpfs02

"/etc/hosts" [dos] 15L, 473C

```

12. Copy this file back to the client machine

```

[root@ls-vm1 ~]# vi /etc/hosts
[root@ls-vm1 ~]# scp .ssh/authorized_keys gpfs02:.ssh
The authenticity of host 'gpfs02 (129.94.165.36)' can't be established.
RSA key fingerprint is df:97:74:9d:84:80:cb:af:cc:43:cc:bd:0c:dc:94:2e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'gpfs02,129.94.165.36' (RSA) to the list of known hosts.
root@gpfs02's password:
authorized_keys                                100% 1783      1.7KB/s   00:00
[root@ls-vm1 ~]# scp /etc/hosts gpfs02:
hosts                                           100% 473       0.5KB/s   00:00
[root@ls-vm1 ~]# _

```

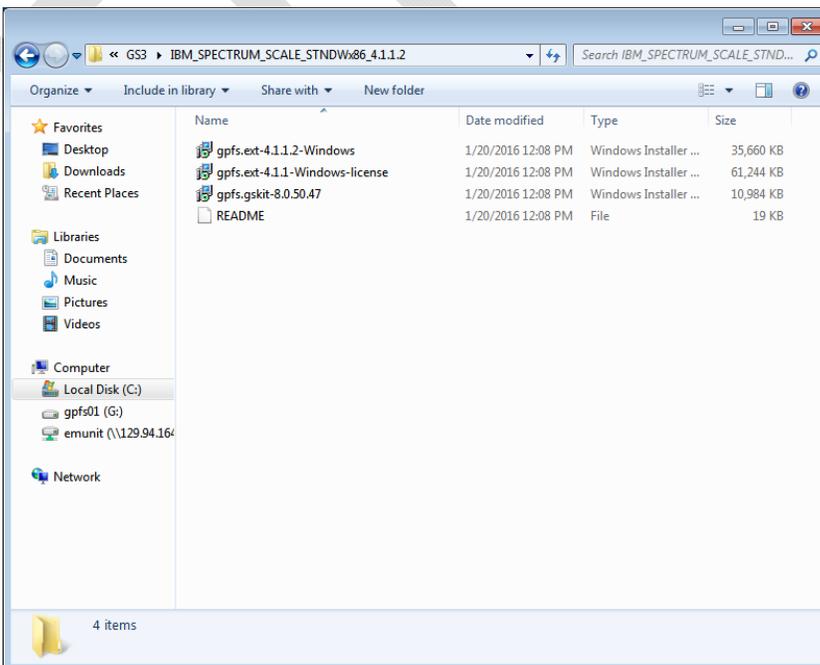
13. Copy the vm's authorized_keys file to the client with the command "scp ~/.ssh/authorized_keys gpfs02:/root/.ssh/"
14. In another shell on the client, add the contents of the hosts file that you just copied to the local machines hosts file using: cat hosts >> /cygdrive/c/windows/system32/drivers/etc/hosts

```

GPFS Admin Korn Shell
root@gpfs2-pc:~ $ cat hosts >> /cygdrive/c/windows/system32/drivers/etc/hosts
root@gpfs2-pc:~ $

```

15. If the node already exists on the GPFS cluster (node reinstallation), then you can add it back to the cluster, using the commands as shown bellow
 - 15.1 [root@ls-vm1 ~]# mmauth genkey propagate -N gpfs02
 - 15.2 [root@ls-vm1 ~]# mmsdrrestore -N gpfs02
 - 15.3 [root@ls-vm1 ~]# mmstartup -N gpfs02
16. If auto-installation not working properly, go to GS3 folder to run 3 programs from the top one by one.



17. Add client node to GPFS with "mmaddnode -N gpfs02" and then accept the license "mmchlicense client --accept -N gpfs02"

```

GPFS Admin Korn Shell
root@gpfs2-pc:~$ ssh ls-vm1
The authenticity of host 'ls-vm1 (129.94.120.62)' can't be established.
RSA key fingerprint is SHA256:Dbwx31nfLUBM8zdM4Wkt+C3hDawcPWROYSUBG0Quz10.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ls-vm1' (RSA) to the list of known hosts.
root@ls-vm1's password:
Last login: Wed Aug 31 17:06:05 2016 from gpfs02
[root@ls-vm1 ~]# mmaddnode -N gpfs02
Wed Aug 31 17:23:24 AEST 2016: mmaddnode: Processing node gpfs02
mmaddnode: Command successfully completed
mmaddnode: Warning: Not all nodes have proper GPFS license designations.
Use the mmchlicense command to designate licenses as needed.
mmaddnode: Propagating the cluster configuration data to all
affected nodes. This is an asynchronous process.
[root@ls-vm1 ~]# mmchlicense client --accept -N gpfs02

The following nodes will be designated as possessing GPFS client licenses:
gpfs02
mmchlicense: Command successfully completed
mmchlicense: Propagating the cluster configuration data to all
affected nodes. This is an asynchronous process.
[root@ls-vm1 ~]# _

```

18. To start up node, type "mmstartup" and enter on the local node terminal
19. Check gpfs02 status, type "mmgetstate" to confirm if gpfs02 is active, if not, just wait and check again till gsclient becomes active

```

mmchlicense: Propagating the cluster configuration data to all
affected nodes. This is an asynchronous process.
[root@ls-vm1 ~]# mmstartup -N gpfs02
Wed Aug 31 17:25:15 AEST 2016: mmstartup: Starting GPFS ...
[root@ls-vm1 ~]# mmgetstate -N gpfs02

```

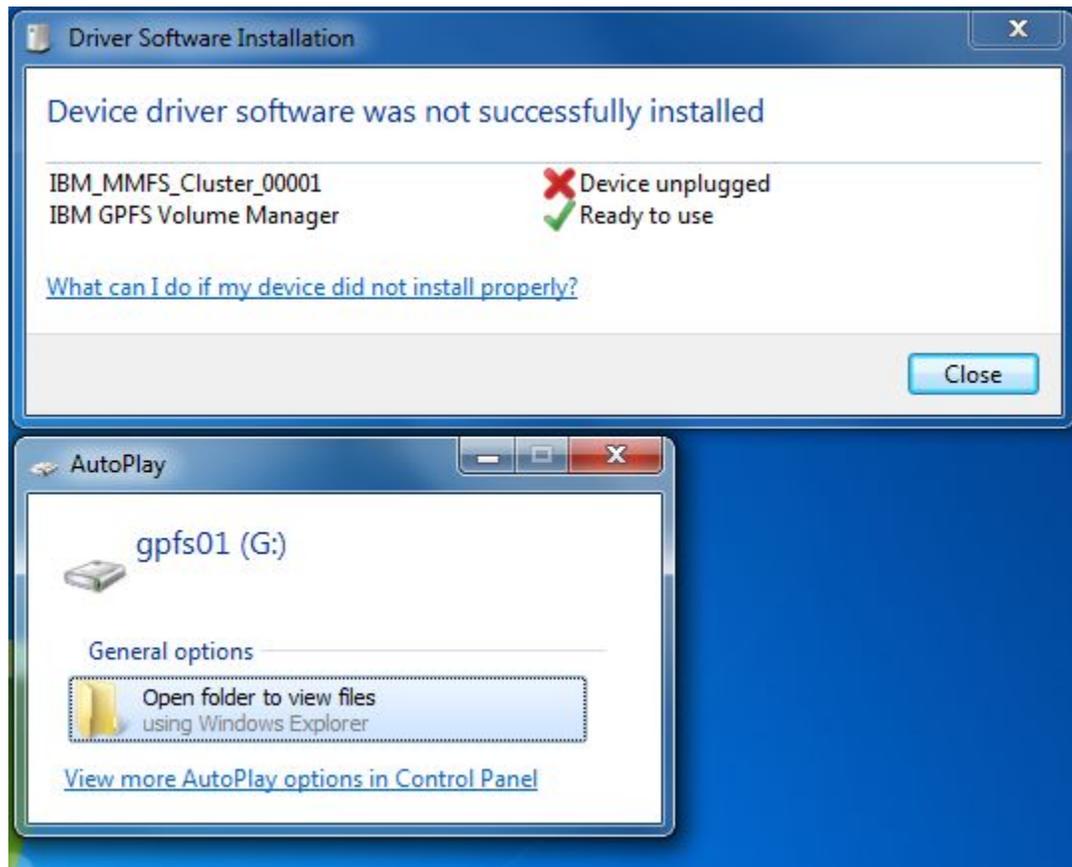
Node number	Node name	GPFS state
12	gpfs02	active

```

[root@ls-vm1 ~]#

```

20. mount gpfs, type "mmmount gpfs01" and enter on the local terminal, it may take 2 minutes to mount. You may need to click on the Windows driver prompt and tell it to accept the gpfs client driver



21. After reboot, G drive may take a 2 minutes to shown up on My Computer depending on the pc and network performance