Grupo 046

Hugo Fernandes (1161155), Norberto Sousa (1120680), Pedro Barbosa (1150486)

Administração de Sistemas

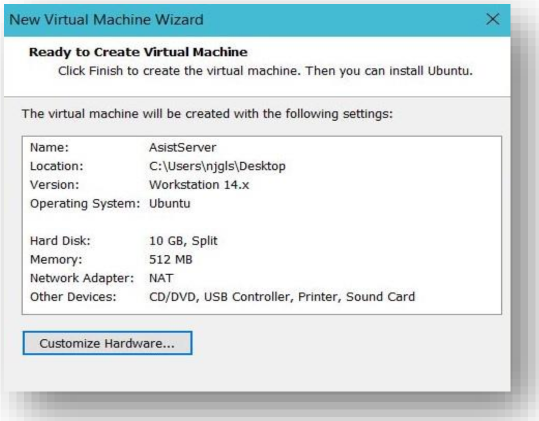
Tarefa Complementar 1, 21 de outubro 2018

Tarefa Complementar

Criação e configuração de uma máquina virtual

Configuração da máquina virtual

- **A placa de rede da máquina virtual encontra-se configurada com NAT, em vez de *bridged* como é pedido, visto que configurar em *bridged* causava problemas no log in que nos bloqueava fora da máquina o que fazia com que ela ficasse inutilizada.**



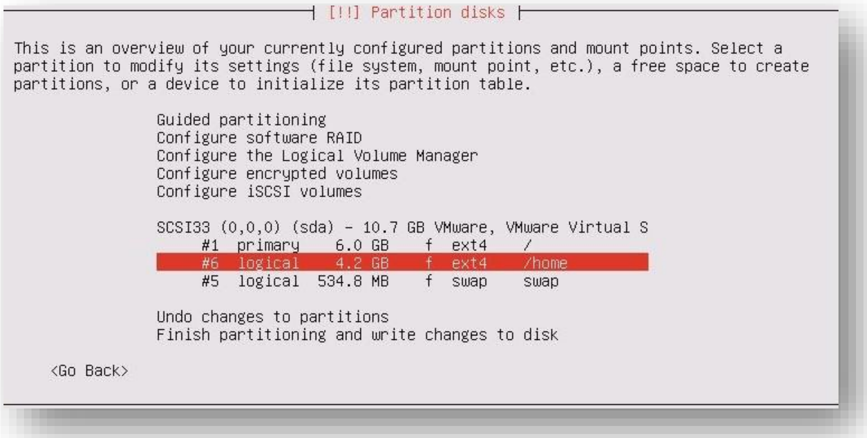
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

The virtual machine will be created with the following settings:

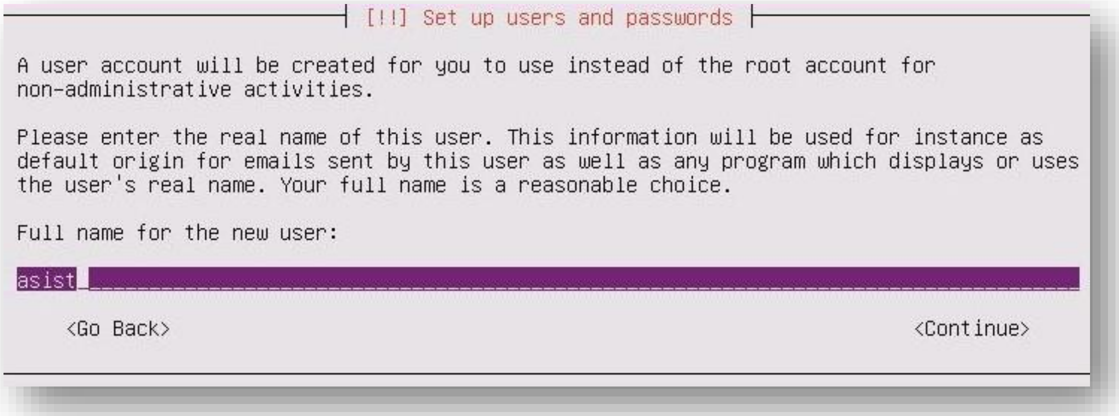
Name:	AsistServer
Location:	C:\Users\njgls\Desktop
Version:	Workstation 14.x
Operating System:	Ubuntu
Hard Disk:	10 GB, Split
Memory:	512 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

- **Disco de 10GB, partição de raiz de 6GB, sendo o resto atribuído a partição *home.***

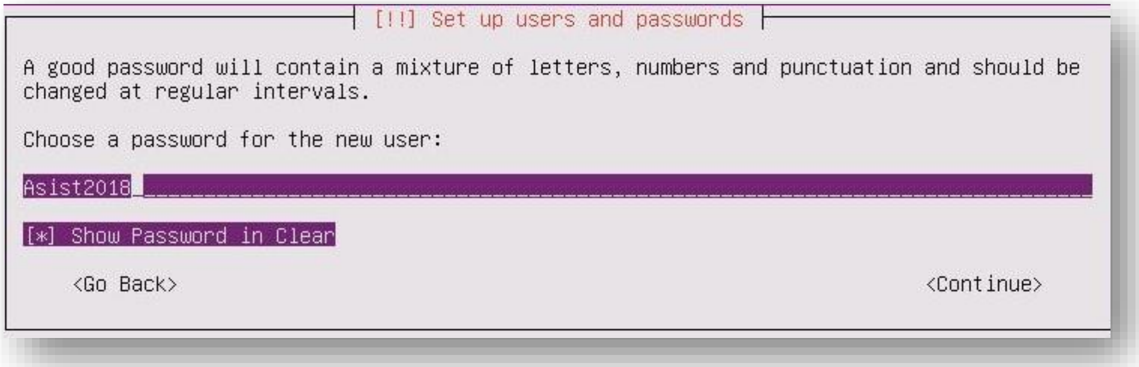


```
[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                Guided partitioning
                Configure software RAID
                Configure the Logical Volume Manager
                Configure encrypted volumes
                Configure iSCSI volumes

                SCSI33 (0,0,0) (sda) - 10.7 GB VMware, VMware Virtual S
                     #1  primary    6.0 GB    f  ext4    /
                     #6  logical    4.2 GB    f  ext4    /home
                     #5  logical  534.8 MB    f  swap    swap

                Undo changes to partitions
                Finish partitioning and write changes to disk

    <Go Back>
```

- **O utilizador “asist” é o utilizador administrador da nossa máquina virtual, tendo assim as permissões de sudo:**

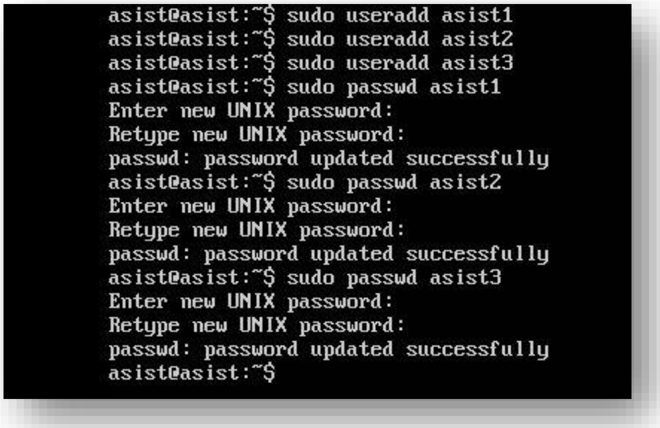


```
[!!] Set up users and passwords

A user account will be created for you to use instead of the root account for
non-administrative activities.

Please enter the real name of this user. This information will be used for instance as
default origin for emails sent by this user as well as any program which displays or uses
the user's real name. Your full name is a reasonable choice.

Full name for the new user:

asist_

    <Go Back>                                                        <Continue>
```



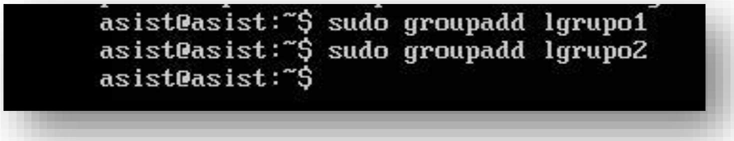
```
[!!] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be
changed at regular intervals.

Choose a password for the new user:

Asist2018_

[*] Show Password in Clear

    <Go Back>                                                        <Continue>
```

- **Utilizamos esse utilizador para gerar os outros utilizadores, asist1, asist2 e asist3 sem permissões sudo:**

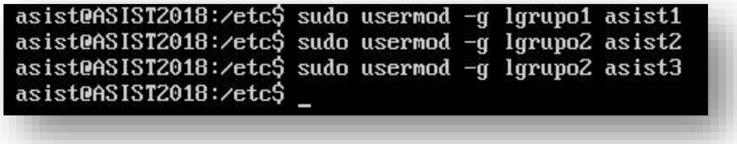


```
asist@asist:~$ sudo useradd asist1
asist@asist:~$ sudo useradd asist2
asist@asist:~$ sudo useradd asist3
asist@asist:~$ sudo passwd asist1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
asist@asist:~$ sudo passwd asist2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
asist@asist:~$ sudo passwd asist3
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
asist@asist:~$
```

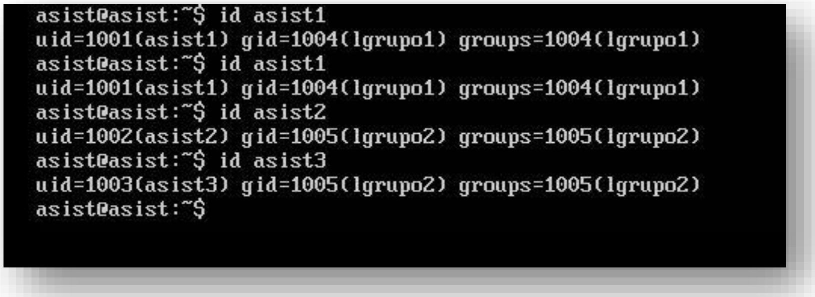
- **Criação dos grupos lgrupo1 e lgrupo2, sendo o lgrupo1 o primário do utilizador asist1 e o lgrupo2 dos asist2 e asist3:**



```
asist@asist:~$ sudo groupadd lgrupo1
asist@asist:~$ sudo groupadd lgrupo2
asist@asist:~$
```

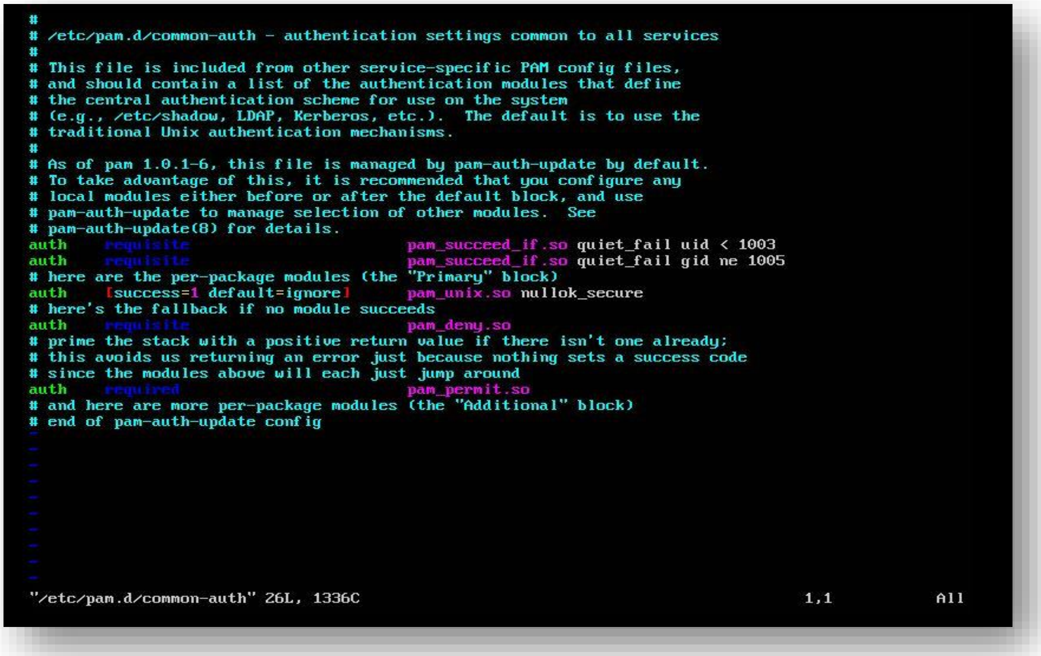


```
asist@ASIST2018:/etc$ sudo usermod -g lgrupo1 asist1
asist@ASIST2018:/etc$ sudo usermod -g lgrupo2 asist2
asist@ASIST2018:/etc$ sudo usermod -g lgrupo2 asist3
asist@ASIST2018:/etc$ _
```



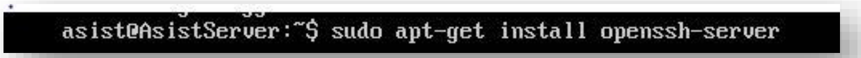
```
asist@asist:~$ id asist1
uid=1001(asist1) gid=1004(lgrupo1) groups=1004(lgrupo1)
asist@asist:~$ id asist1
uid=1001(asist1) gid=1004(lgrupo1) groups=1004(lgrupo1)
asist@asist:~$ id asist2
uid=1002(asist2) gid=1005(lgrupo2) groups=1005(lgrupo2)
asist@asist:~$ id asist3
uid=1003(asist3) gid=1005(lgrupo2) groups=1005(lgrupo2)
asist@asist:~$
```

- **Limitar o acesso ao sistema só a *users* com UID inferior a 1003 e que não pertençam ao lgrupo2:**

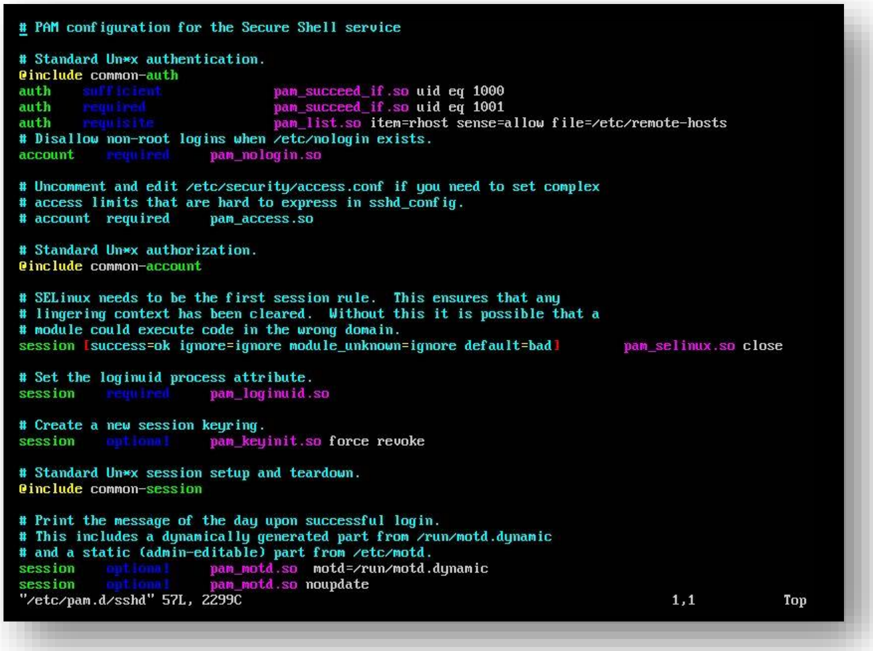


```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
auth    requisite                       pam_succeed_if.so quiet_fail uid < 1003
auth    requisite                       pam_succeed_if.so quiet_fail gid ne 1005
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
~
~
~
~
~
~
~
~
~
~
"/etc/pam.d/common-auth" 26L, 1336C                          1,1           All
```

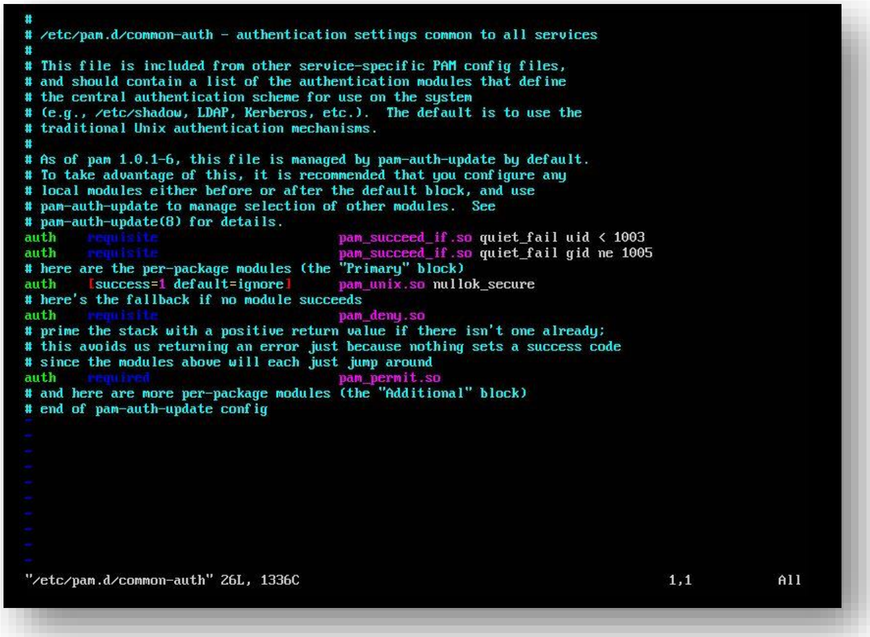
- **Limitar o acesso SSH ao utilizador asist1 se for** lançado **de uma má**quina **a criar *Limitar o acesso SSH ao utilizador asist1 se for* e ao utilizador asist independentemente da** máquina **a partir da qual inicia o SSH:**



```
asist@AsistServer:~$ sudo apt-get install openssh-server
```

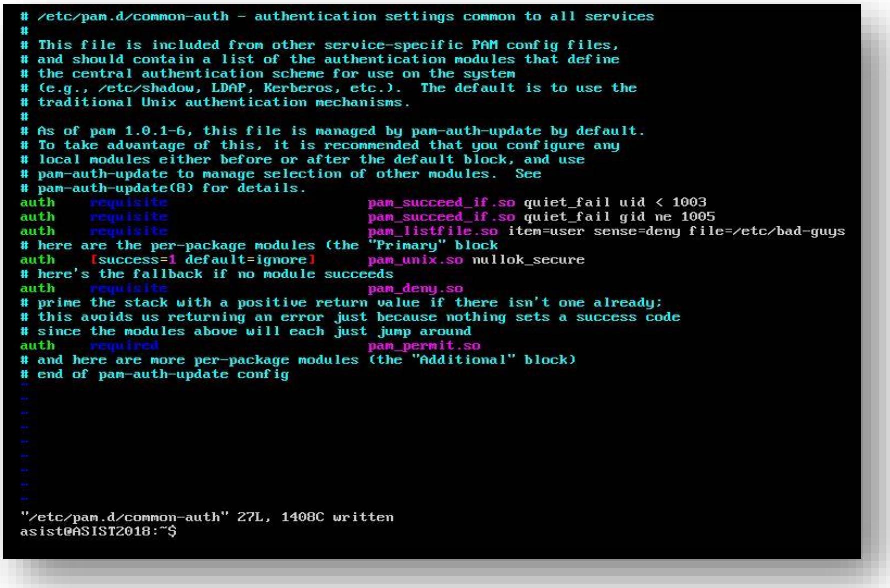


```
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
@include common-auth
auth    sufficient              pam_succeed_if.so uid eq 1000
auth    required                pam_succeed_if.so uid eq 1001
auth    requisite               pam_list.so item=rhost sense=allow file=/etc/remote-hosts
# Disallow non-root logins when /etc/nologin exists.
account    required     pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so

# Standard Un*x authorization.
@include common-account

# SELinux needs to be the first session rule.  This ensures that any
# lingering context has been cleared.  Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so close

# Set the loginuid process attribute.
session    required     pam_loginuid.so

# Create a new session keyring.
session    optional     pam_keyinit.so force revoke

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional     pam_motd.so  motd=/run/motd.dynamic
session    optional     pam_motd.so noupdate
"/etc/pam.d/sshd" 57L, 2299C                                              1,1           Top
```



```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
auth    requisite                       pam_succeed_if.so quiet_fail uid < 1003
auth    requisite                       pam_succeed_if.so quiet_fail gid ne 1005
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
~
~
~
~
~
~
~
~
~
~
"/etc/pam.d/common-auth" 26L, 1336C                                       1,1           All
```

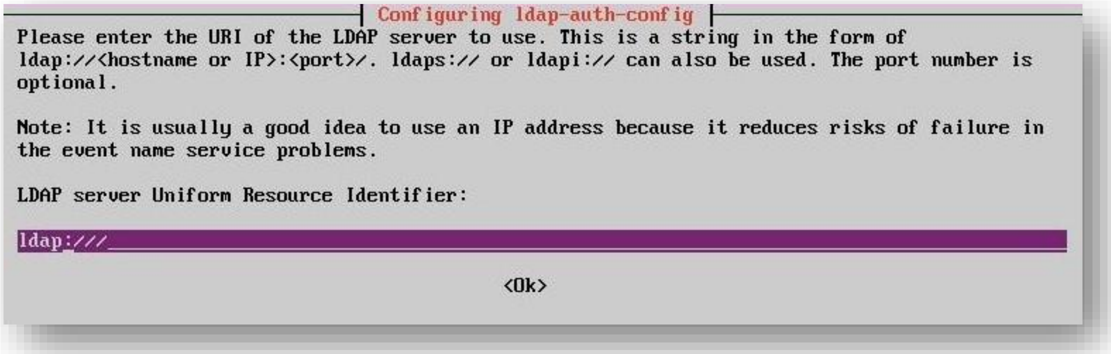
- **O acesso será negado aos users que estejam registados no ficheiro */etc/bad-guys*:**



```
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
auth    requisite                       pam_succeed_if.so quiet_fail uid < 1003
auth    requisite                       pam_succeed_if.so quiet_fail gid ne 1005
auth    requisite                       pam_listfile.so item=user sense=deny file=/etc/bad-guys
# here are the per-package modules (the "Primary" block
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
~
~
~
~
~
~
~
~
~
"/etc/pam.d/common-auth" 27L, 1408C written
asist@ASIST2018:~$
```

Configuração do LDAP do DEI

1. **LDAP server**



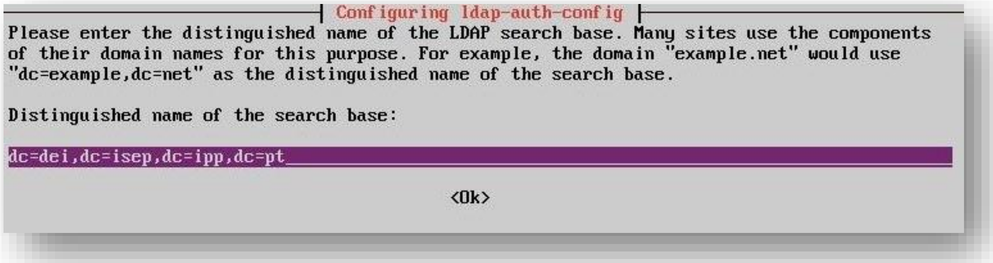
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldap:///

2. **Search base**

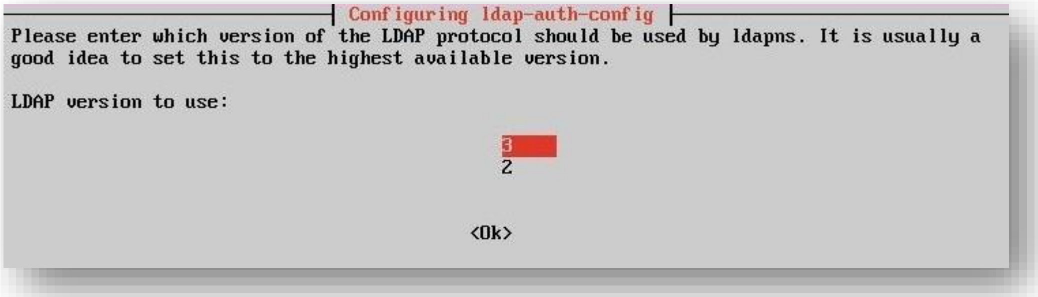


Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=dei,dc=isep,dc=ipp,dc=pt

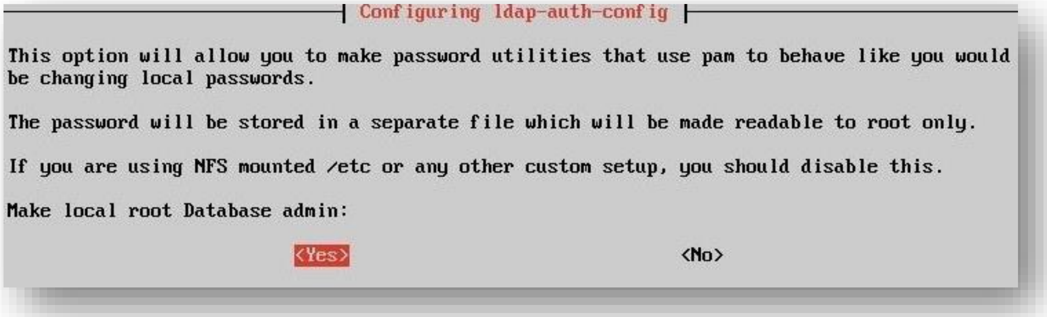
3. **Versão**



Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

4. **Administrar base de dados (não)**



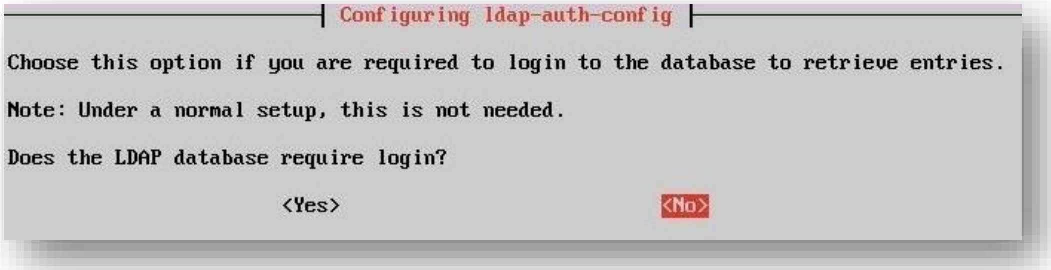
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

5. **Base de dados requer login (não)**

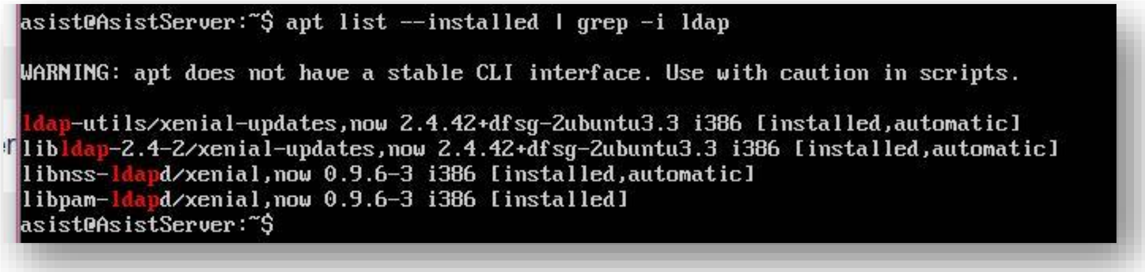


Choose this option if you are required to login to the database to retrieve entries.

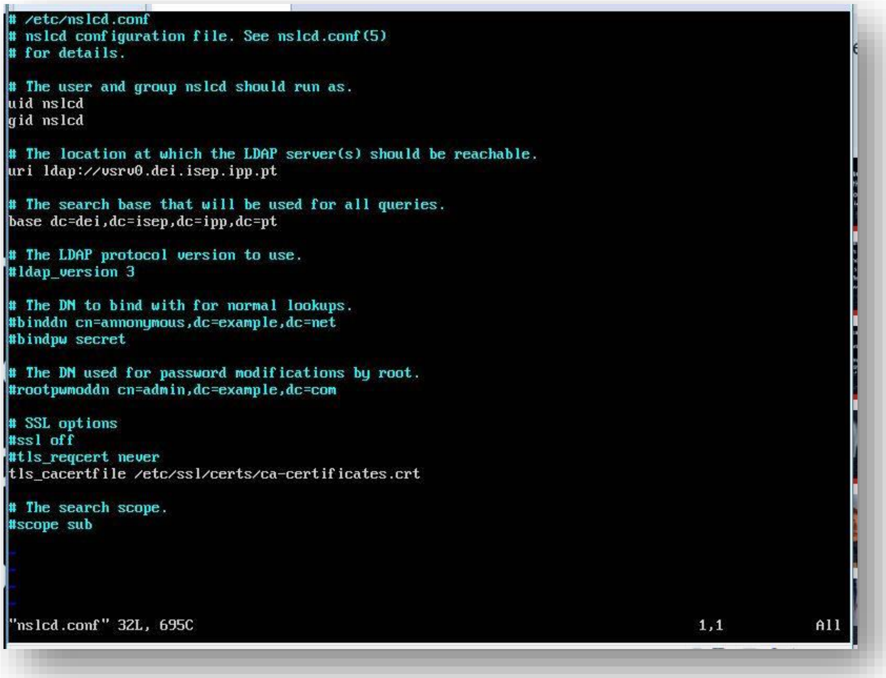
Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

6. **LDAP instalado**

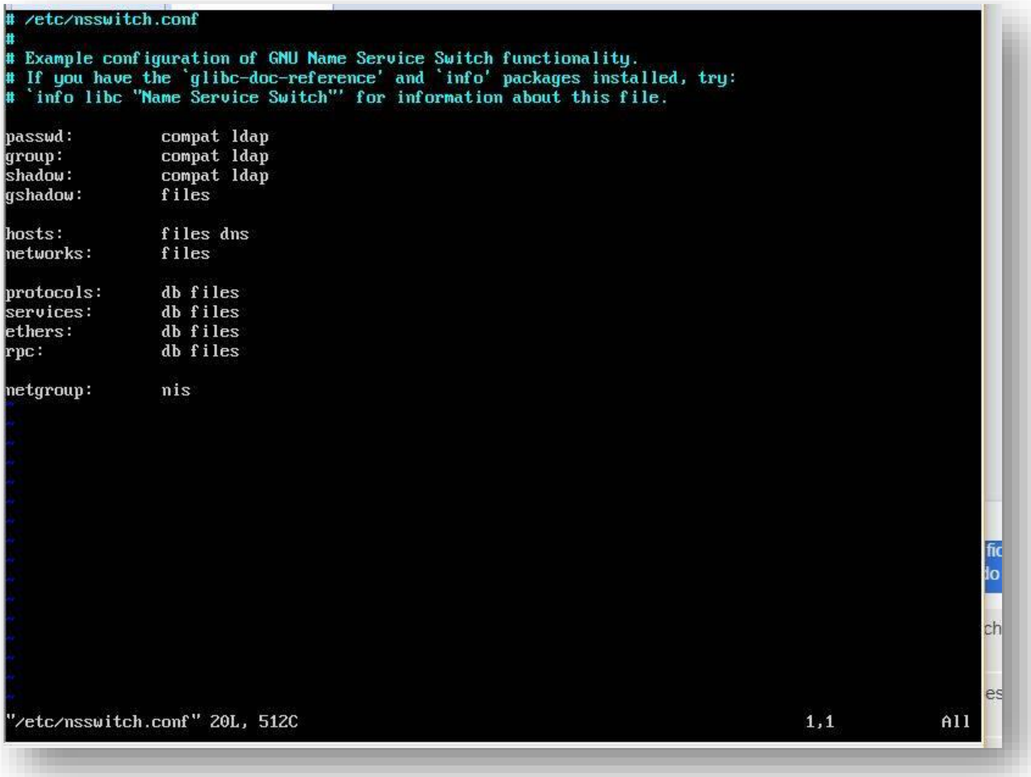


```
asist@AsistServer:~$ apt list --installed | grep -i ldap

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

ldap-utils/xenial-updates,now 2.4.42+dfsg-2ubuntu3.3 i386 [installed,automatic]
libldap-2.4-2/xenial-updates,now 2.4.42+dfsg-2ubuntu3.3 i386 [installed,automatic]
libnss-ldapd/xenial,now 0.9.6-3 i386 [installed,automatic]
libpam-ldapd/xenial,now 0.9.6-3 i386 [installed]
asist@AsistServer:~$
```



```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable.
uri ldap://vsrv0.dei.isep.ipp.pt

# The search base that will be used for all queries.
base dc=dei,dc=isep,dc=ipp,dc=pt

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
#bindpw secret

# The DN used for password modifications by root.
#rootpwmoddn cn=admin,dc=example,dc=com

# SSL options
#ssl off
#tls_reqcert never
tls_cacertfile /etc/ssl/certs/ca-certificates.crt

# The search scope.
#scope sub

~
~
~
~
"nslcd.conf" 32L, 695C                                              1,1           All
```

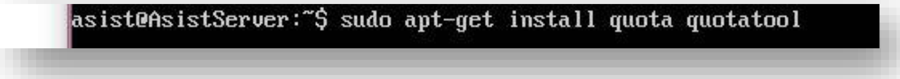
7. Ficheiro de nsswitch.conf



```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/nsswitch.conf" 20L, 512C                                   1,1           All
```

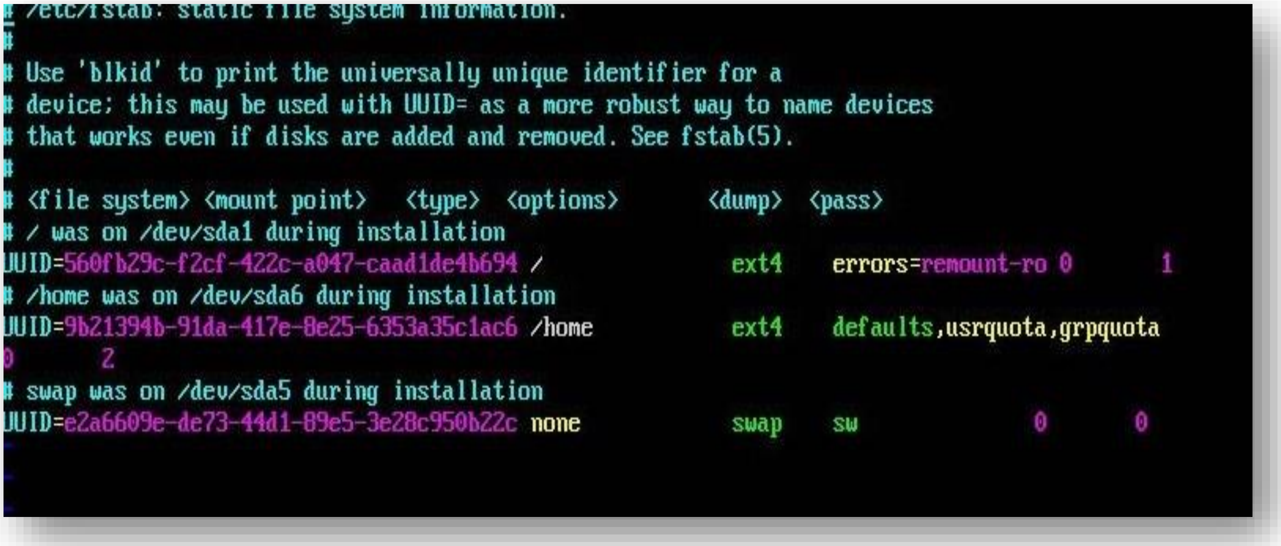
Quotas

1. **Instalar quota**



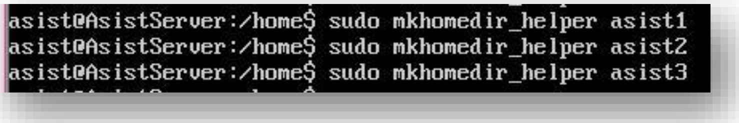
```
asist@AsistServer:~$ sudo apt-get install quota quotatool
```

2. **Ficheiro das quotas**



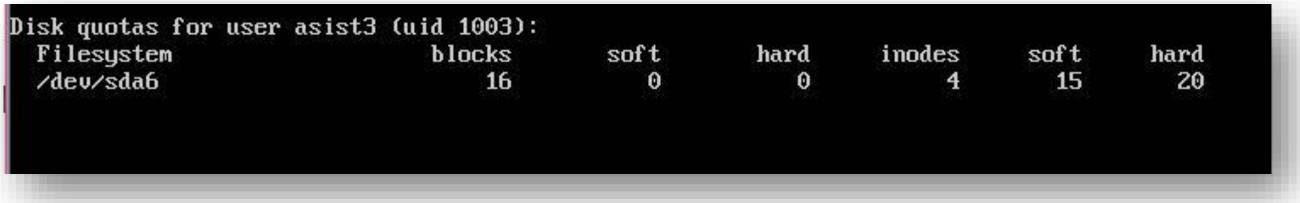
```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=560fb29c-f2cf-422c-a047-caad1de4b694 /               ext4    errors=remount-ro 0       1
# /home was on /dev/sda6 during installation
UUID=9b21394b-91da-417e-8e25-6353a35c1ac6 /home           ext4    defaults,usrquota,grpquota
0       2
# swap was on /dev/sda5 during installation
UUID=e2a6609e-de73-44d1-89e5-3e28c950b22c none            swap    sw              0       0
```

3. **Criar *homedir***



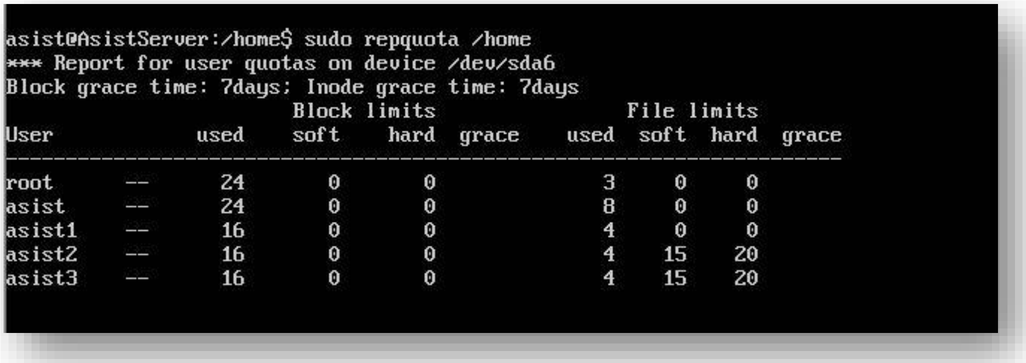
```
asist@AsistServer:/home$ sudo mkhomedir_helper asist1
asist@AsistServer:/home$ sudo mkhomedir_helper asist2
asist@AsistServer:/home$ sudo mkhomedir_helper asist3
```

4. **Editar quotas**



```
Disk quotas for user asist3 (uid 1003):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/sda6                        16          0          0          4       15       20
```

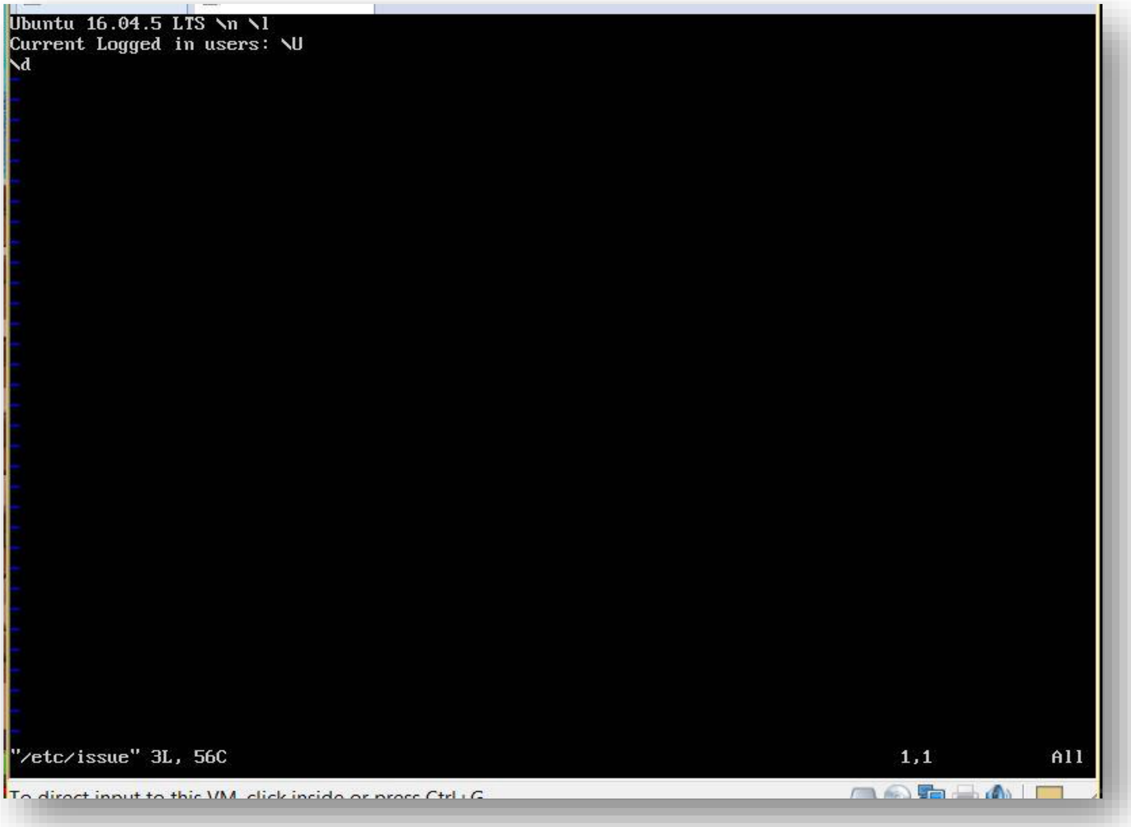
5. **Todas as quotas**



```
asist@AsistServer:/home$ sudo repquota /home
*** Report for user quotas on device /dev/sda6
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --      24       0       0              3     0     0
asist     --      24       0       0              8     0     0
asist1    --      16       0       0              4     0     0
asist2    --      16       0       0              4    15    20
asist3    --      16       0       0              4    15    20
```

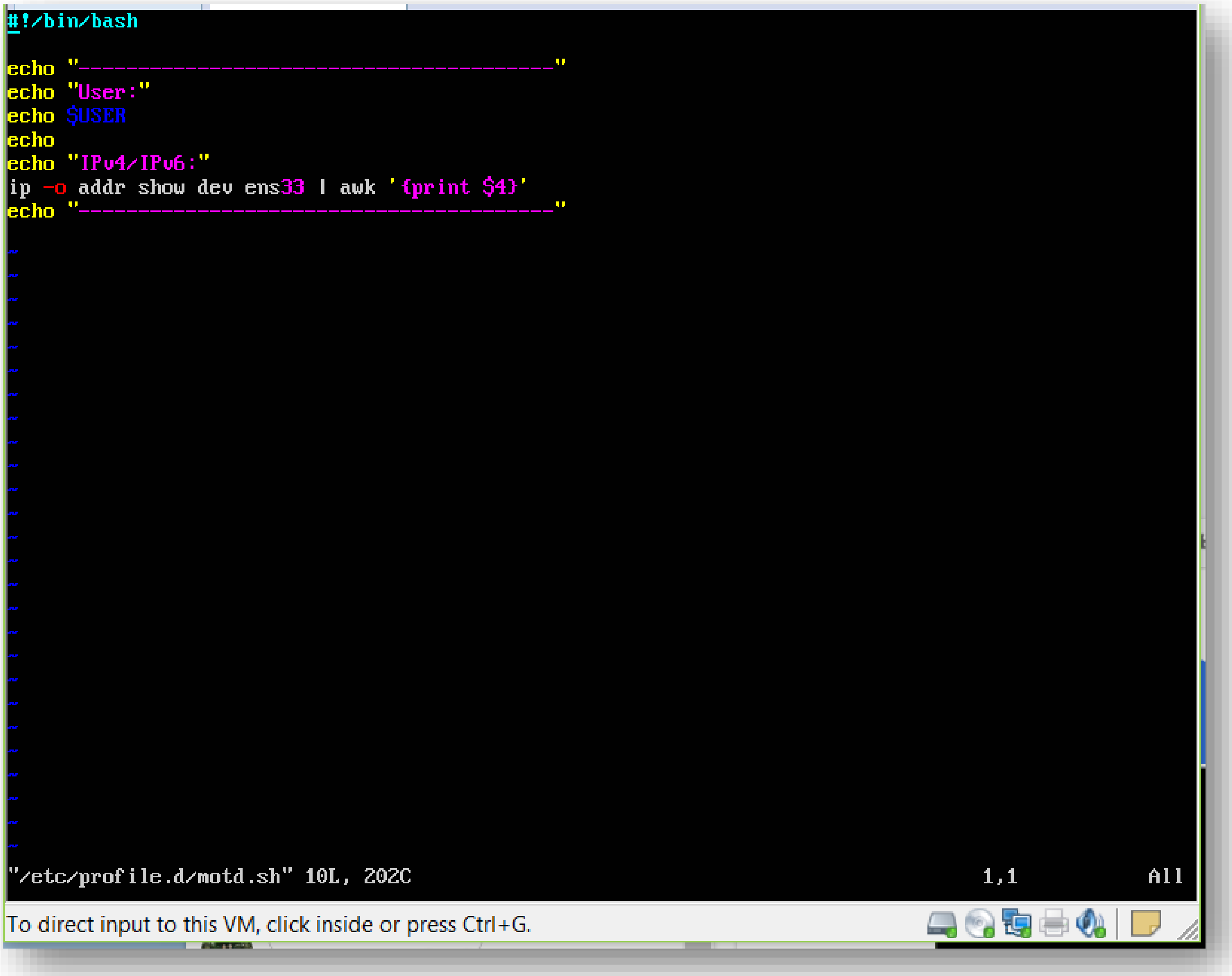
MOTD

1. **Informação pré-autenticação**



```
Ubuntu 16.04.5 LTS \n \l
Current Logged in users: \U
\d




"/etc/issue" 3L, 56C                                          1,1           All
```

2. Ficheiro MOTD



```
#!/bin/bash

echo "----------------------------------------"
echo "User:"
echo $USER
echo
echo "IPv4/IPv6:"
ip -o addr show dev ens33 | awk '{print $4}'
echo "----------------------------------------"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/profile.d/motd.sh" 10L, 202C                    1,1           All
```

To direct input to this VM, click inside or press Ctrl+G.