

# Operating Systems Coursework

---

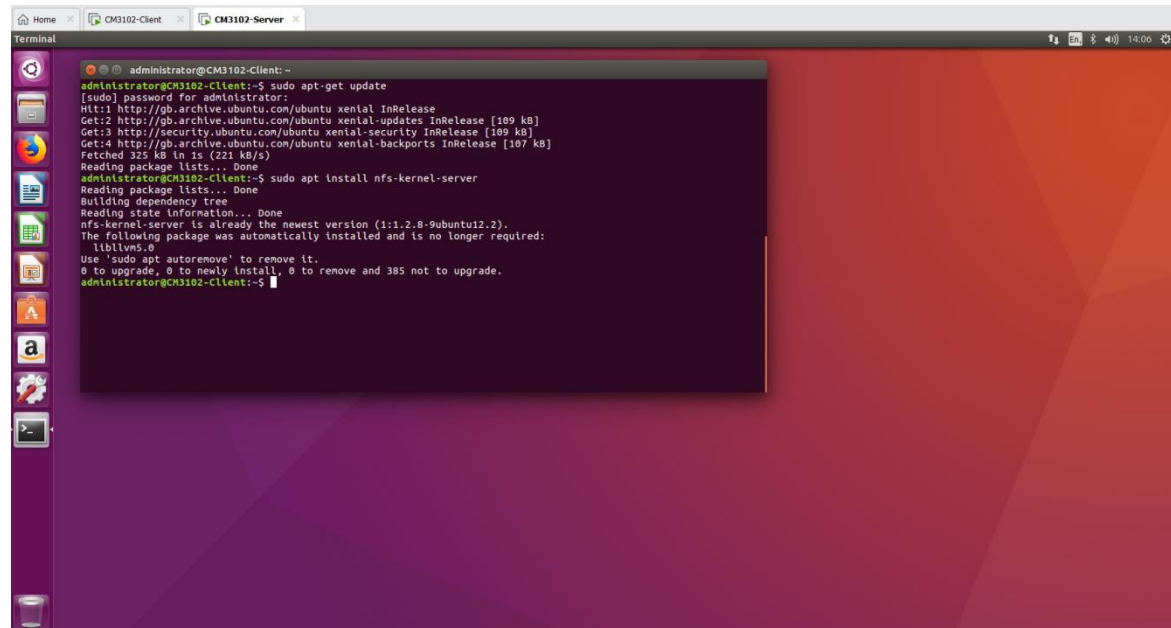
## Part 2 – Operating Systems Services and Related Tools

**Darie-Dragos Mitoiu**

**11/20/2019**

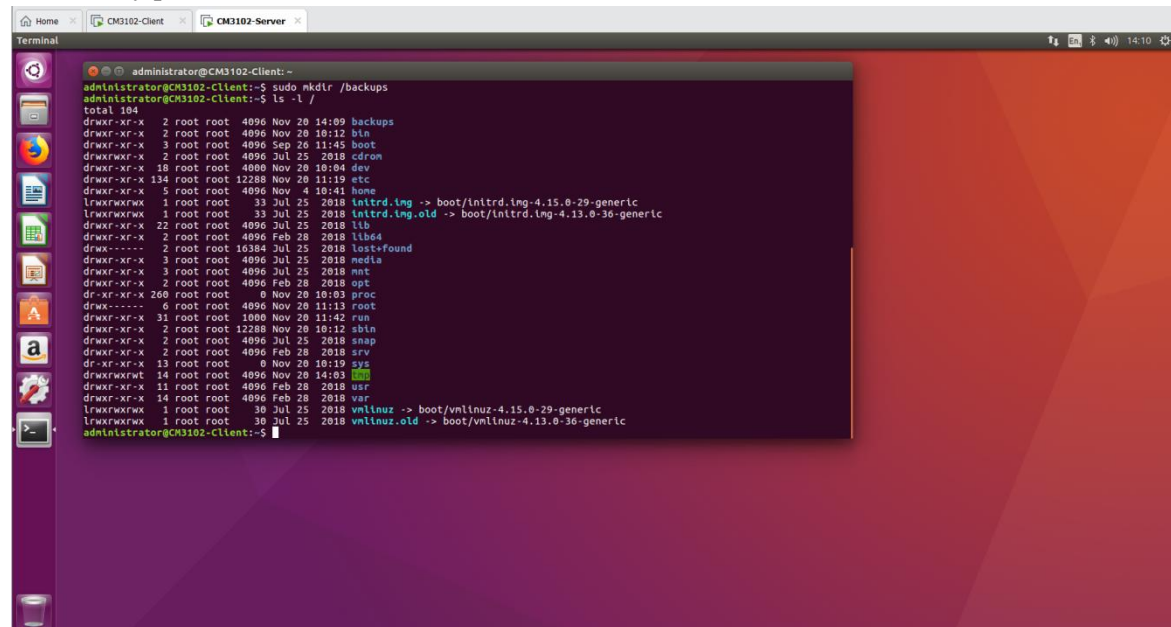
1.

1.1



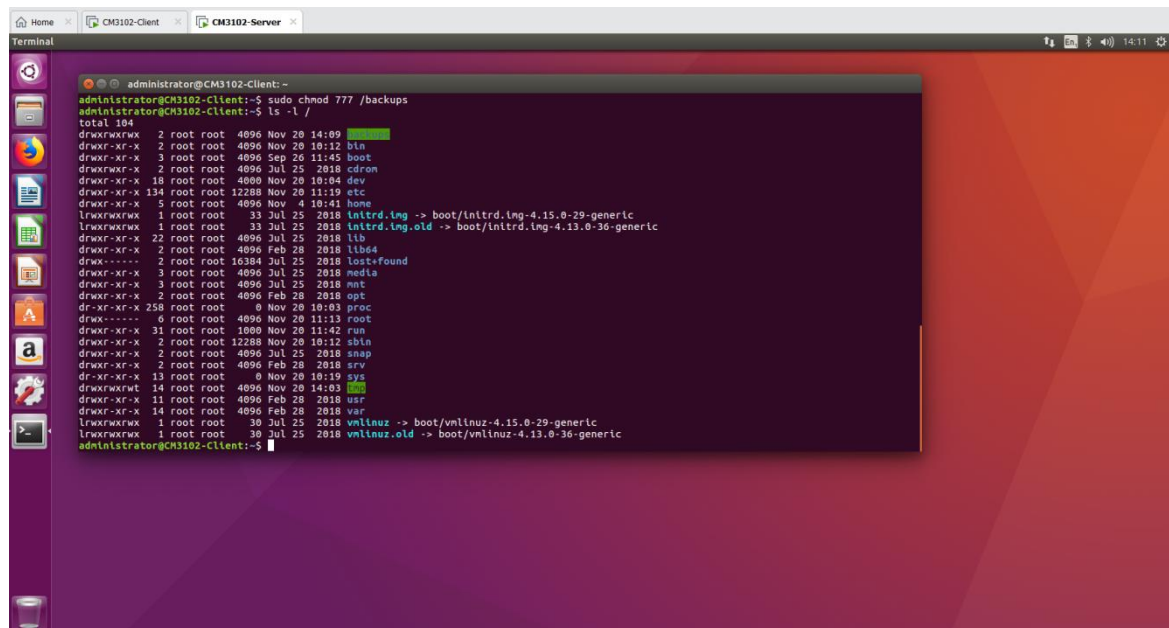
```
administrator@CM3102-Client:~$ sudo apt-get update
[sudo] password for administrator:
Hit:1 http://gb.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://gb.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Fetched 355 kB in 1s (221 kB/s)
Reading package lists... Done
administrator@CM3102-Client:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
nfs-kernel-server is already the newest version (1:1.2.0-9ubuntu12.2).
The following package was automatically installed and is no longer required:
  liblvm2-0
Use 'sudo apt autoremove' to remove it.
0 to upgrade, 0 to newly install, 0 to remove and 385 not to upgrade.
administrator@CM3102-Client:~$
```

In order to setup the network file system (NTF) mount, the following commands must be executed on the server virtual machine: “sudo apt-get update”, “sudo apt install nfs-kernel-server”. The command “sudo apt-get update” will update the system’s repository and the command “sudo apt install nfs-kernel-server” will install the network file system server on the server virtual machine. In the image from above the installation of the network file system server was already performed.



```
administrator@CM3102-Client:~$ sudo mkdir /backups
administrator@CM3102-Client:~$ ls -l /
total 104
drwxr-xr-x  2 root root 4096 Nov 20 14:09 backups
drwxr-xr-x  2 root root 4096 Nov 20 10:12 bin
drwxr-xr-x  3 root root 4096 Sep 26 11:45 boot
drwxrwxr-x  2 root root 4096 Jul 25 2018 cdrom
drwxr-xr-x 18 root root 4080 Nov 20 10:04 dev
drwxr-xr-x 134 root root 12288 Nov 20 11:19 etc
drwxr-xr-x  5 root root 4096 Nov  4 10:41 home
lrwxrwxrwx  1 root root   33 Jul 25 2018 initrd.img -> boot/initrd.img-4.15.0-29-generic
drwxr-xr-x 22 root root 4096 Jul 25 2018 lib
drwxr-xr-x  2 root root 4096 Feb 28 2018 lib64
drwx----- 2 root root 16384 Jul 25 2018 lost+found
drwxr-xr-x  3 root root 4096 Jul 25 2018 media
drwxr-xr-x  3 root root 4096 Jul 25 2018 mnt
drwxr-xr-x  2 root root 4096 Feb 28 2018 opt
dr-xr-xr-x 260 root root   0 Nov 20 10:03 proc
drwx----- 0 root root 4096 Nov 20 11:13 root
drwxr-xr-x 31 root root 1000 Nov 20 11:42 run
drwxr-xr-x  2 root root 12288 Nov 20 10:12 sbin
drwxr-xr-x  2 root root 4096 Jul 25 2018 snap
drwxr-xr-x  2 root root 4096 Feb 28 2018 srv
dr-xr-xr-x 13 root root   0 Nov 20 10:19 sys
drwxrwxrwt 14 root root 4096 Nov 20 14:03 tmp
drwxr-xr-x 13 root root 4096 Feb 28 2018 usr
drwxr-xr-x 14 root root 4096 Feb 28 2018 var
lrwxrwxrwx  1 root root   30 Jul 25 2018 vmlinuz -> boot/vmlinuz-4.15.0-29-generic
lrwxrwxrwx  1 root root   30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.13.0-36-generic
administrator@CM3102-Client:~$
```

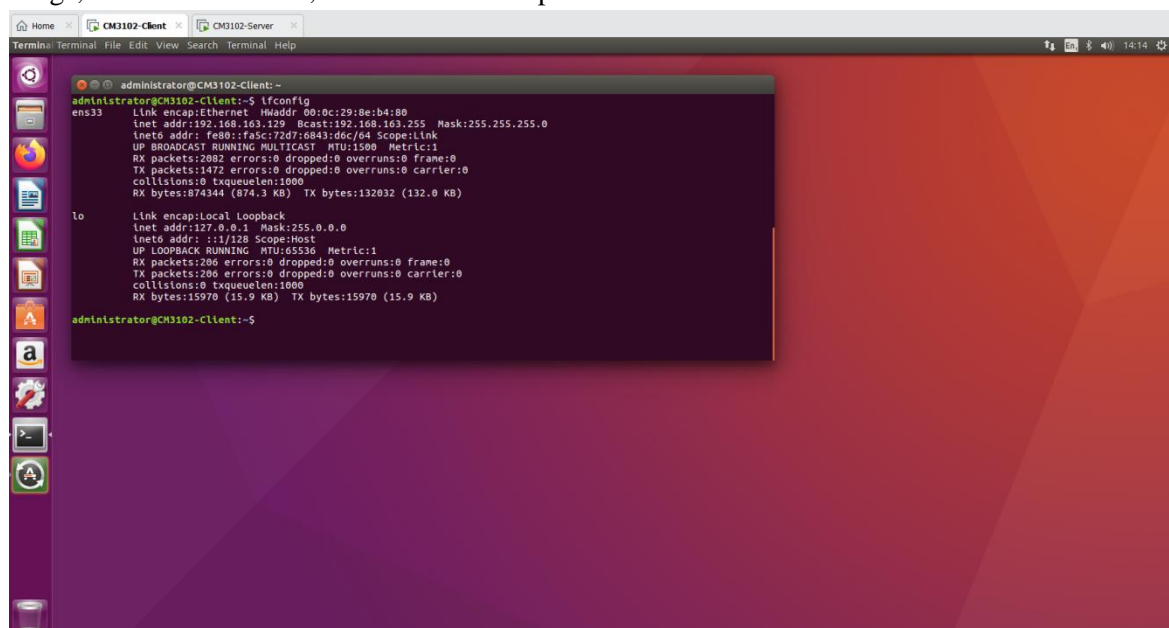
In order to create the “/backups” directory on the server virtual machine, the following commands must be executed: “sudo mkdir /backups”, “ls -l /”. The command “sudo mkdir /backups” will allow the creation of the “/backups” directory and the command “ls -l /” will confirm the operation was completed with success.



The image shows a terminal window on a Linux desktop environment. The terminal is titled 'administrator@CM3102-Client:~'. The user has executed the command 'sudo chmod 777 /backups' and then 'ls -l /'. The output shows the permissions for the root directory and its contents, including 'boot', 'cdrom', 'dev', 'etc', 'home', 'initrd.img', 'lib', 'lib64', 'lost+found', 'media', 'mnt', 'opt', 'proc', 'root', 'run', 'sbin', 'snap', 'srv', 'sys', 'usr', 'var', and 'vmlinuz'. The permissions for the root directory are 'drwxr-xr-x 1 root root 4096 Nov 20 14:09 /'. The permissions for the 'backups' directory are 'drwxr-xr-x 2 root root 4096 Nov 20 10:12 backups'.

```
administrator@CM3102-Client:~$ sudo chmod 777 /backups
administrator@CM3102-Client:~$ ls -l /
total 104
drwxr-xr-x 2 root root 4096 Nov 20 14:09 /
drwxr-xr-x 2 root root 4096 Nov 20 10:12 bin
drwxr-xr-x 3 root root 4096 Sep 26 11:45 boot
drwxr-xr-x 2 root root 4096 Jul 25 2018 cdrom
drwxr-xr-x 18 root root 4096 Nov 20 19:04 dev
drwxr-xr-x 134 root root 12288 Nov 20 11:19 etc
drwxr-xr-x 5 root root 4096 Nov 4 18:41 home
lrwxrwxrwx 1 root root 33 Jul 25 2018 initrd.img -> boot/initrd.img-4.15.0-29-generic
lrwxrwxrwx 1 root root 33 Jul 25 2018 initrd.img.old -> boot/initrd.img-4.13.0-36-generic
drwxr-xr-x 22 root root 4096 Jul 25 2018 lib
drwxr-xr-x 2 root root 4096 Feb 28 2018 lib64
drwxr-xr-x 2 root root 16384 Jul 25 2018 lost+found
drwxr-xr-x 3 root root 4096 Jul 25 2018 media
drwxr-xr-x 3 root root 4096 Jul 25 2018 mnt
drwxr-xr-x 2 root root 4096 Feb 28 2018 opt
drwxr-xr-x 258 root root 0 Nov 20 10:03 proc
drwxr-xr-x 6 root root 4096 Nov 20 11:13 root
drwxr-xr-x 31 root root 1088 Nov 20 11:42 run
drwxr-xr-x 2 root root 12288 Nov 20 10:12 sbin
drwxr-xr-x 2 root root 4096 Jul 25 2018 snap
drwxr-xr-x 2 root root 4096 Feb 28 2018 srv
drwxr-xr-x 13 root root 0 Nov 20 10:19 sys
drwxrwxrwt 14 root root 4096 Nov 20 14:03 tmp
drwxr-xr-x 11 root root 4096 Feb 28 2018 usr
drwxr-xr-x 14 root root 4096 Feb 28 2018 var
lrwxrwxrwx 1 root root 30 Jul 25 2018 vmlinuz -> boot/vmlinuz-4.15.0-29-generic
lrwxrwxrwx 1 root root 30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.13.0-36-generic
administrator@CM3102-Client:~$
```

In order to give write and read permission to all the users present on the client virtual machine, the following commands must be executed: “sudo chmod 777 /backups”, “ls -l /”. The command “sudo chmod 777 /backups” will give full control (read, write and execute permissions) to all users, the command “ls -l /” will confirm the previous command, as we can see in the above image, all users have read, write and execute permission.



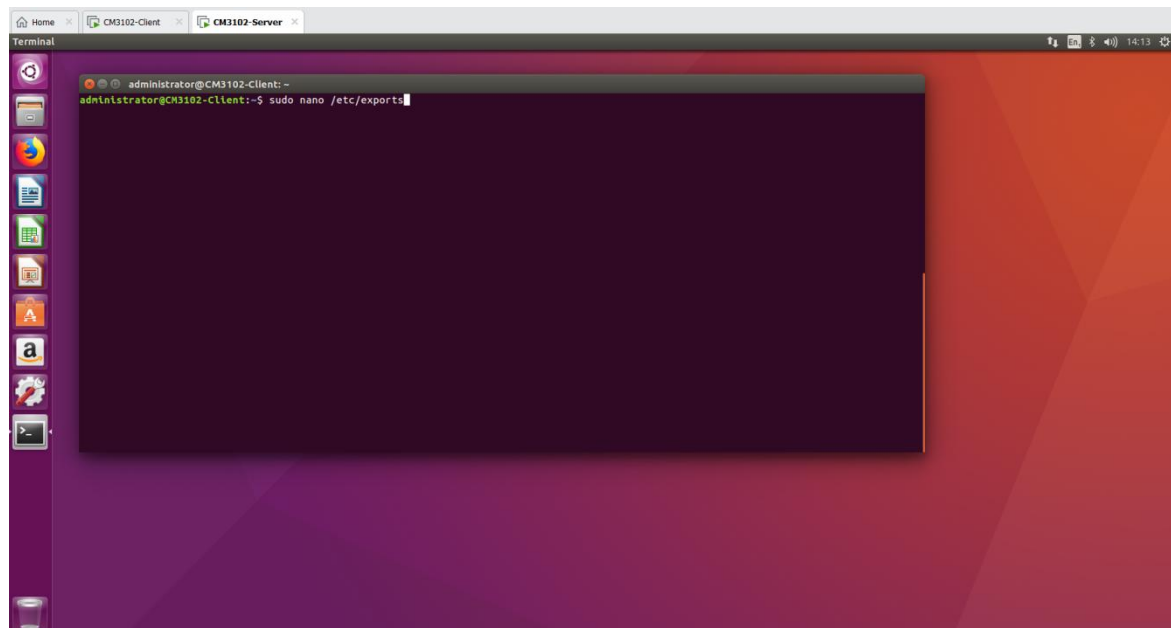
The image shows a terminal window on a Linux desktop environment. The terminal is titled 'administrator@CM3102-Client:~'. The user has executed the command 'ifconfig'. The output shows the configuration for the 'ens33' and 'lo' interfaces. The 'ens33' interface has an IP address of 192.168.163.129. The 'lo' interface has an IP address of 127.0.0.1.

```
administrator@CM3102-Client:~$ ifconfig
ens33:
    Link encap:Ethernet HWaddr 00:0c:29:8e:b4:80
    inet addr:192.168.163.129 Bcast:192.168.163.255 Mask:255.255.255.0
    inet6 addr: fe80::f85c:72d7:6843:d6c/64 Scope:link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:2082 errors:0 dropped:0 overruns:0 frame:0
    TX packets:1472 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:874344 (874.3 KB) TX bytes:132032 (132.0 KB)

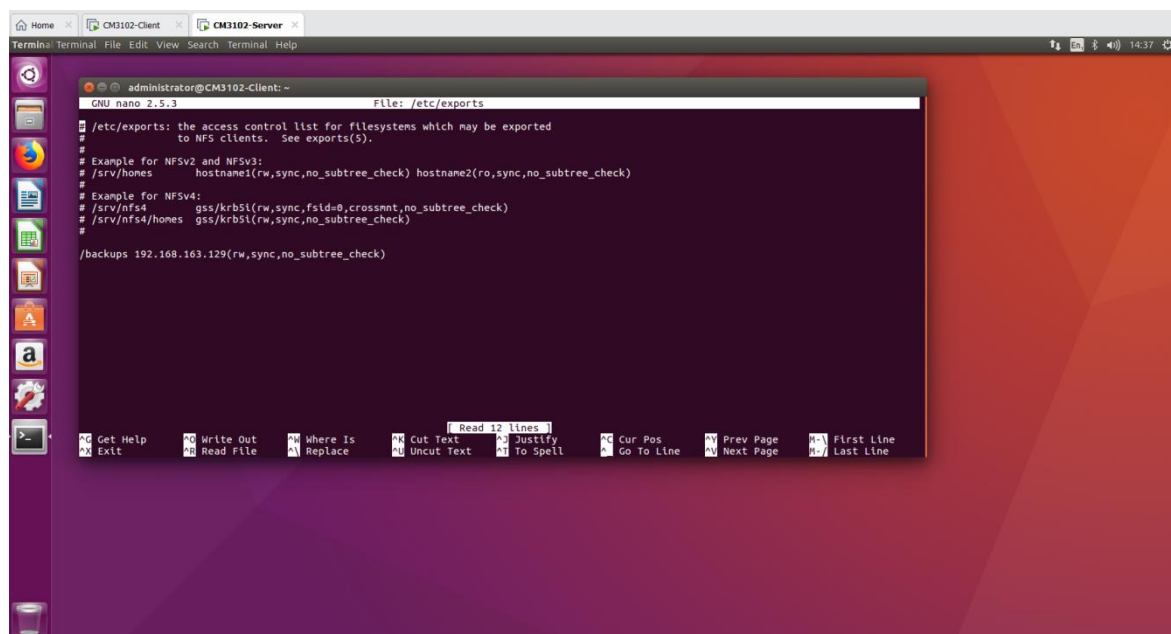
lo:
    Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:286 errors:0 dropped:0 overruns:0 frame:0
    TX packets:286 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:15970 (15.9 KB) TX bytes:15970 (15.9 KB)

administrator@CM3102-Client:~$
```

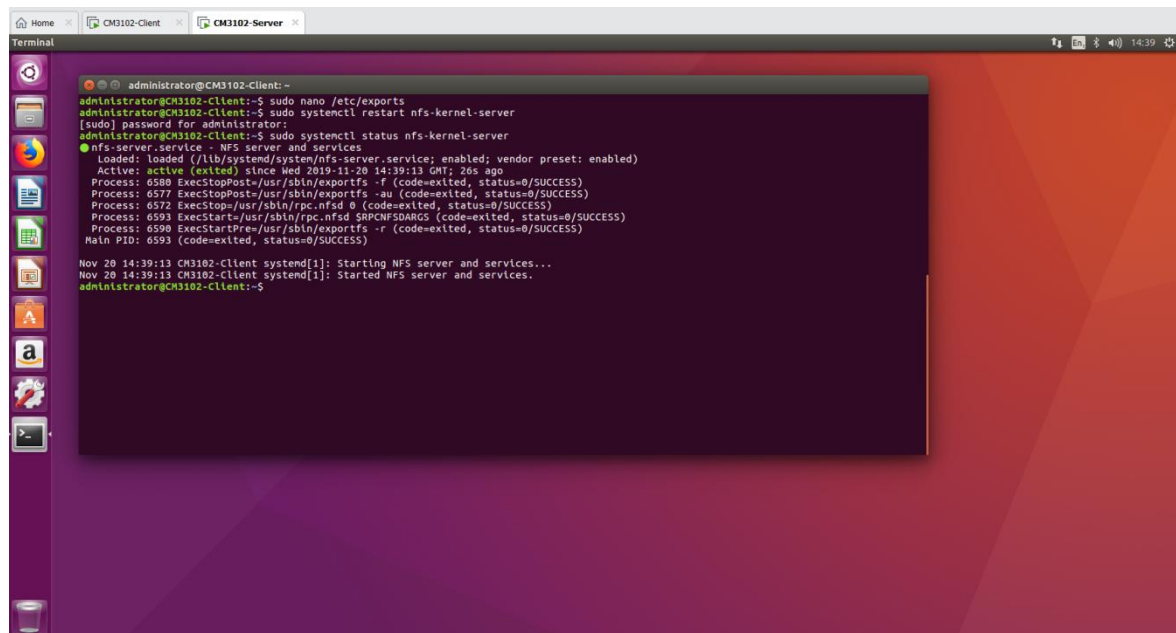
Once the read, write and execute permissions have been given to all users, the IP address of the client virtual machine must be identified in order to allow the client virtual machine to access the “/backups” directory present on the server virtual machine. In order to identify the IP address of the client virtual machine, the following command must be executed: “ifconfig”, as we can see in the above image the IP address of the client virtual machine is: 192.168.163.129.



After the IP address of the client virtual machine has been indentified, the IP address of the client virtual machine must be added to the network file system exports file present at the location /etc/exports. In order to add the IP address of the client virtual machine to the exports file, the following command must be executed: “sudo nano /etc/exports”. The command “sudo nano /etc/exports” will open the exports file using the nano command line text editor and will allow the addition of the client’s IP address by using root write permission rights allowed by the sudo command.



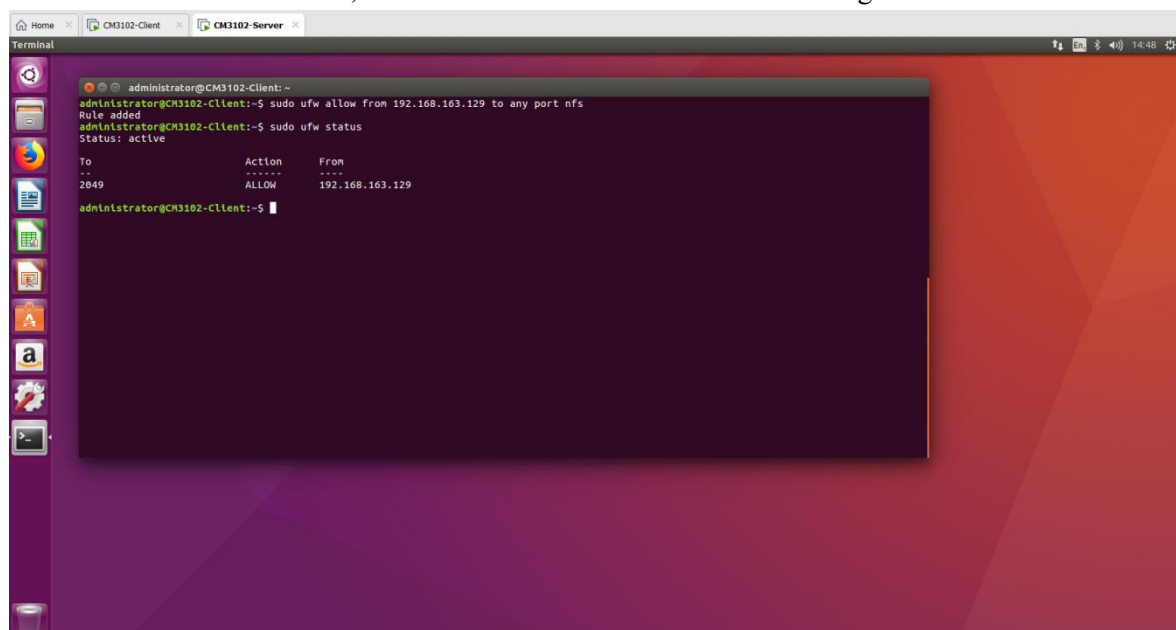
Once the command “sudo nano /etc/exports” have been executed, the command line editor will show the content of the exports file where the following line will be added at the end of the file: “/backups 192.168.163.129(rw, sync, no\_subtree\_check)”. The new line added at the of the file, which is “/backups 192.168.163.129(rw, sync, no\_subtree\_check)” will allow the client virtual machine to access the “/backups” directory having reading and writing permissions over the directory.

A terminal window on a Linux desktop environment. The user is logged in as 'administrator' on a machine named 'CM3102-Client'. The terminal shows the following commands and output:

```
administrator@CM3102-Client:~$ sudo nano /etc/exports
[sudo] password for administrator:
administrator@CM3102-Client:~$ sudo systemctl restart nfs-kernel-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2019-11-20 14:39:13 GMT; 26s ago
     Process: 6590 ExecStopPost=/usr/sbin/exports -f (code=exited, status=0/SUCCESS)
     Process: 6577 ExecStopPost=/usr/sbin/exports -au (code=exited, status=0/SUCCESS)
     Process: 6572 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/SUCCESS)
     Process: 6593 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
     Process: 6590 ExecStartPre=/usr/sbin/exports -r (code=exited, status=0/SUCCESS)
    Main PID: 6593 (code=exited, status=0/SUCCESS)

Nov 20 14:39:13 CM3102-Client systemd[1]: Starting NFS server and services...
Nov 20 14:39:13 CM3102-Client systemd[1]: Started NFS server and services.
administrator@CM3102-Client:~$
```

When the IP address of the client virtual machine has been added to the `/etc/exports` file and the file has been saved, the `nfs-kernel-server` must be restarted in order for the changes to have effect. In order to restart the `nfs-kernel-server`, the following commands must be executed: “`sudo systemctl restart nfs-kernel-server`” and “`sudo systemctl status nfs-kernel-server`”. The command “`sudo systemctl restart-nfs-kernel-server`” will restart the `nfs` server and the changes to the exports will take effect, the command “`sudo systemctl status nfs-kernel-server`” will allow the visualisation of the `nfs` server, which is “active” as we can see in the image above.

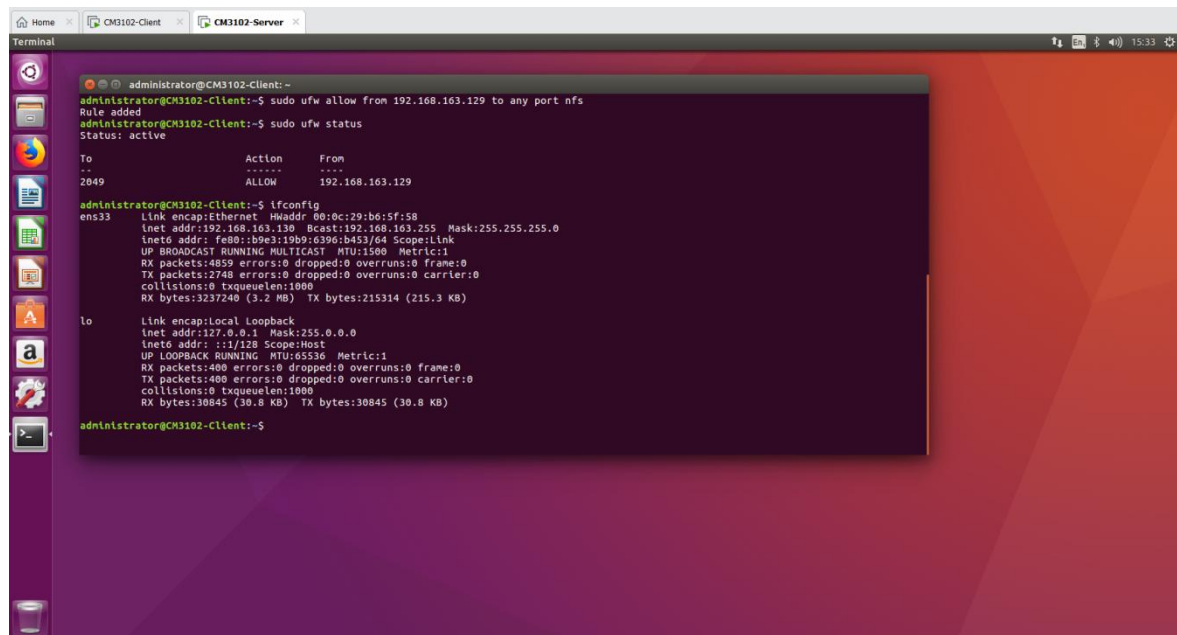
A terminal window on a Linux desktop environment. The user is logged in as 'administrator' on a machine named 'CM3102-Client'. The terminal shows the following commands and output:

```
administrator@CM3102-Client:~$ sudo ufw allow from 192.168.163.129 to any port nfs
Rule added
administrator@CM3102-Client:~$ sudo ufw status
Status: active

To Action From
--
2049 ALLOW 192.168.163.129

administrator@CM3102-Client:~$
```

In order to allow the client virtual machine to have access to the “/backups” directory on the server using the network file system (`nfs`), a firewall rule must be added on the server virtual machine. In order to add a new firewall rule to allow the client virtual machine to access the “/backups” directory the following commands must be executed: “`sudo ufw allow from 192.168.163.129 to any port nfs`”, “`sudo ufw status`”. The command “`sudo ufw allow from 192.168.163.129 to any port nfs`” will add the client virtual machine IP address to the allow incoming connections on any port and the “`sudo ufw status`” command will verify the previous command.



```
administrator@CM3102-Client:~$ sudo ufw allow from 192.168.163.129 to any port nfs
Rule added
administrator@CM3102-Client:~$ sudo ufw status
Status: active

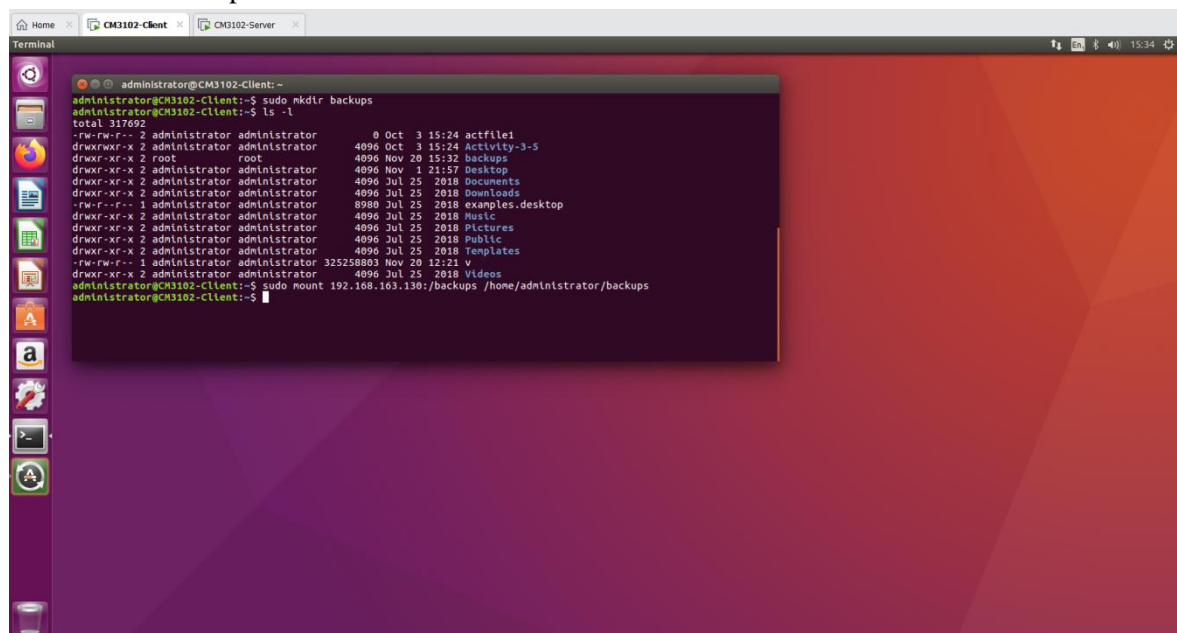
To Action From
--
2049 ALLOW 192.168.163.129

administrator@CM3102-Client:~$ ifconfig
ens33:
Link encap:Ethernet HWaddr 08:0c:29:b6:5f:58
inet addr:192.168.163.130 Bcast:192.168.163.255 Mask:255.255.255.0
inet6 addr: fe80::b9e3:19b9:6396:b453/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4859 errors:0 dropped:0 overruns:0 frame:0
TX packets:2748 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3237240 (3.2 MB) TX bytes:215314 (215.3 KB)

lo:
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:408 errors:0 dropped:0 overruns:0 frame:0
TX packets:408 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:30845 (30.8 KB) TX bytes:30845 (30.8 KB)

administrator@CM3102-Client:~$
```

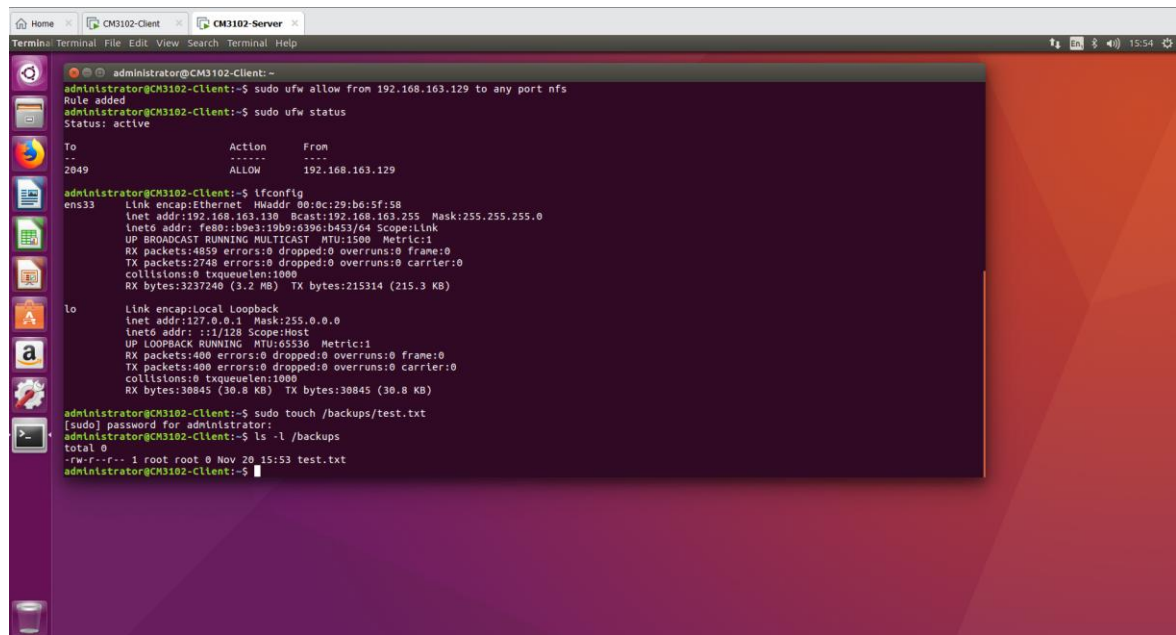
In order to allow the client machine connect to the server virtual machine and have access to the “/backups” directory present on the server virtual machine, the server virtual machine IP address must be identified. In order to identify the server virtual machine IP address the following command must be executed: “ifconfig”. The command “ifconfig” will allow the visualisation of the IP address of the server virtual machine which is: “192.168.163.130”, this IP address will be used in the next steps.



```
administrator@CM3102-Client:~$ sudo mkdir backups
administrator@CM3102-Client:~$ ls -l
total 317692
-rw-rw-r-- 2 administrator administrator 0 Oct 3 15:24 actfile1
drwxrwxr-x 2 administrator administrator 4096 Oct 3 15:24 Activity-3-5
drwxr-xr-x 2 root root 4096 Nov 20 15:32 backups
drwxr-xr-x 2 administrator administrator 4096 Nov 1 21:57 Desktop
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Documents
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Downloads
-rw-r--r-- 1 administrator administrator 8980 Jul 25 2018 examples.desktop
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Music
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Pictures
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Public
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Templates
-rw-rw-r-- 1 administrator administrator 325258083 Nov 20 12:21 v
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Videos
administrator@CM3102-Client:~$ sudo mount 192.168.163.130:/backups /home/administrator/backups
administrator@CM3102-Client:~$
```

In order to allow the client virtual machine to have access to the “/backups” directory present on the server virtual machine, the following commands must be executed: “sudo mkdir backups”, “ls -l”, “sudo mount 192.168.163.130:/backups /home/administrator/backups”. The command “sudo mkdir backups” will create a directory on the client virtual machine at the location /home/administrator/, the command “ls -l” will verify the previous command and the command “sudo mount 192.168.163.130:/backups /home/administrator/backups” will allow the client virtual machine to sync the backups directory located on the client virtual machine with the one present on the server virtual machine.





```
administrator@CM3102-Client:~$ sudo ufw allow from 192.168.163.129 to any port nfs
Rule added
administrator@CM3102-Client:~$ sudo ufw status
Status: active

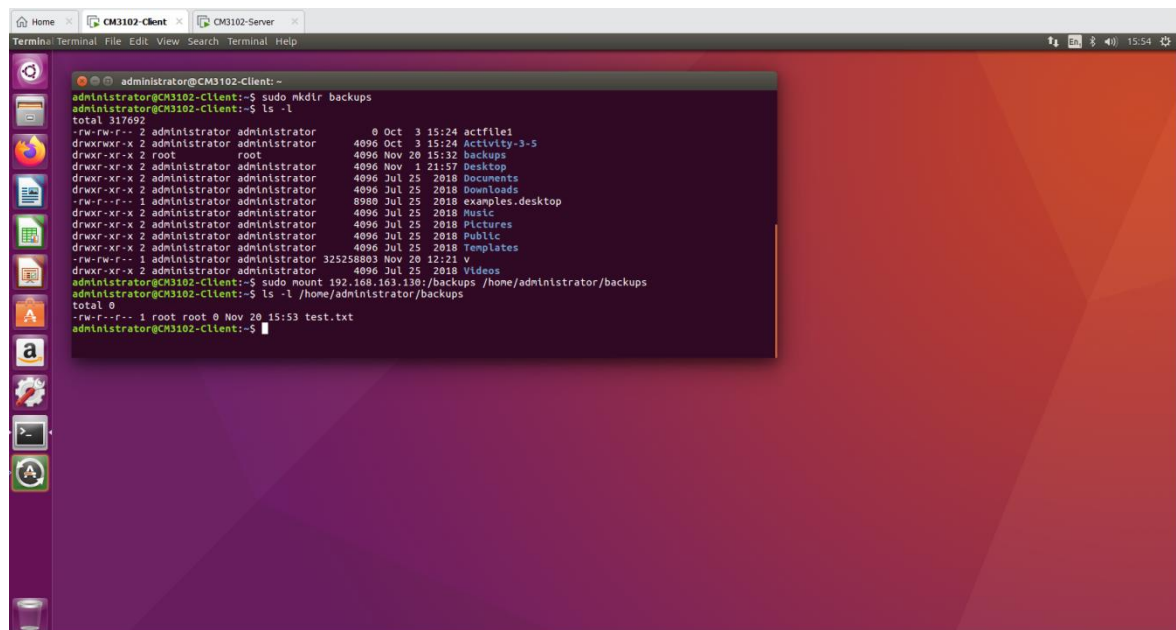
To Action From
--
2049 ALLOW 192.168.163.129

administrator@CM3102-Client:~$ ifconfig
ens33 Link encap:Ethernet HWaddr 00:0c:29:b6:5f:58
      inet addr:192.168.163.130 Bcast:192.168.163.255 Mask:255.255.255.0
      inet6 addr: fe80::b9e3:19b9:6396:b453/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:4859 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2748 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:3237240 (3.2 MB) TX bytes:215314 (215.3 KB)

lo Link encap:Local Loopback
   inet addr:127.0.0.1 Mask:255.0.0.0
   inet6 addr: ::1/128 Scope:Host
   UP LOOPBACK RUNNING MTU:65536 Metric:1
   RX packets:400 errors:0 dropped:0 overruns:0 frame:0
   TX packets:400 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1000
   RX bytes:30845 (30.8 KB) TX bytes:30845 (30.8 KB)

administrator@CM3102-Client:~$ sudo touch /backups/test.txt
[sudo] password for administrator:
administrator@CM3102-Client:~$ ls -l /backups
total 0
-rw-r--r-- 1 root root 0 Nov 20 15:53 test.txt
administrator@CM3102-Client:~$
```

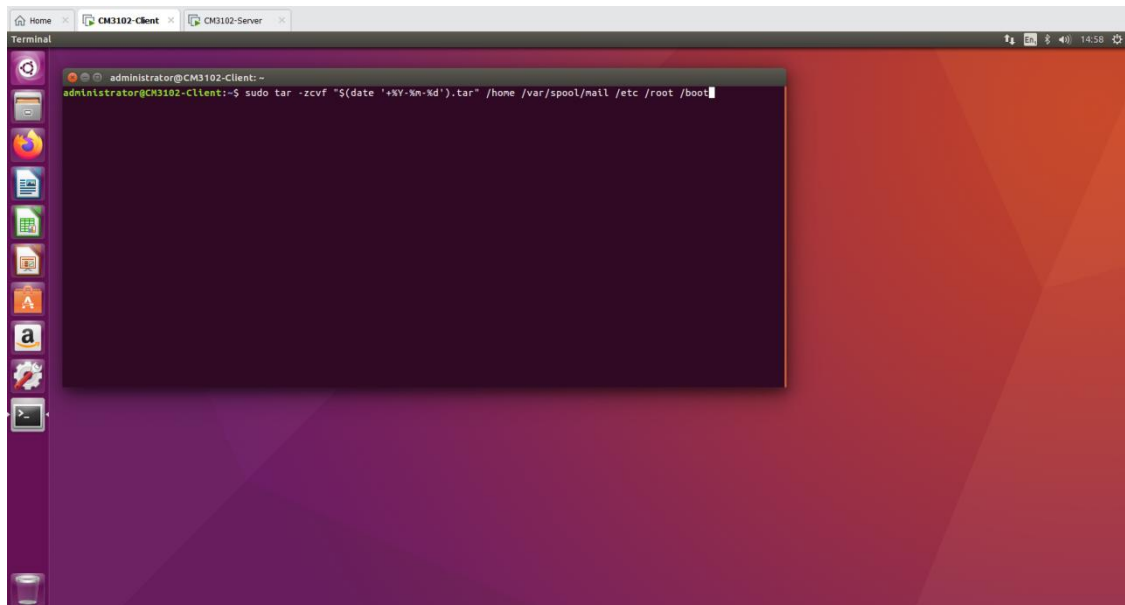
In order to test if the sync between the client virtual machine and the server virtual machine is working, a file should be added to the “/backups” directory present on the server, to do this the following commands must be executed: “sudo touch /backups/test.txt” and “ls -l /backups”. The command “sudo touch /backups/test.txt” will create a txt file in the backups directory, once this is done the file should also be visible on the client virtual machine.



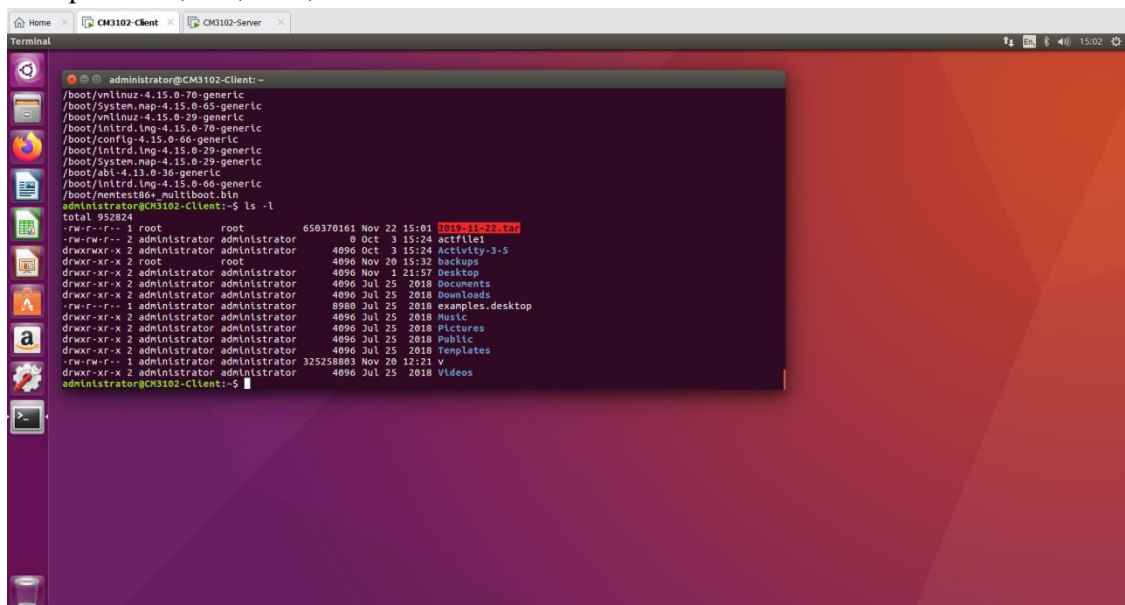
```
administrator@CM3102-Client:~$ sudo mkdir backups
administrator@CM3102-Client:~$ ls -l
total 317692
-rw-rw-r-- 2 administrator administrator 0 Oct 3 15:24 actfile1
drwxrwxr-x 2 administrator administrator 4096 Oct 3 15:24 Activity-3-5
drwxr-xr-x 2 root root 4096 Nov 20 15:52 backups
drwxr-xr-x 2 administrator administrator 4096 Nov 1 21:57 Desktop
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Documents
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Downloads
-rw-r--r-- 1 administrator administrator 8980 Jul 25 2018 examples.desktop
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Music
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Pictures
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Public
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Templates
-rw-rw-r-- 1 administrator administrator 325258803 Nov 20 12:21 v
drwxr-xr-x 2 administrator administrator 4096 Jul 25 2018 Videos
administrator@CM3102-Client:~$ sudo mount 192.168.163.130:/backups /home/administrator/backups
administrator@CM3102-Client:~$ ls -l /home/administrator/backups
total 0
-rw-r--r-- 1 root root 0 Nov 20 15:53 test.txt
administrator@CM3102-Client:~$
```

After the file was created on the server virtual machine, on the client virtual machine the file should be also present, to verify this, the following command must be executed: “ls -l /home/administrator/backups”, as we can see in the image above the file is present on the client virtual machine.

1.2  
1.3  
1.4



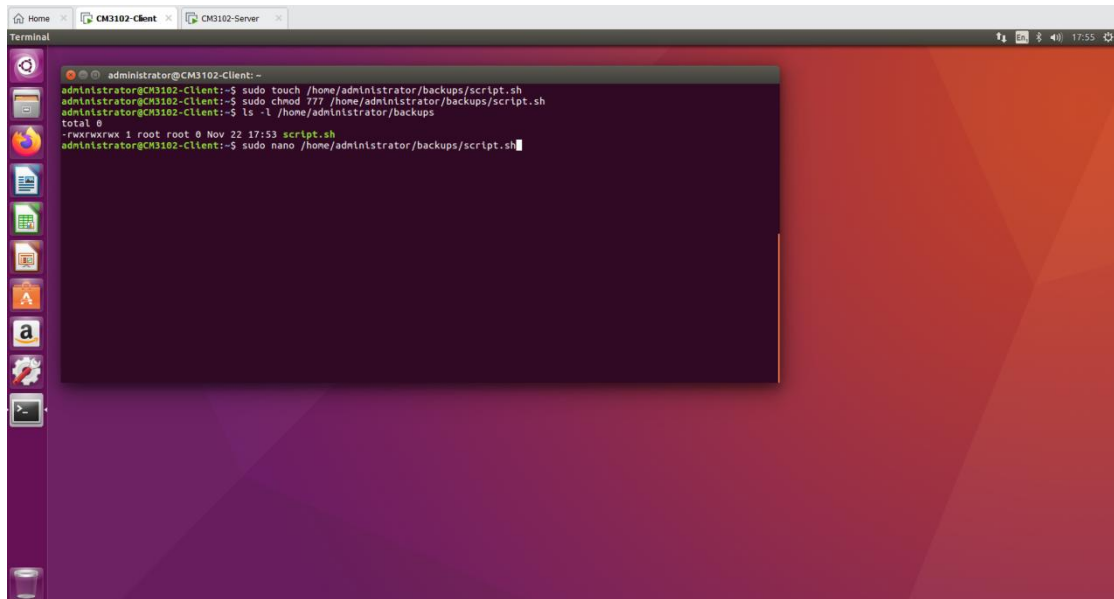
In order to backup the directories “/home”, “/var/spool/mail”, “/etc”, “/root”, “/boot” using the tar command and the date command so the file will contain the date as filename, the following command must be executed: `sudo tar -zcvf “$(date( ‘+%%Y-%%m-%%d’)).tar” /home /var/spool/mail /etc/ /root /boot`. The command in the image above will create a tar file using the current date as a filename and add inside the file the directories mentioned: /home, /var/spool/mail, /etc, /root, /boot.



To verify if the file was created successfully after the tar command was completed, the following command must be executed: “ls -l”. As we can see in the image above the tar file was created successfully.



## 1.5

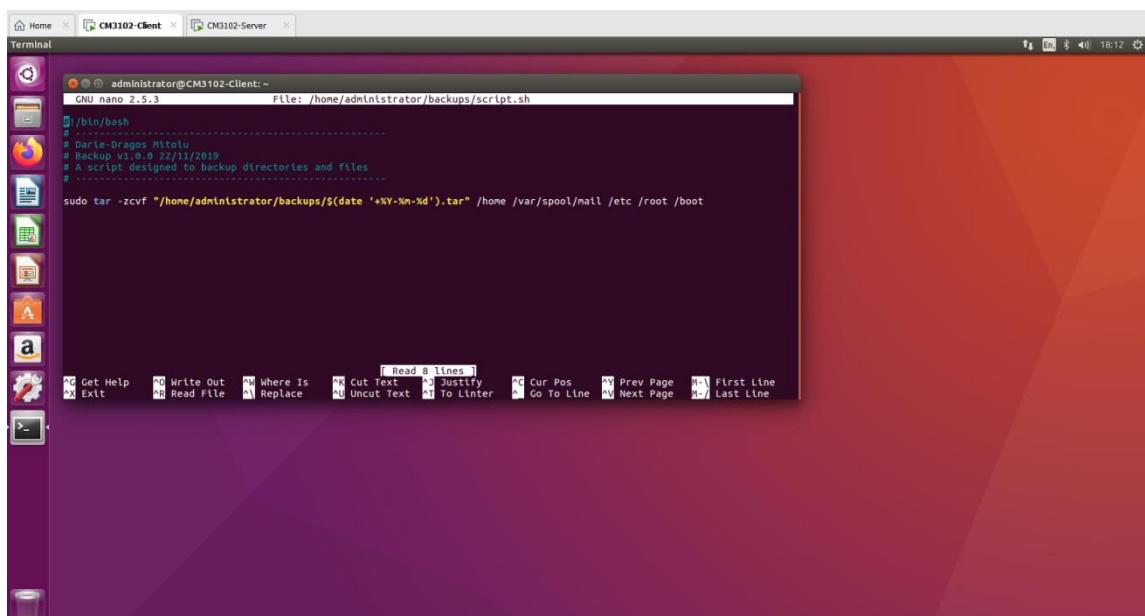


```

administrator@CM3102-Client: ~
administrator@CM3102-Client:~$ sudo touch /home/administrator/backups/script.sh
administrator@CM3102-Client:~$ sudo chmod 777 /home/administrator/backups/script.sh
administrator@CM3102-Client:~$ ls -l /home/administrator/backups
total 0
-rwxrwxrwx 1 root root 0 Nov 22 17:53 script.sh
administrator@CM3102-Client:~$ sudo nano /home/administrator/backups/script.sh

```

In order to create a script to backup of folders in section 1.2, the following commands must be executed: “`sudo touch /home/administrator/backups/script.sh`”, “`sudo chmod 777 /home/administrator/backups/script.sh`”, “`ls -l /home/administrator/backups`” and “`sudo nano /home/administrator/backups/script.sh`”. The first command executed, which is “`sudo touch /home/administrator/backups/script.sh`” will allow the creation of the script.sh file located at the location `/home/administrator/backups`, the command “`sudo chmod 777 /home/administrator/backups/script.sh`” will give read, write and execute permission to all users on the client virtual machine, the command “`ls -l`” will confirm the previous commands and last command which is executed in the image below will open the script.sh file using the nano command line editor.

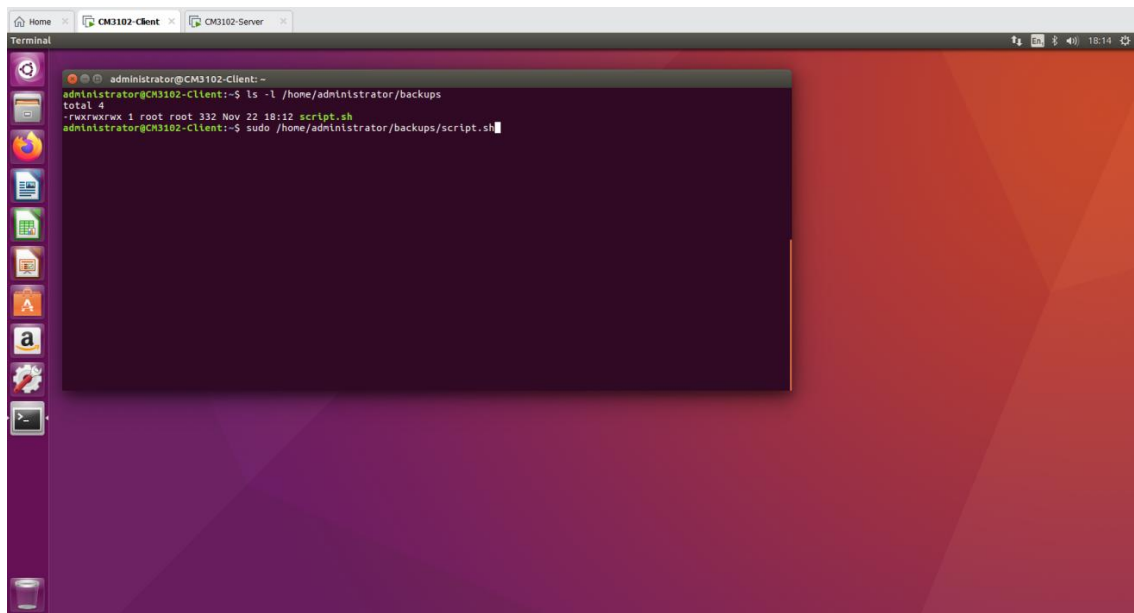


```

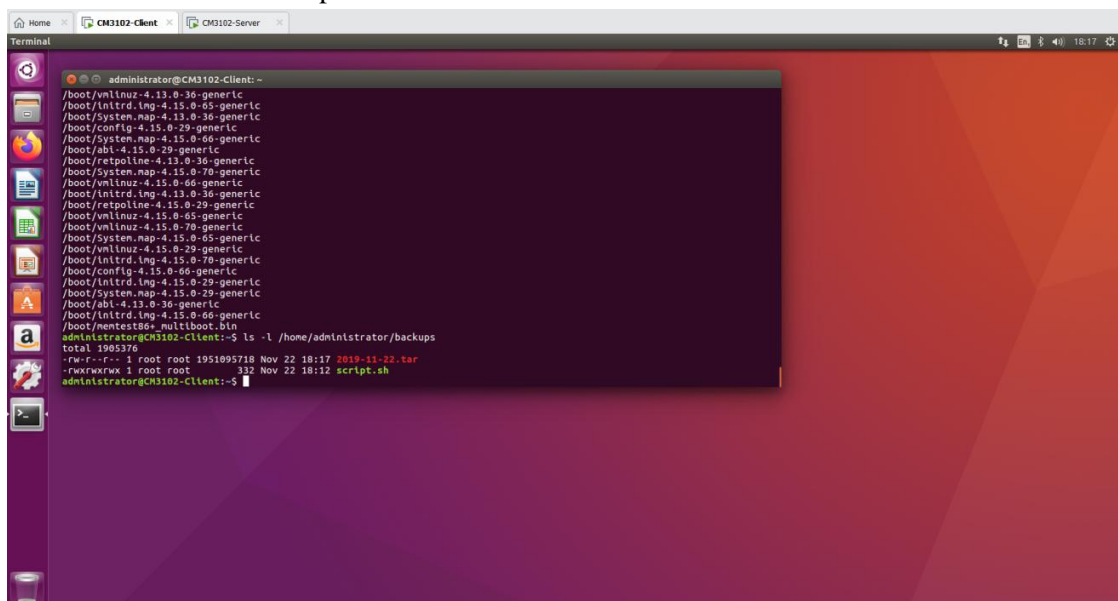
GNU nano 2.5.3 File: /home/administrator/backups/script.sh
#!/bin/bash
#
# Darle-Dragos Mitolu
# Backup v1.0:0 22/11/2019
# A script designed to backup directories and files
#
sudo tar -zcvf "/home/administrator/backups/${date '+%Y-%m-%d'}.tar" /home /var/spool/mail /etc /root /boot

```

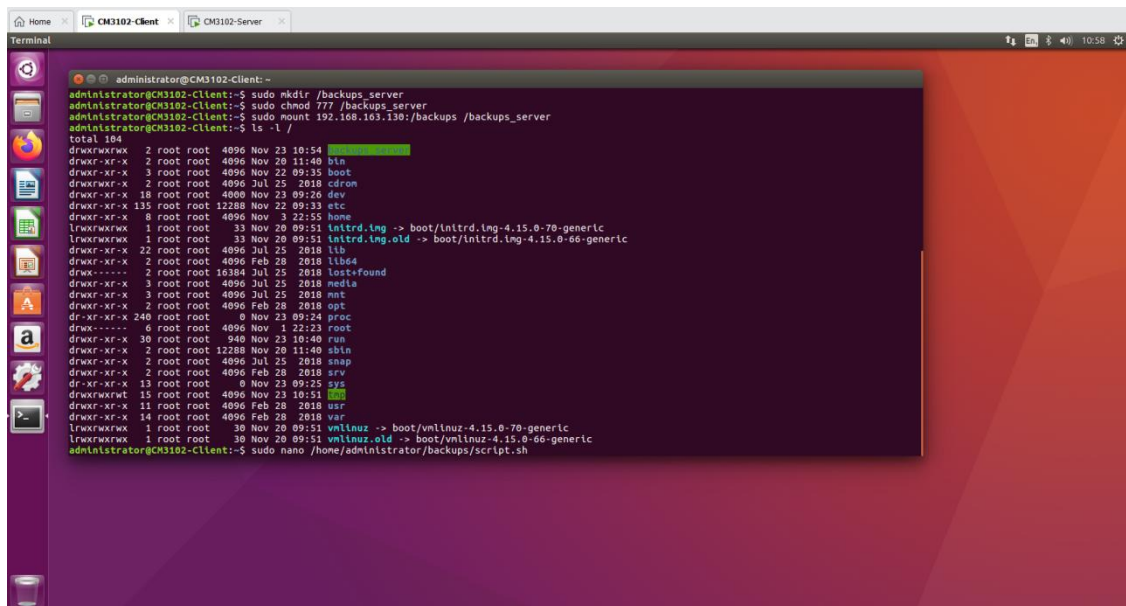
As we can see in the image above, the script.sh file was opened using the nano command line editor and the command: “`sudo tar -zcvf /home/administrator/backups/${date( ‘+%Y-%m-%d’)}.tar” /home /var/spool/mail /etc /root /boot`” was added to the script. This command will create a tar archive adding the `/home /var/spool/mail /etc /root /boot` directories at the location `/home/administrator/backups/` on the client machine using the current date as a filename.

A terminal window titled 'Terminal' is open on a desktop with a red and purple geometric background. The window has tabs for 'Home', 'CM3102-Client', and 'CM3102-Server'. The terminal shows the user 'administrator@CM3102-Client' running the command 'ls -l /home/administrator/backups'. The output shows a file 'script.sh' with permissions 'rwxrwxrwx' and size '1', owned by 'root' and 'root', dated 'Nov 22 18:12'. The user then runs 'sudo /home/administrator/backups/script.sh'.

In order to run the script the following command must be executed: “sudo /home/administrator/backups/script.sh”. The script will add the following directories: /home , var/spool/mail, etc/ /root /boot to a tar archive located at the location /home/administrator/backups.

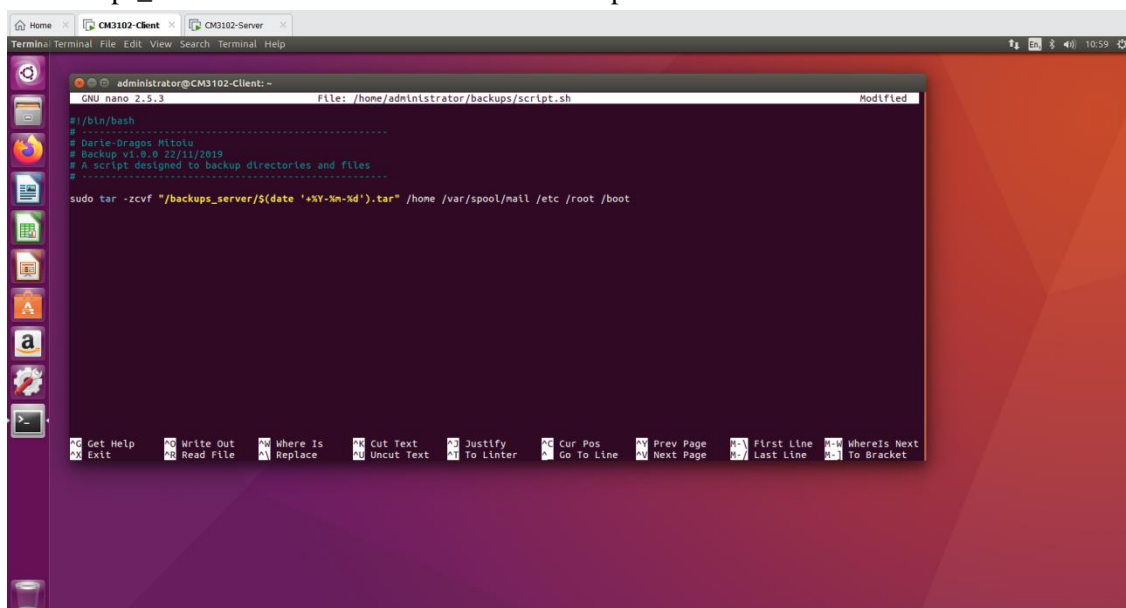
A terminal window titled 'Terminal' is open on the same desktop. The terminal shows the user 'administrator@CM3102-Client' running the command 'ls -l /home/administrator/backups'. The output shows a long list of files and directories, including various boot files like 'vmlinuz', 'initrd', 'config', 'system.map', 'abi', 'retpoline', and 'nmentest64', as well as a new tar archive '2019-11-22.tar' with permissions 'rwxr-xr-x' and size '1965376', owned by 'root' and 'root', dated 'Nov 22 18:17'.

After the script has been executed, the tar archive should be located at the /home/administrator/backups directory, to visualise the content of the directory, the following command must be executed: “ls -l /home/administrator/backups”. As we can see in the image above the tar archive is present in the backups directory. The script has been executed successfully. In the next steps the tar file will be created in a new directory which will be mounted using the network file system to demonstrate the operation of backing up files using the client virtual machine and not the server virtual machine.



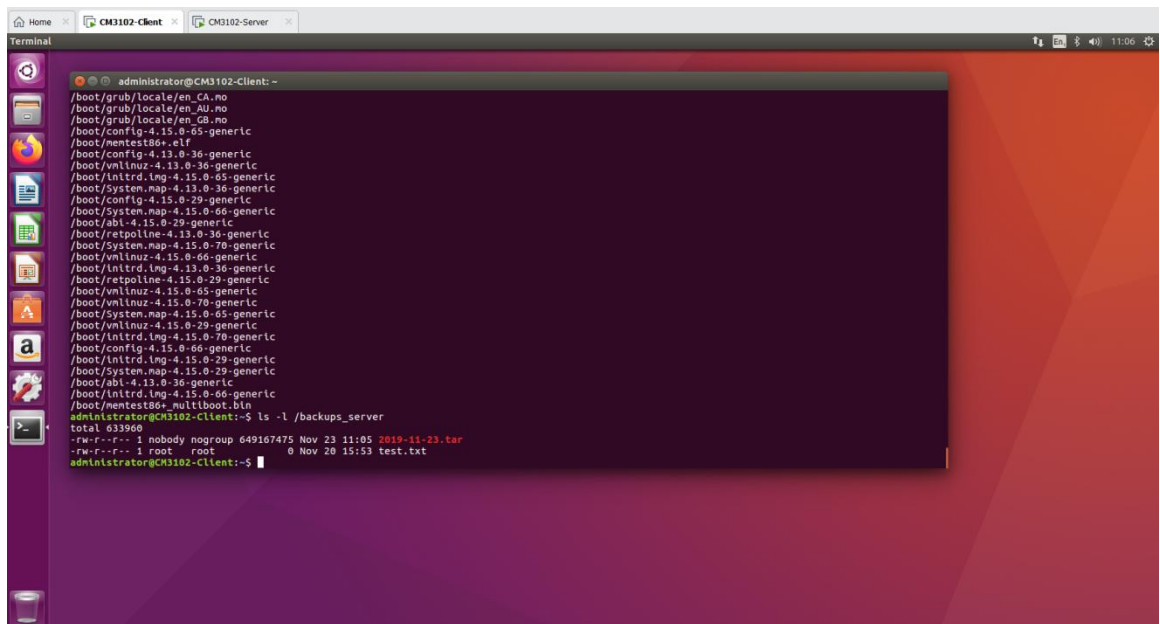
```
administrator@CM3102-Client:~$ sudo mkdir /backups_server
administrator@CM3102-Client:~$ sudo chmod 777 /backups_server
administrator@CM3102-Client:~$ sudo mount 192.168.163.130:/backups /backups_server
administrator@CM3102-Client:~$ ls -l /
total 104
drwxr-xr-x 2 root root 4096 Nov 23 10:54 [redacted]
drwxr-xr-x 2 root root 4096 Nov 20 11:40 bin
drwxr-xr-x 3 root root 4096 Nov 22 09:35 boot
drwxr-xr-x 2 root root 4096 Jul 25 2018 cdrom
drwxr-xr-x 18 root root 4096 Nov 23 09:26 dev
drwxr-xr-x 135 root root 12288 Nov 22 09:33 etc
drwxr-xr-x 8 root root 4096 Nov 3 22:55 home
lrwxrwxrwx 1 root root 33 Nov 20 09:51 initrd.img -> boot/initrd.img-4.15.0-70-generic
lrwxrwxrwx 1 root root 33 Nov 20 09:51 initrd.img.old -> boot/initrd.img-4.15.0-66-generic
drwxr-xr-x 22 root root 4096 Jul 25 2018 lib
drwxr-xr-x 2 root root 4096 Feb 28 2018 lib64
drwx----- 2 root root 16384 Jul 25 2018 lost+found
drwxr-xr-x 3 root root 4096 Jul 25 2018 media
drwxr-xr-x 3 root root 4096 Jul 25 2018 net
drwxr-xr-x 2 root root 4096 Feb 28 2018 opt
dr-xr-xr-x 240 root root 0 Nov 23 09:24 proc
drwx----- 6 root root 4096 Nov 1 22:23 root
drwxr-xr-x 30 root root 940 Nov 23 10:40 run
drwxr-xr-x 2 root root 12288 Nov 20 11:40/sbin
drwxr-xr-x 2 root root 4096 Jul 25 2018 snap
drwxr-xr-x 2 root root 4096 Feb 28 2018 srv
dr-xr-xr-x 13 root root 0 Nov 23 09:25 sys
drwxrwxrwx 15 root root 4096 Nov 23 10:51 [redacted]
drwxr-xr-x 11 root root 4096 Feb 28 2018 usr
drwxr-xr-x 14 root root 4096 Feb 28 2018 var
lrwxrwxrwx 1 root root 30 Nov 20 09:51 vmlinuz -> boot/vmlinuz-4.15.0-70-generic
lrwxrwxrwx 1 root root 30 Nov 20 09:51 vmlinuz.old -> boot/vmlinuz-4.15.0-66-generic
administrator@CM3102-Client:~$ sudo nano /home/administrator/backups/script.sh
```

In order to create a connection between the client virtual machine and the server virtual machine using the network file system and send the backed up files to the server, the following commands must be executed: “sudo mkdir /backups\_server”, “sudo chmod 777 /backups\_server”, “sudo mount 192.168.163.130:/backups /backups\_server”, “ls -l” and “sudo nano /home/administrator/backups/script.sh”. The command “sudo mkdir /backups\_server” will create a directory called backups\_server, the command “sudo chmod 777 /backups\_server” will give read, write and execute permission to all users on client virtual machine over the backups\_server directory, the command “sudo mount 192.168.163.130:/backups /backups\_server” will create a connection between client virtual machine and the server virtual machine using the nfs, the command “ls -l” will verify the previous commands and the command “sudo nano /home/administrator/backups/script.sh” which is executed in the image below, will be used in order to change the tar file destination to /backups\_server from /home/administrator/backups.

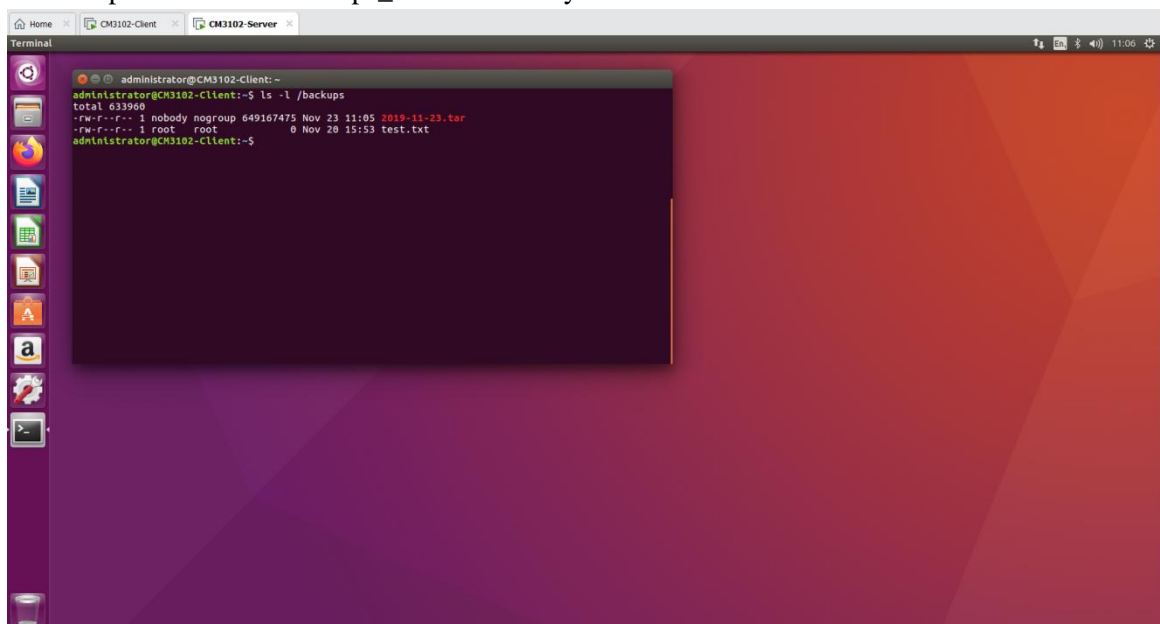


```
GNU nano 2.5.3 File: /home/administrator/backups/script.sh Modified
#!/bin/bash
#
# Darle-Orages Mitola
# Backup v1.0.0 22/11/2019
# A script designed to backup directories and files
#
sudo tar -czvf "/backups_server/$(date +%Y-%m-%d').tar" /home /var/spool/mail /etc /root /boot
```

In the image above, the script has been modified in order to send the backed up files, which are: /home /var/spool/mail /etc /root and /boot to /backups\_server directory instead of /home/administrator/backups once the script is executed.



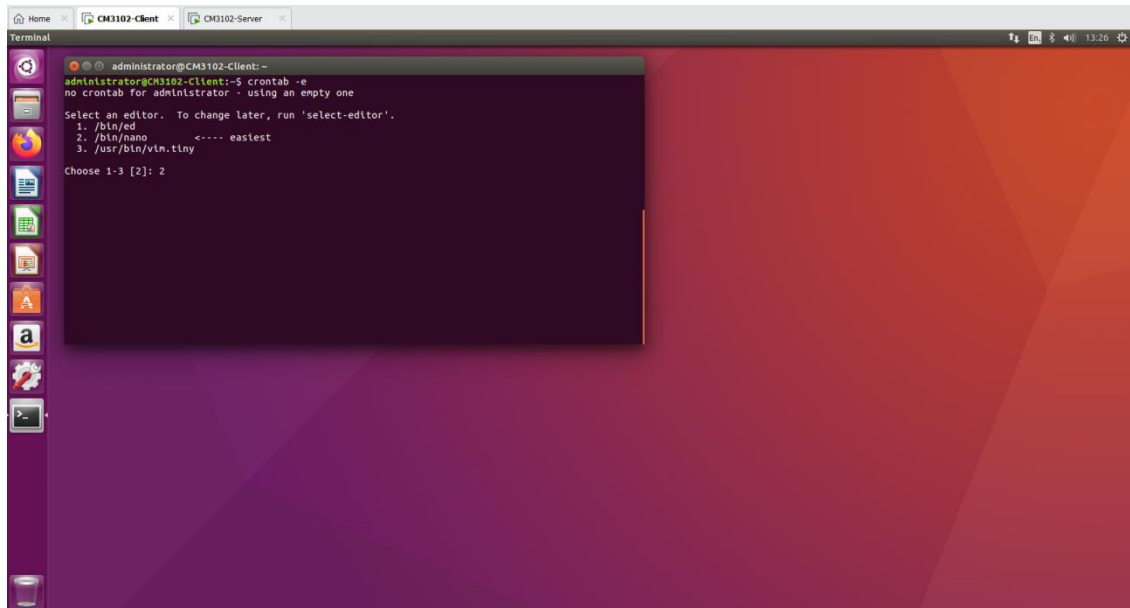
After the script has been executed, we can visualise on the client virtual machine the tar file which is present in the /backups\_server directory.



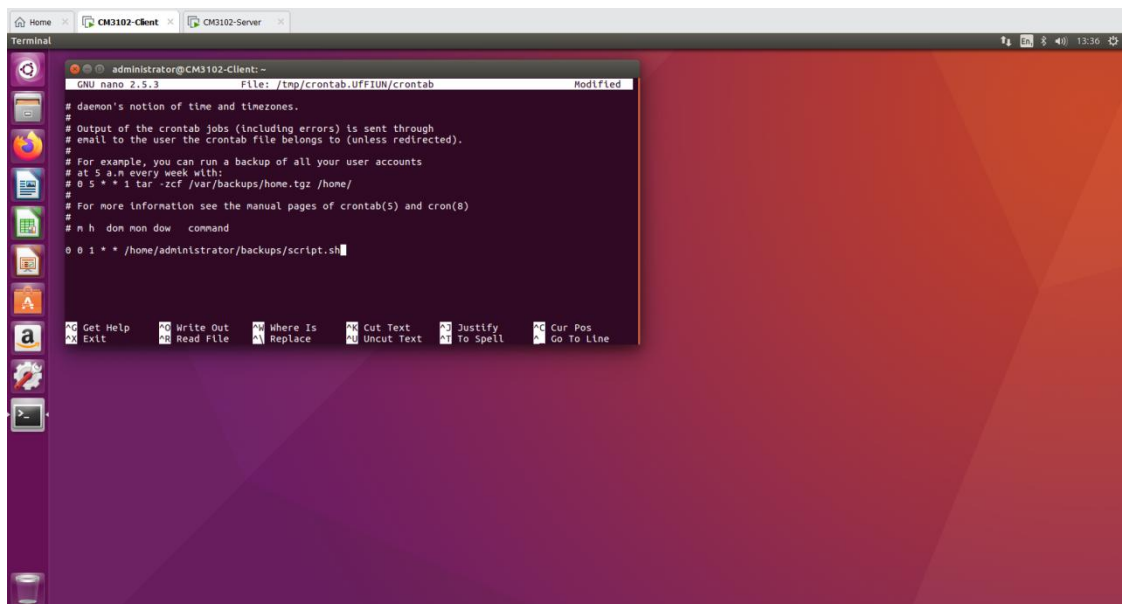
To confirm the fact that the files have been backed up successfully, the tar file should also be present on the server virtual machine, in order to visualise the content of the /backups directory present on the server virtual machine, the command “ls -l /backups” must be executed, as we can see in the image above the tar file is also visible on the server virtual machine.

N.B: The backup operations above have been performed again because once the client virtual machine will be shut down, the “/backups” directory on the client virtual machine will not be mounted anymore and the directory already presents some files inside, if the directory will be mounted again, the files present before the mount will not be visible anymore.

## 1.6

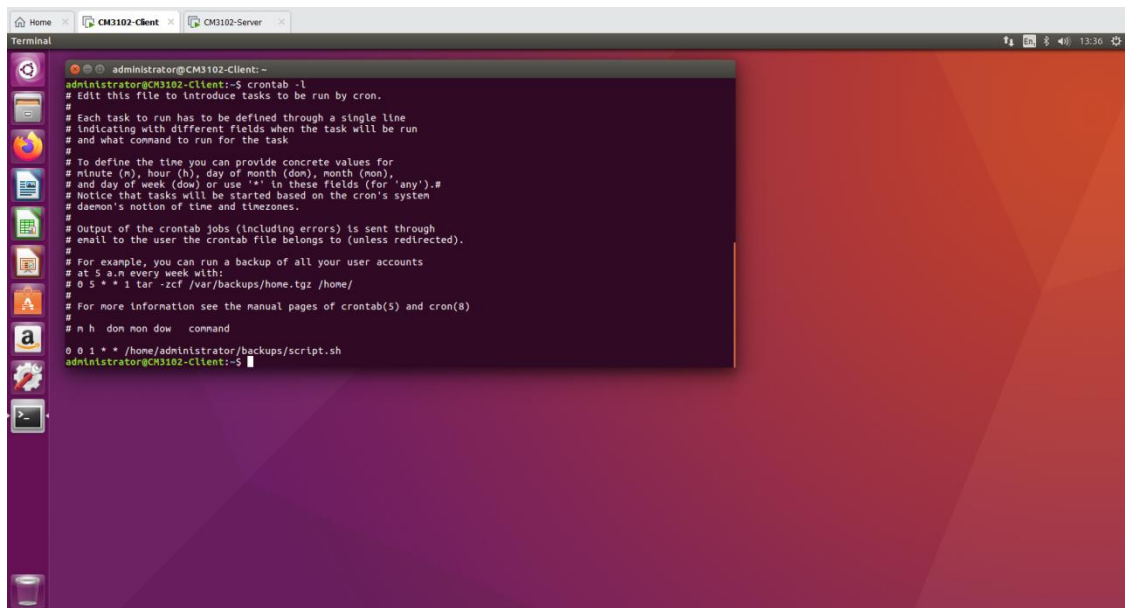


In order to use the crontab to configure the automated script execution, the following command must be executed: “crontab -e”. The command “crontab -e” will create a new crontab list where scheduled tasks could be added.



In order to allow the execution of the script to be done once a month, the following line should be added at the end of the crontab file: “0 0 1 \* \* /home/administrator/backups/script.sh”. As we can see in the image above the representation of the period of execution is the following: minute, hour, day of month, month, day of week and last but not the least the star symbol represents any possibility, in the case in cause, the star symbol would represent any month and any day of the week.

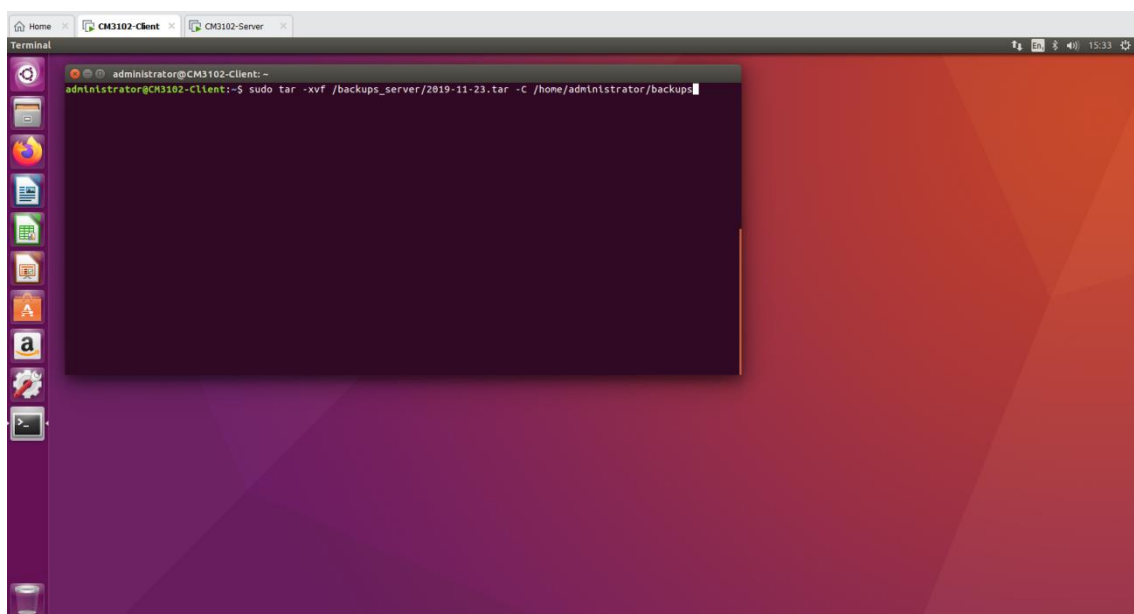


A terminal window on a Linux desktop with a purple and red geometric background. The terminal shows the command 'crontab -l' being executed. The output displays the content of the crontab file, which includes comments about task scheduling and a single cron job: '0 5 \* \* 1 tar -zcf /var/backups/home.tgz /home/'. The desktop has a sidebar with application icons and a top bar with window titles 'Home', 'CM3102-Client', and 'CM3102-Server'.

```
administrator@CM3102-Client:~$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
m h dom mon dow   command
0 5 * * 1 /home/administrator/backups/script.sh
administrator@CM3102-Client:~$
```

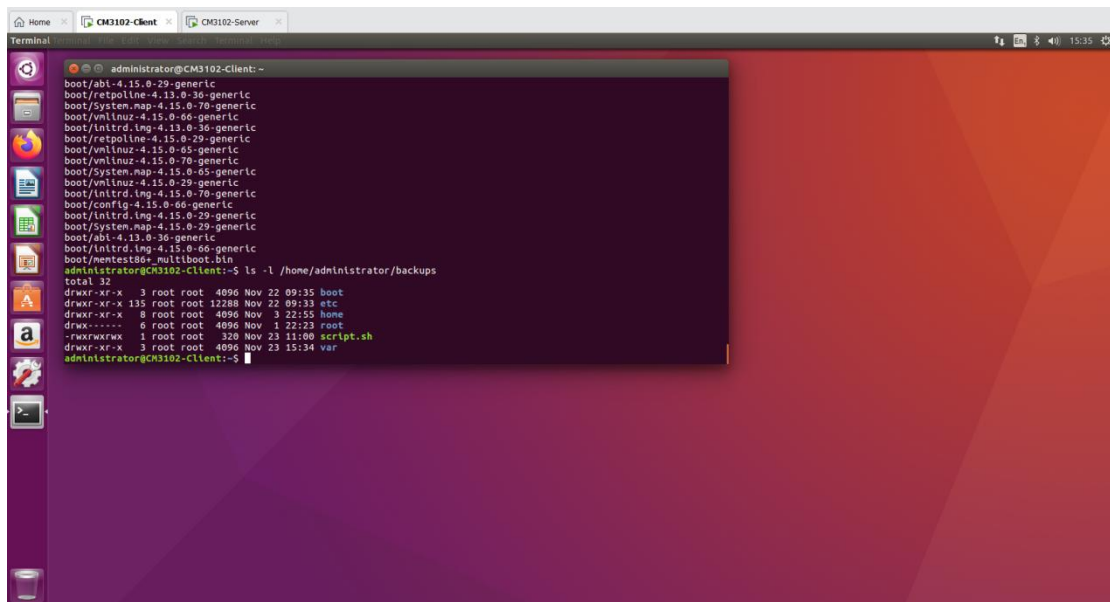
In order to visualise the content of the crontab file, the following command must be executed: “crontab -l”. The command “crontab -l” will display the content of the crontab file, as we can see in the image above the file has been saved successfully.

## 1.7

A terminal window on the same Linux desktop as the previous image. The terminal shows the command 'sudo tar -xvf /backups\_server/2019-11-23.tar -C /home/administrator/backups' being executed. The desktop environment is identical to the previous image.

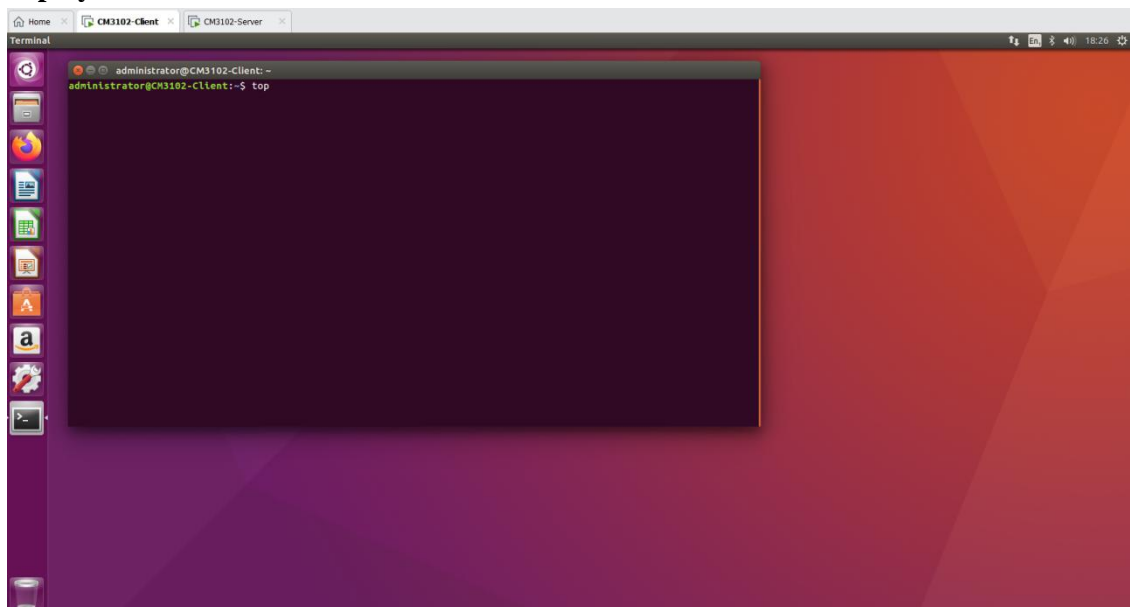
```
administrator@CM3102-Client:~$ sudo tar -xvf /backups_server/2019-11-23.tar -C /home/administrator/backups
```

In order to restore the specified directories when necessary, the following command must be executed: “sudo tar -xvf /backups\_server/2019-11-23.tar” -C /home/administrator/backups”, this command will extract the content of the tar file and send the content of that tar file to the location /home/administrator/backups. The argument “-xvf” passed to the tar command will allow the extraction of the tar file content in a verbose mode and the argument -C passed to the tar argument after the verbose extraction of the file will allow to specify a destination for the directories or files that will be extracted.



After the extraction process has been completed, all the directories and files present in the tar file should be present at the specified destination, which is “/home/administrator/backups”, in order to verify the tar file extraction command, the following command must be executed after the completion of the extraction: “ls -l /home/administrator/backups”. The command “ls -l /home/administrator/backups” will allow the visualisation of the specified destination for extraction of the tar file, as we can see in the image above, the directories and files present in the tar file have been extracted successfully to the destination mentioned in the command.

## 2. Top System Monitor



An accessible and convenient Linux system monitoring tool would be the “top” system monitoring tool, this system monitoring tool it is a command line system monitoring tool very simple and efficient when analysing characteristics like CPU usage and memory usage. In order to access the “top” system monitor, the following command must be executed in the terminal: “top”, this command will open the “top” command line system monitor.

```
top - 10:26:35 up 5:09, 1 user, load average: 0.31, 0.15, 0.06
Tasks: 233 total, 1 running, 160 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.8 sy, 0.0 ni, 98.8 id, 0.0 wa, 0.0 hi, 0.2 st, 0.0 st
KiB Mem : 985704 total, 48276 free, 685824 used, 232404 buff/cache
KiB Swap: 1046524 total, 938492 free, 108032 used, 103280 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     time+ COMMAND
  970 root        20   0 470348 64044 12288 S   1.7   6.5   1:02.28 Xorg
3696 administ+ 20   0 666048 33488 26540 S   1.0   3.4   0:00.34 gnome-terminal-
2163 administ+ 20   0 1000748 22404 14360 S   0.7   2.3   0:06.44 nautilus
1529 root       20   0 151504 3820 2980 S   0.3   0.4   0:25.00 vntoolsd
3714 administ+ 20   0 49020 3712 2992 R   0.3   0.4   0:00.02 top
   1 root       20   0 185492 4208 2820 S   0.0   0.4   0:05.68 systemd
   2 root       20   0 0 0 0 S   0.0   0.0   0:00.02 kthreadd
   4 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kworker/0:0H
   6 root       20   0 0 0 0 S   0.0   0.0   0:00.00 mm_percpu_wq
   7 root       20   0 0 0 0 S   0.0   0.0   0:00.14 ksoftirqd/0
   8 root       20   0 0 0 0 S   0.0   0.0   0:04.59 rcu_sched
   9 root       20   0 0 0 0 S   0.0   0.0   0:00.00 rcu_bh
  10 root       20   0 0 0 0 S   0.0   0.0   0:00.01 migration/0
  11 root       20   0 0 0 0 S   0.0   0.0   0:00.00 watchdog/0
  12 root       20   0 0 0 0 S   0.0   0.0   0:00.00 cpuhp/0
  13 root       20   0 0 0 0 S   0.0   0.0   0:00.00 cpuhp/1
  14 root       20   0 0 0 0 S   0.0   0.0   0:00.00 watchdog/1
  15 root       20   0 0 0 0 S   0.0   0.0   0:00.00 migration/1
  16 root       20   0 0 0 0 S   0.0   0.0   0:06.64 ksoftirqd/1
  18 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kworker/1:0H
  19 root       20   0 0 0 0 S   0.0   0.0   0:00.02 kdevtmpfs
  20 root       20   0 0 0 0 S   0.0   0.0   0:00.00 netns
  21 root       20   0 0 0 0 S   0.0   0.0   0:00.00 rcu_tasks_kthre
  22 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kauditd
```

As we can see in the image above, once the “top” command was executed the running processes appear in the command line associated with their characteristics, some of the features provided by the “top” system monitor are the sort feature which can be used by pressing any of the following commands while the “top” system monitor is running:

```
top - 19:29:19 up 6:12, 1 user, load average: 0.02, 0.02, 0.00
Tasks: 233 total, 1 running, 161 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.3 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.2 st, 0.0 st
KiB Mem : 985704 total, 139636 free, 656228 used, 189840 buff/cache
KiB Swap: 1046524 total, 901096 free, 145428 used, 136308 avail Mem

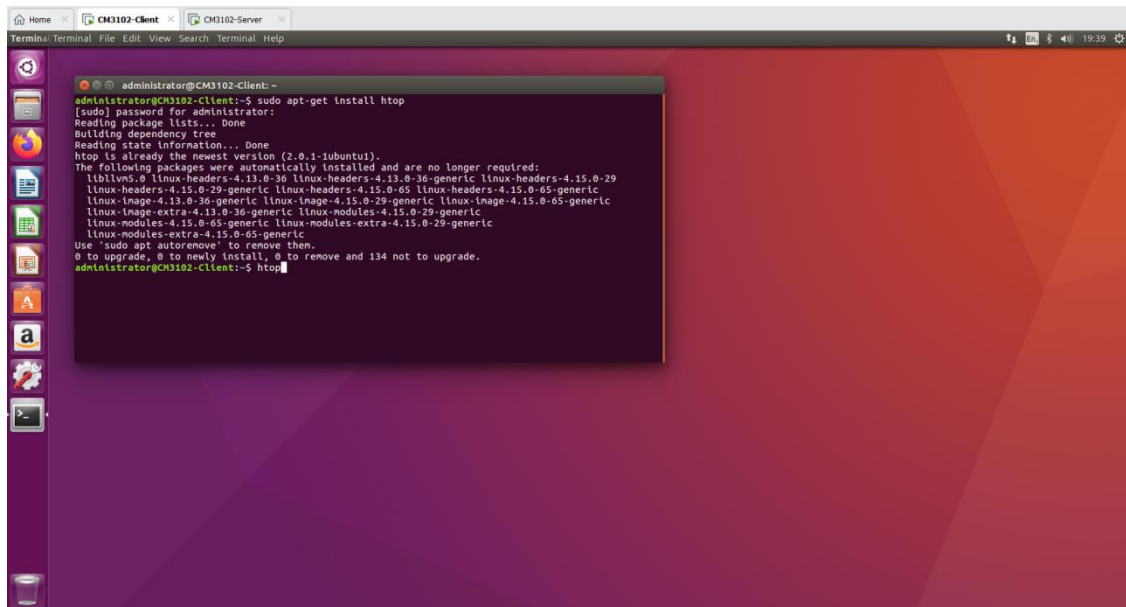
  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     time+ COMMAND
2123 administ+ 20   0 1610544 81200 25832 S   0.7   8.2   3:13.10 comptz
  970 root       20   0 479908 65944 13716 S   1.0   6.7   1:15.88 Xorg
2165 administ+ 20   0 746056 57176 7384 S   0.0   5.8   0:12.51 gnome-software
2298 administ+ 20   0 872884 40232 3856 S   0.0   4.1   0:03.13 evolution-calen
2232 administ+ 20   0 814904 38744 3500 S   0.0   3.9   0:03.21 evolution-calen
3696 administ+ 20   0 607516 33024 25600 S   0.7   3.4   0:03.93 gnome-terminal-
3830 administ+ 20   0 496240 28584 23872 S   0.0   2.9   0:00.83 notify-ord
2171 administ+ 20   0 270256 22376 7784 S   0.0   2.3   0:35.07 vntoolsd
2163 administ+ 20   0 1000748 21812 14112 S   0.3   2.2   0:06.63 nautilus
2161 administ+ 20   0 670240 15856 12024 S   0.0   1.5   0:03.55 nm-applet
2529 administ+ 20   0 589744 15044 7588 S   0.0   1.5   0:02.03 unity-scope-loa
1985 administ+ 20   0 576680 14236 10264 S   0.0   1.4   0:03.97 unity-panel-ser
2463 administ+ 20   0 574168 12248 7620 S   0.0   1.2   0:01.76 update-notifier
1966 administ+ 20   0 651588 12160 9896 S   0.0   1.2   0:01.57 hud-service
1881 administ+ 20   0 529716 11920 8548 S   0.0   1.2   0:02.98 bamfdaemon
2406 administ+ 20   0 317328 11064 8324 S   0.0   1.1   0:00.50 zeitgeist-fs
2528 administ+ 20   0 637684 9776 7592 S   0.0   1.0   0:00.92 unity-files-dae
1911 administ+ 20   0 484636 9728 7484 S   0.0   1.0   0:01.10 ibus-ut-gtk3
1968 administ+ 20   0 861092 9440 7224 S   0.0   1.0   0:03.47 unity-settings-
2516 administ+ 20   0 651840 9276 7736 S   0.0   0.9   0:01.51 unity-scope-hom
  886 root       20   0 456388 8420 6840 S   0.0   0.9   0:02.93 NetworkManager
2036 administ+ 20   0 656204 8328 6948 S   0.0   0.8   0:01.52 indicator-keybo
1582 whoopsie 20   0 382188 7532 6804 S   0.0   0.8   0:01.94 whoopsie
2038 administ+ 20   0 554564 7348 6544 S   0.0   0.7   0:00.67 indicator-print
1916 administ+ 20   0 435004 7304 6440 S   0.0   0.7   0:00.89 ibus-x11
2164 administ+ 20   0 583984 6776 5820 S   0.0   0.7   0:00.82 unity-fallback-
2382 administ+ 20   0 697076 6592 3924 S   0.0   0.7   0:00.23 evolution-adre
```

Pressing the “M” letter associated with the “x” letter and “b” letter will sort the processes by memory and highlighting the memory column, as we can see in the image above, some other sorting commands are: “P” letter for sorting by CPU usage, “N” letter to sort by processes id and “T” letter to sort by process run time (the letters must be capital when pressed).

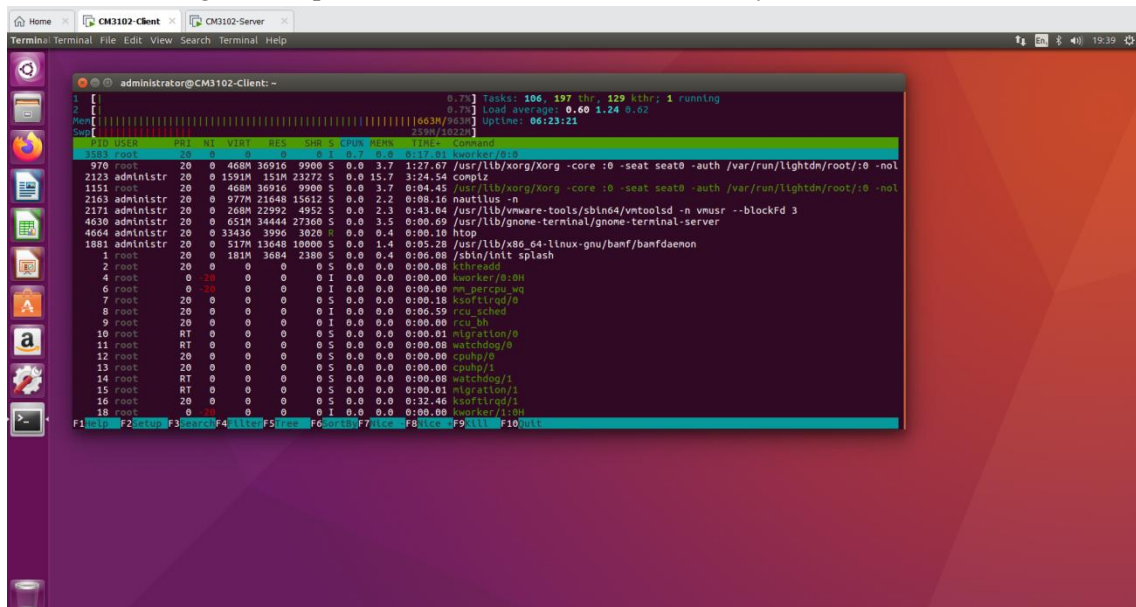
## 2.1 Alternatives:

- **Htop System Monitor**
- **Ubuntu System Monitor**

## 2.2

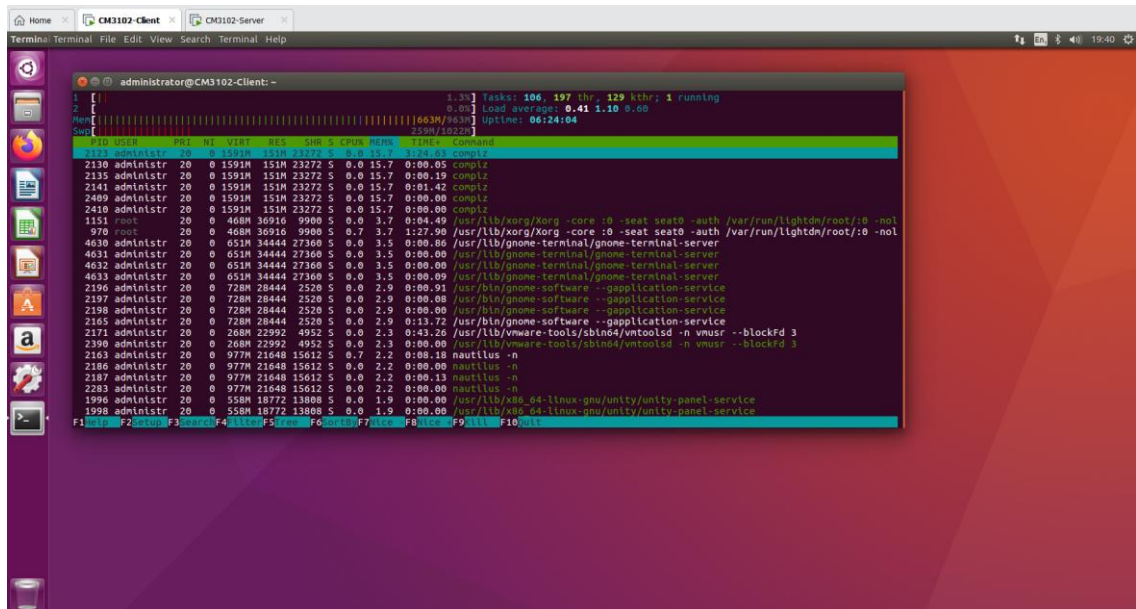


An alternative for the “top” system monitor would be the “htop” system monitor, which is also a command line system monitor, but more intuitive than “top” system monitor. The “htop” system monitor would have to be installed using the “sudo apt-get install htop” command in order to be used. Once the htop installation is completed the system monitor can be executed using the “htop” command which will execute the system monitor.



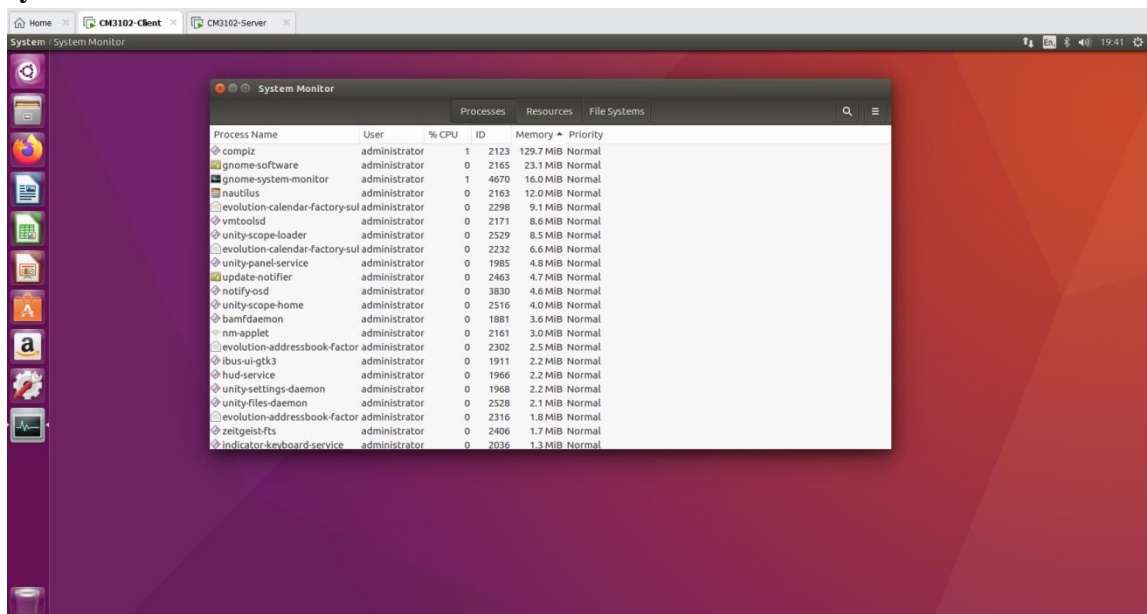
After the “htop” system monitor has been executed he will present a similar interface to the “top” system monitor, in order to make use of the “htop” system monitor the buttons mentioned at the bottom of the monitor must be used, a simple command of the “htop” would be the sorting command which can be accessed by pressing the F6 button, the result of performing this command can be seen in the image below.





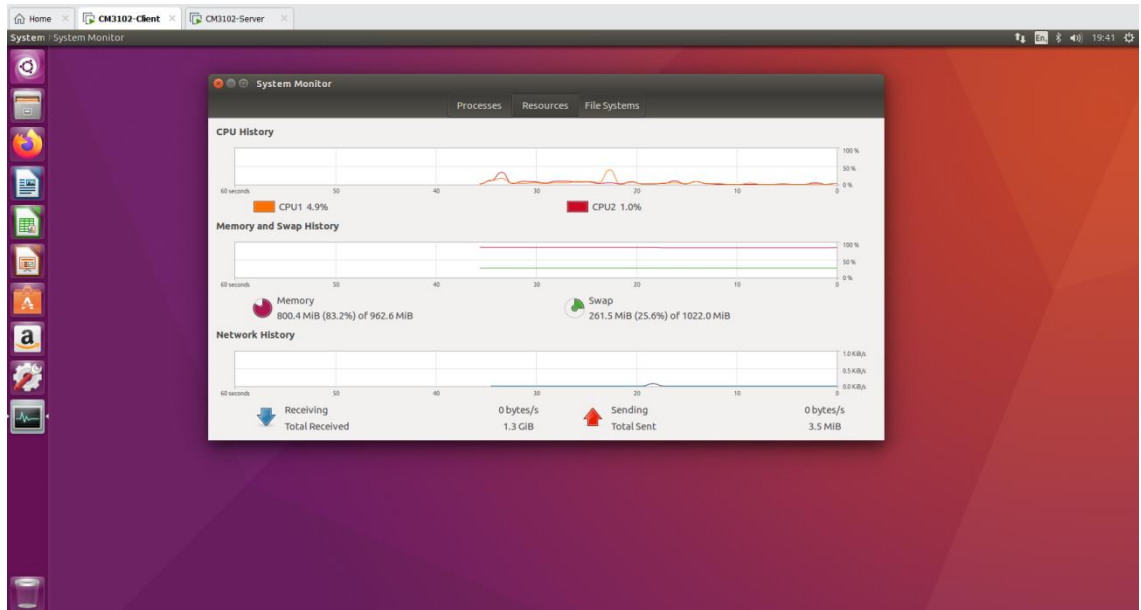
As we can see in the image above the sorting of the running processes is done by memory usage, this was done using the F6 command and selecting the memory field in the menu presented by the “htop” system monitor.

## System Monitor



Another alternative of system monitor would be the default graphical user interface system monitor provided by the Ubuntu Operating System, as we can see in the image above the system monitor presents a simple graphical user interface and very easy to work with, one of the features provided by the system monitor is the sorting feature which can be used by pressing on the columns seen in the image above, this will sort the table based on the column selected.





A feature present in the system monitor provided by the Ubuntu Operating System is the ability to visualise the network information, as we can see in the image above.

## 2.3

All the system monitors mentioned above are simple and efficient but the most efficient system monitor would be “htop” system monitor as it presents a convenient interface in order to perform any operations on the current running processes of the system.