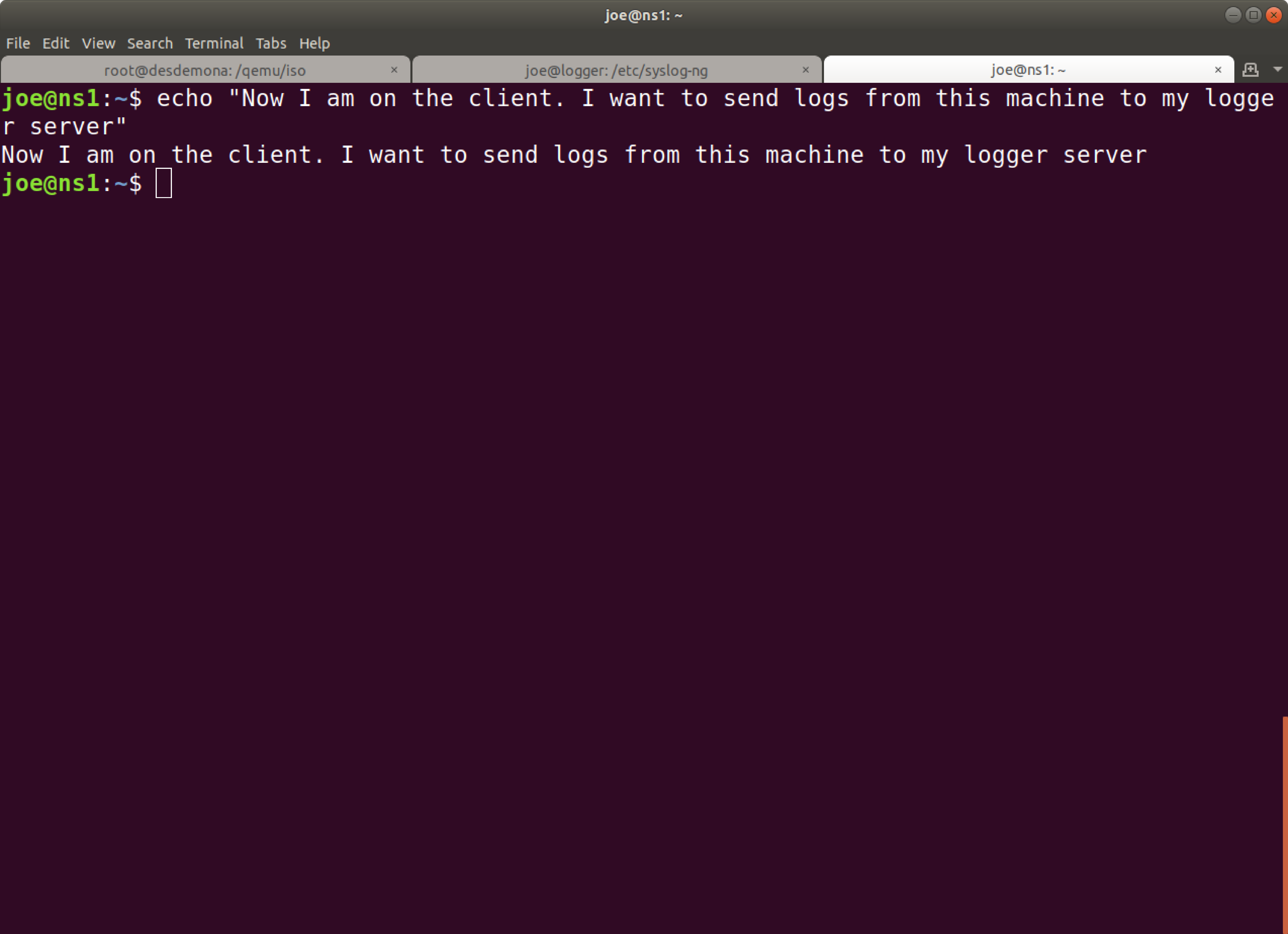
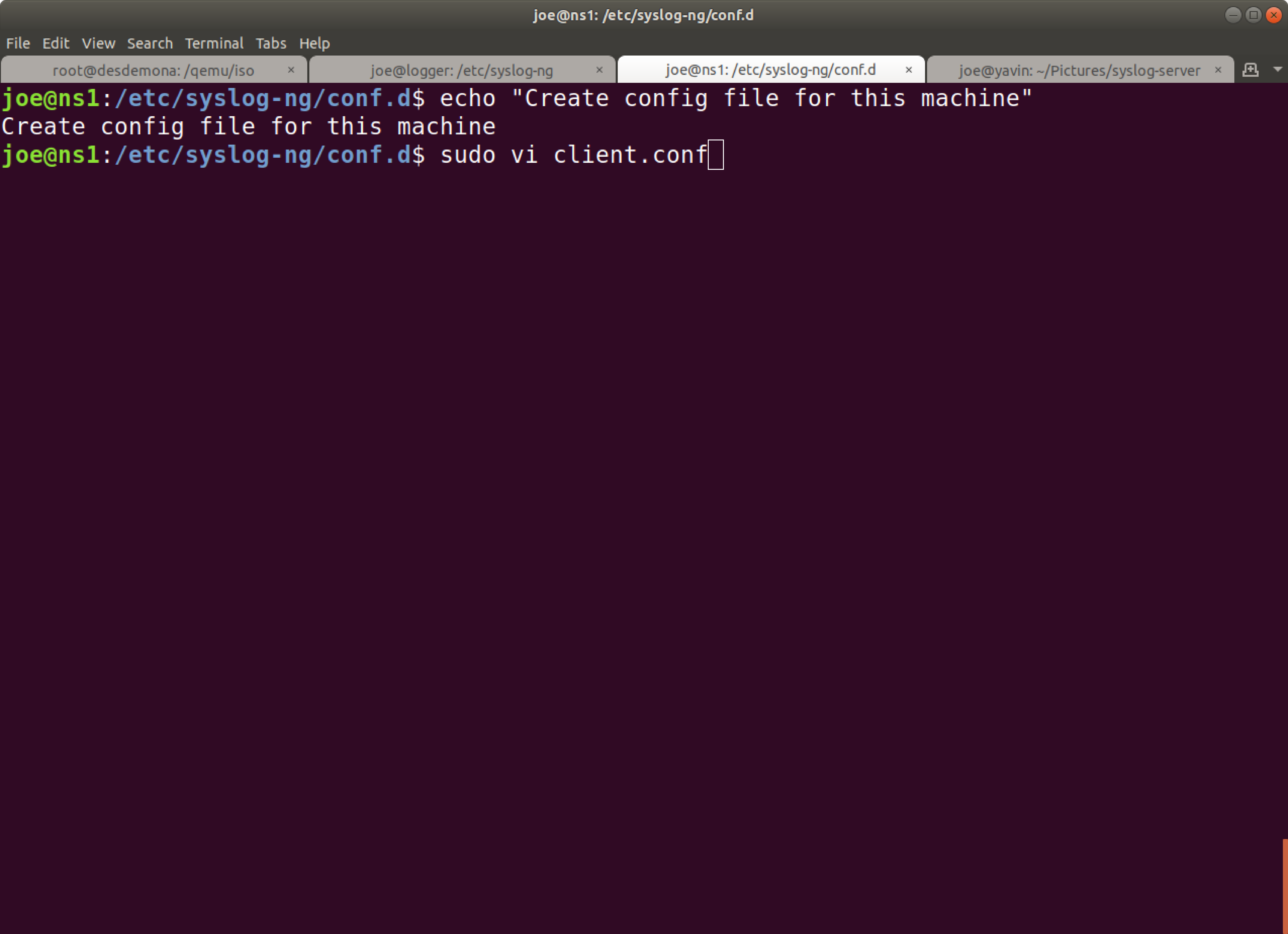
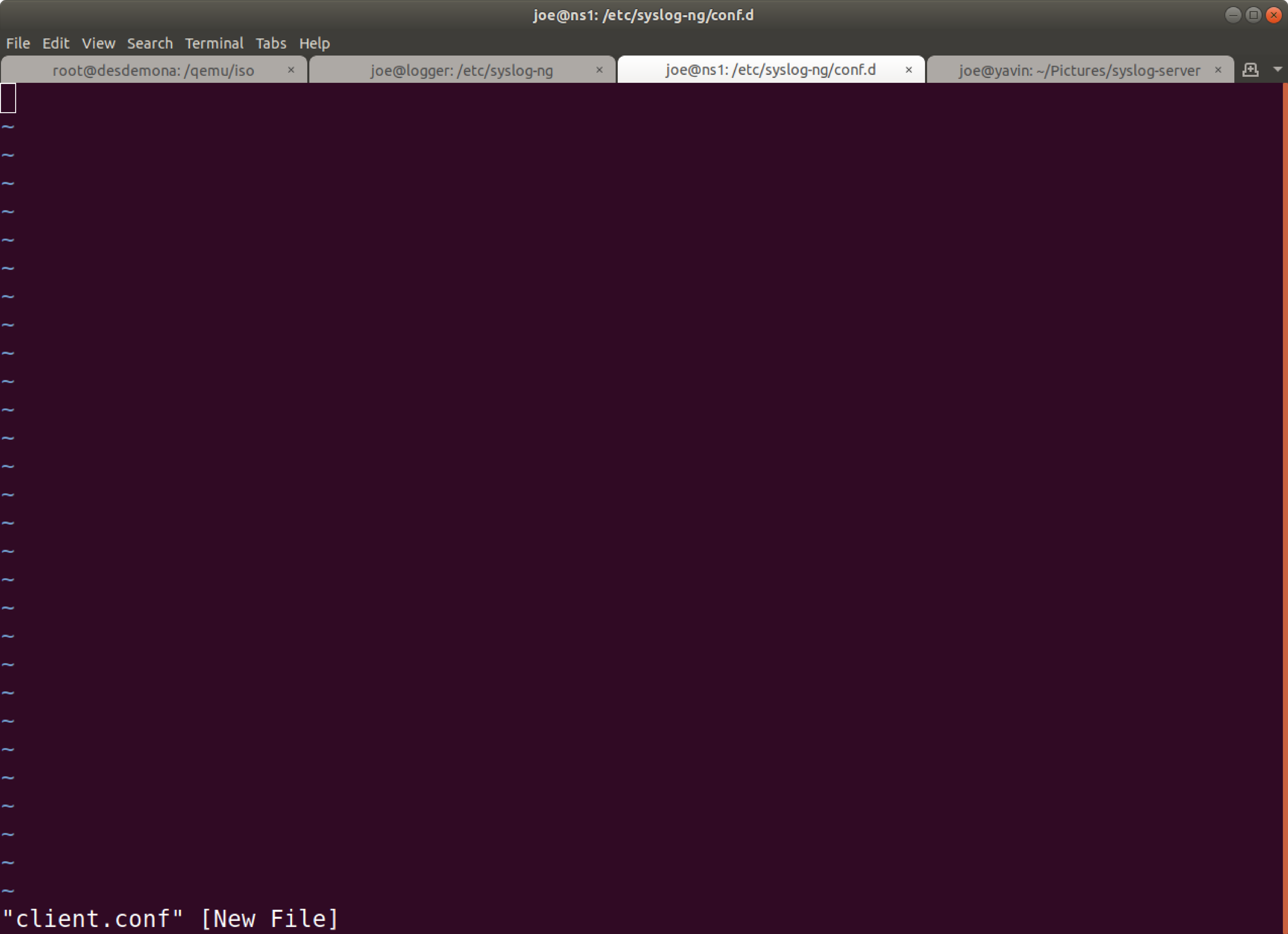


```
joe@ns1:~$ echo "Now I am on the client. I want to send logs from this machine to my logge
r server"
Now I am on the client. I want to send logs from this machine to my logger server
joe@ns1:~$ 
```

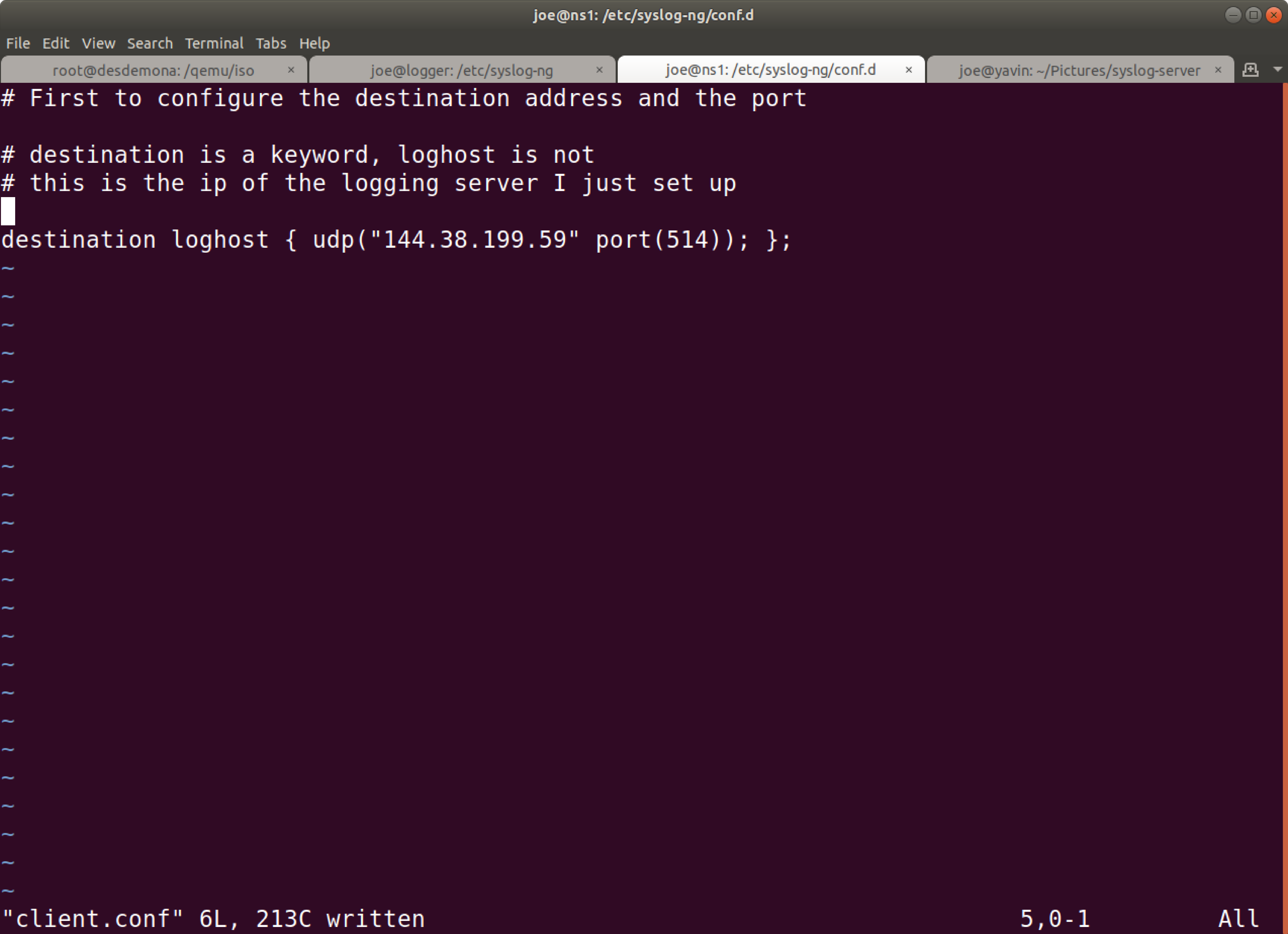


joe@ns1: /etc/syslog-ng/conf.d
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng/conf.d
joe@yavin: ~/Pictures/syslog-server

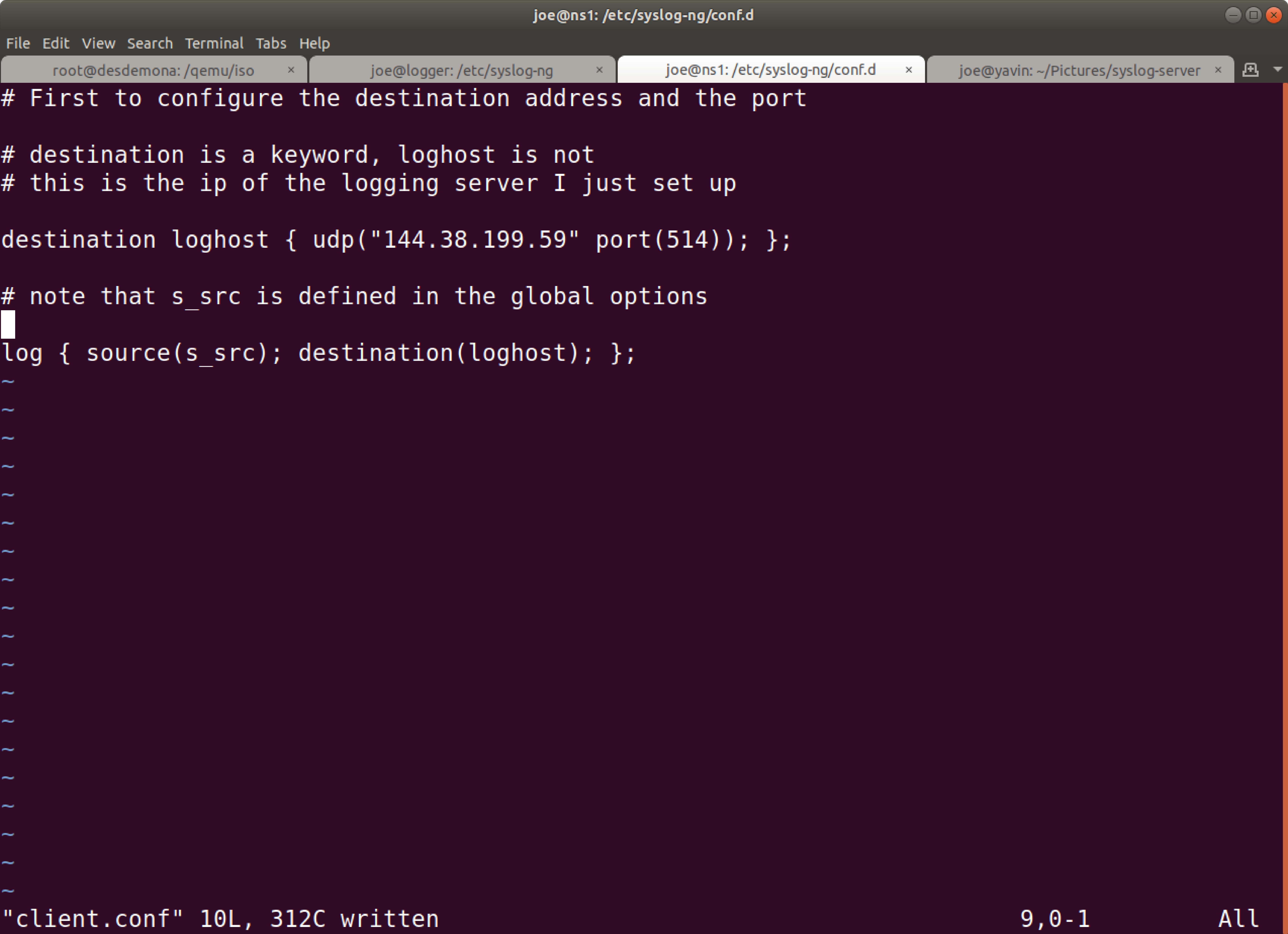
```
joe@ns1:/etc/syslog-ng/conf.d$ echo "Create config file for this machine"
Create config file for this machine
joe@ns1:/etc/syslog-ng/conf.d$ sudo vi client.conf
```


joe@ns1: /etc/syslog-ng/conf.d
File
Edit
View
Search
Terminal
Tabs
Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng/conf.d
joe@yavin: ~/Pictures/syslog-server

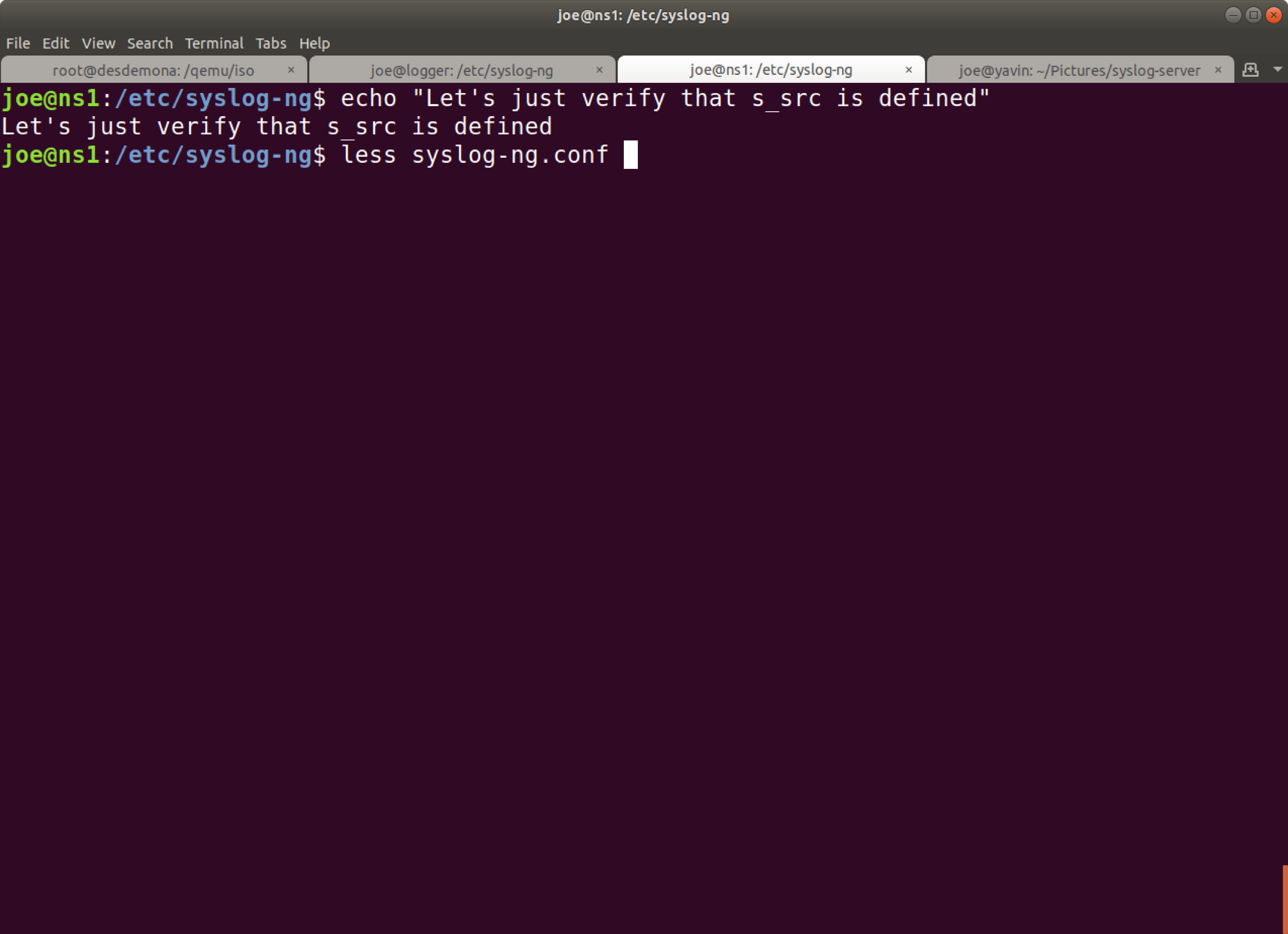
```

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"client.conf" [New File]
```


joe@ns1: /etc/syslog-ng/conf.d
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng/conf.d
joe@yavin: ~/Pictures/syslog-server

```
# First to configure the destination address and the port

# destination is a keyword, loghost is not
# this is the ip of the logging server I just set up

destination loghost { udp("144.38.199.59" port(514)); };
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"client.conf" 6L, 213C written                                    5,0-1         All
```

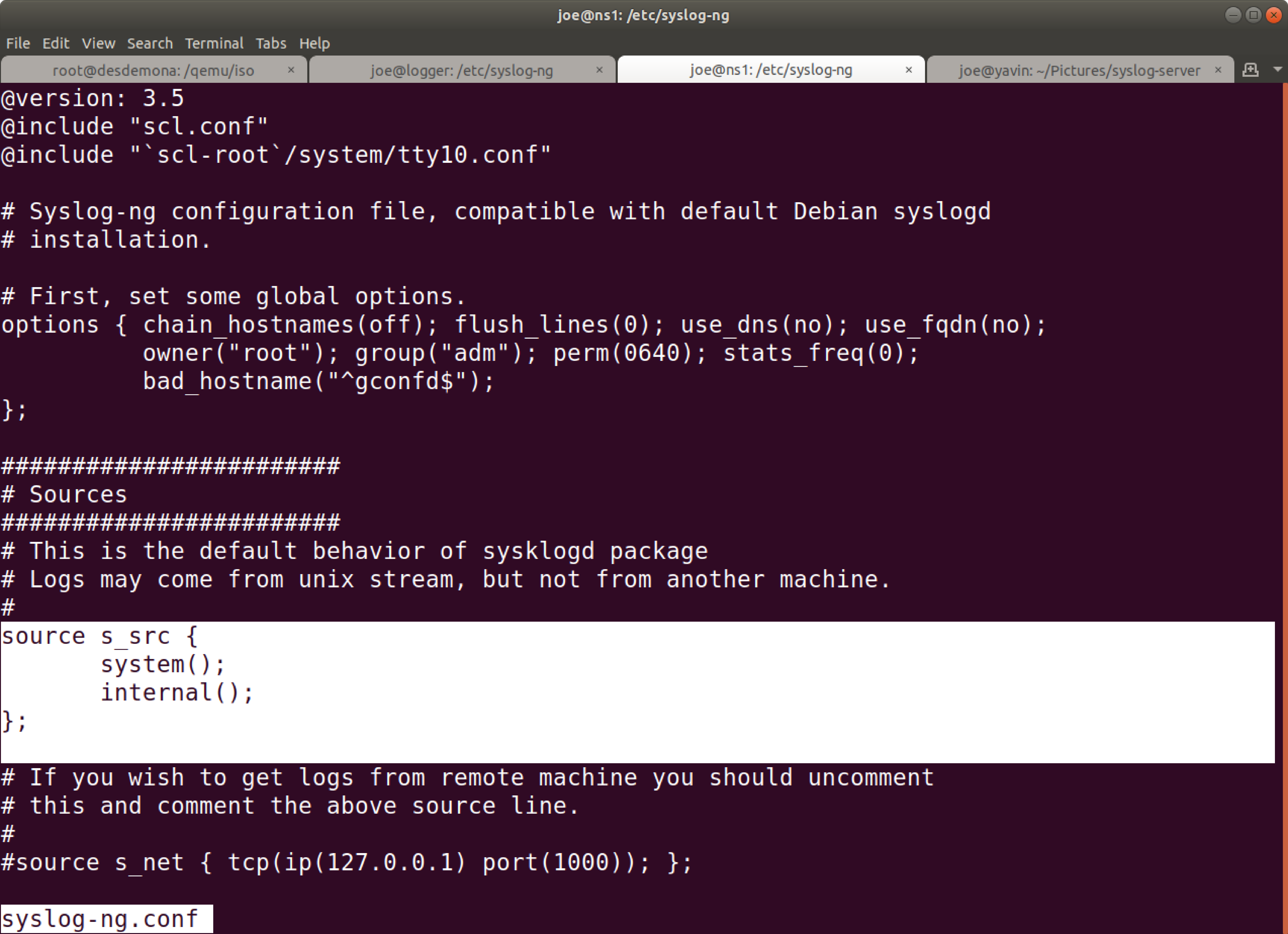

joe@ns1: /etc/syslog-ng/conf.d
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng/conf.d
joe@yavin: ~/Pictures/syslog-server

```
# First to configure the destination address and the port

# destination is a keyword, loghost is not
# this is the ip of the logging server I just set up

destination loghost { udp("144.38.199.59" port(514)); };

# note that s_src is defined in the global options

log { source(s_src); destination(loghost); };
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"client.conf" 10L, 312C written                                    9,0-1         All
```

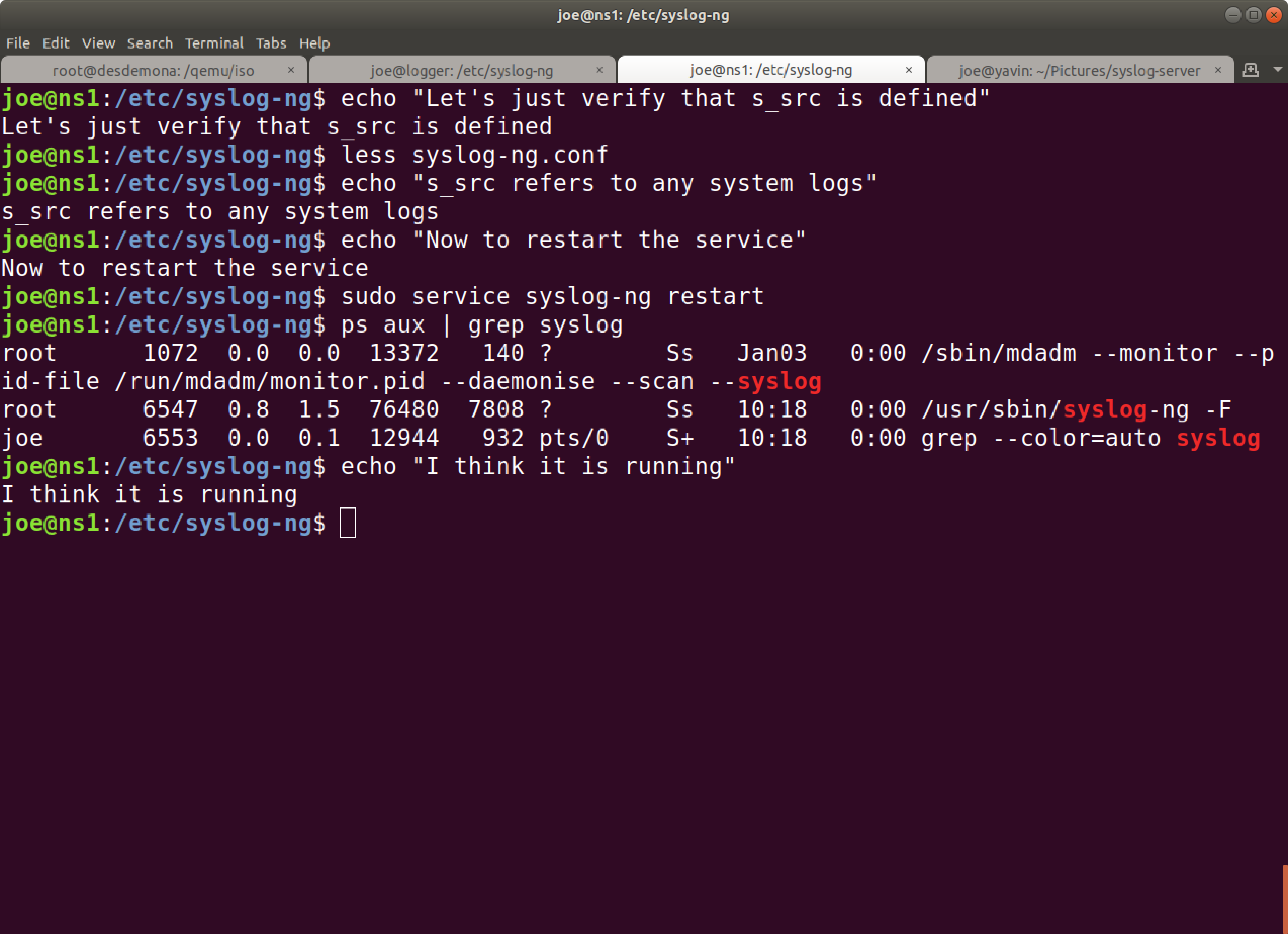


joe@ns1: /etc/syslog-ng
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng
joe@yavin: ~/Pictures/syslog-server

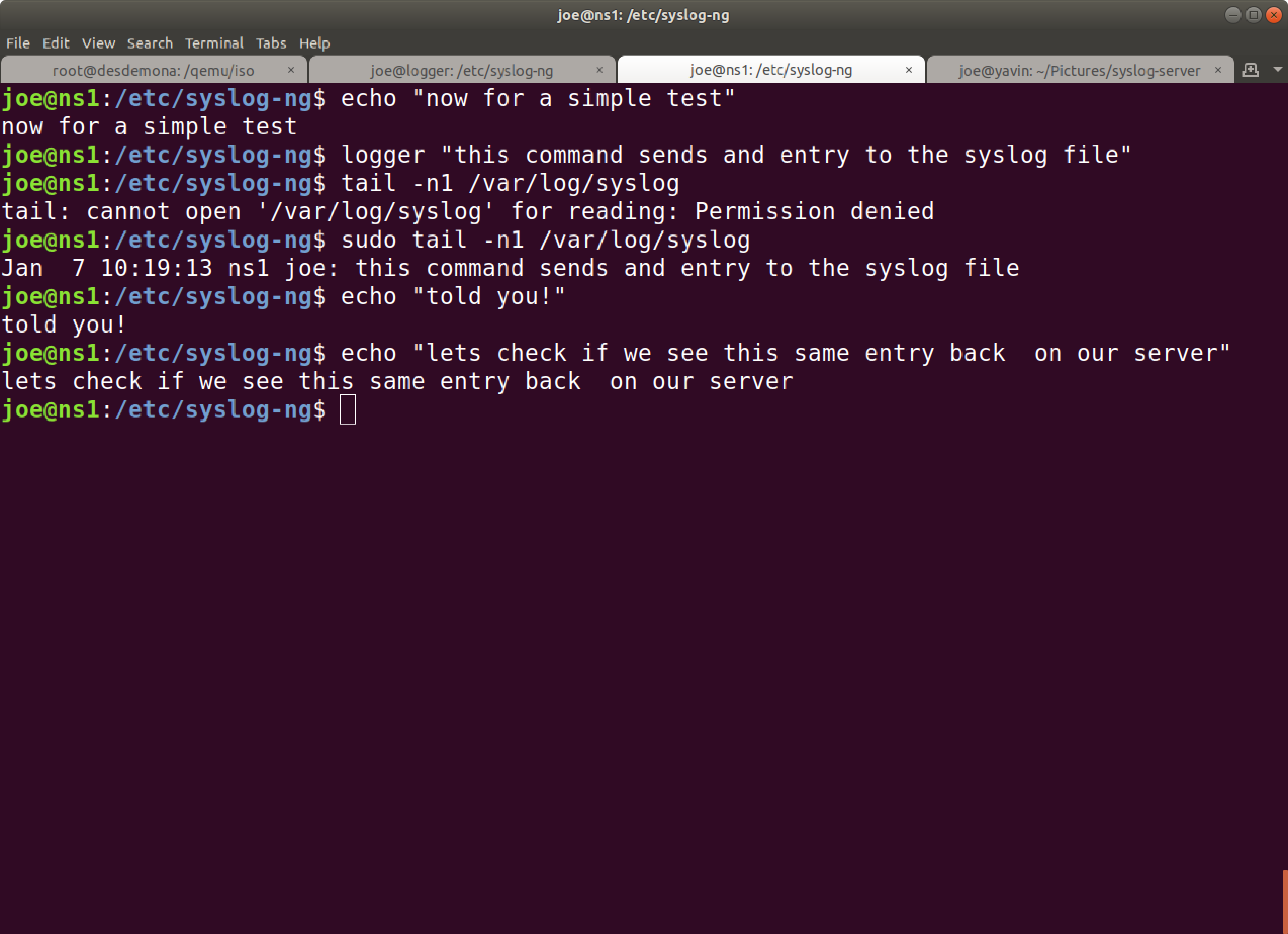
```
joe@ns1:/etc/syslog-ng$ echo "Let's just verify that s_src is defined"
Let's just verify that s_src is defined
joe@ns1:/etc/syslog-ng$ less syslog-ng.conf
```


joe@ns1: /etc/syslog-ng
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng
joe@yavin: ~/Pictures/syslog-server

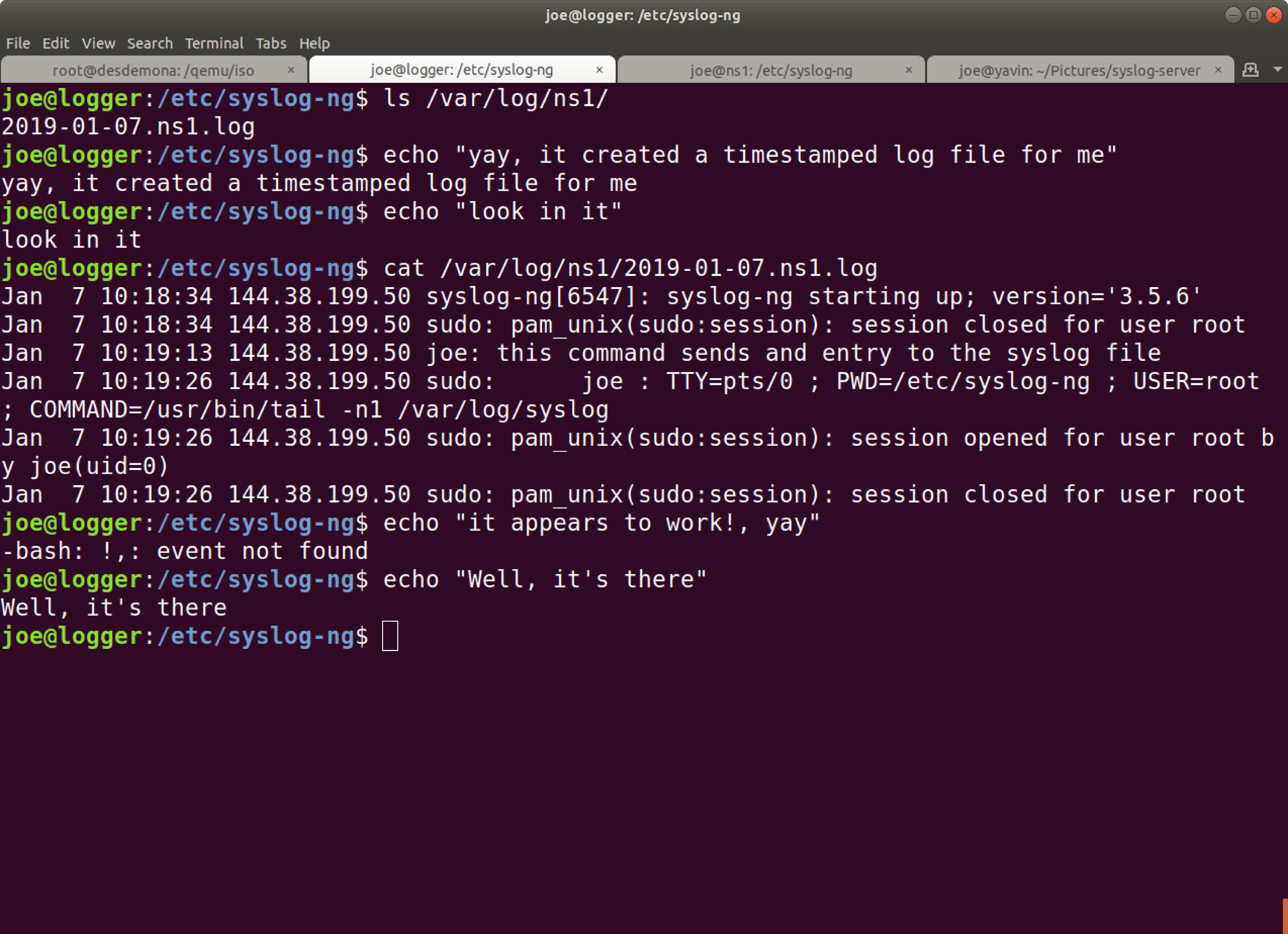
```
@version: 3.5
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"

# Syslog-ng configuration file, compatible with default Debian syslogd
# installation.

# First, set some global options.
options { chain_hostnames(off); flush_lines(0); use_dns(no); use_fqdn(no);
          owner("root"); group("adm"); perm(0640); stats_freq(0);
          bad_hostname("^gconfd$");
};

########################
# Sources
########################
# This is the default behavior of sysklogd package
# Logs may come from unix stream, but not from another machine.
#
source s_src {
       system();
       internal();
};

# If you wish to get logs from remote machine you should uncomment
# this and comment the above source line.
#
#source s_net { tcp(ip(127.0.0.1) port(1000)); };

syslog-ng.conf
```


joe@ns1: /etc/syslog-ng
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng
joe@yavin: ~/Pictures/syslog-server

```
joe@ns1:/etc/syslog-ng$ echo "Let's just verify that s_src is defined"
Let's just verify that s_src is defined
joe@ns1:/etc/syslog-ng$ less syslog-ng.conf
joe@ns1:/etc/syslog-ng$ echo "s_src refers to any system logs"
s_src refers to any system logs
joe@ns1:/etc/syslog-ng$ echo "Now to restart the service"
Now to restart the service
joe@ns1:/etc/syslog-ng$ sudo service syslog-ng restart
joe@ns1:/etc/syslog-ng$ ps aux | grep syslog
root      1072  0.0  0.0  13372   140 ?        Ss   Jan03   0:00 /sbin/mdadm --monitor --p
id-file /run/mdadm/monitor.pid --daemonise --scan --syslog
root      6547  0.8  1.5  76480  7808 ?        Ss   10:18   0:00 /usr/sbin/syslog-ng -F
joe       6553  0.0  0.1  12944   932 pts/0    S+   10:18   0:00 grep --color=auto syslog
joe@ns1:/etc/syslog-ng$ echo "I think it is running"
I think it is running
joe@ns1:/etc/syslog-ng$ 
```


joe@ns1: /etc/syslog-ng
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng
joe@yavin: ~/Pictures/syslog-server

```
joe@ns1:/etc/syslog-ng$ echo "now for a simple test"
now for a simple test
joe@ns1:/etc/syslog-ng$ logger "this command sends and entry to the syslog file"
joe@ns1:/etc/syslog-ng$ tail -n1 /var/log/syslog
tail: cannot open '/var/log/syslog' for reading: Permission denied
joe@ns1:/etc/syslog-ng$ sudo tail -n1 /var/log/syslog
Jan  7 10:19:13 ns1 joe: this command sends and entry to the syslog file
joe@ns1:/etc/syslog-ng$ echo "told you!"
told you!
joe@ns1:/etc/syslog-ng$ echo "lets check if we see this same entry back  on our server"
lets check if we see this same entry back  on our server
joe@ns1:/etc/syslog-ng$ 
```


joe@logger: /etc/syslog-ng
File Edit View Search Terminal Tabs Help
root@desdemona: /qemu/iso
joe@logger: /etc/syslog-ng
joe@ns1: /etc/syslog-ng
joe@yavin: ~/Pictures/syslog-server

```
joe@logger:/etc/syslog-ng$ ls /var/log/ns1/
2019-01-07.ns1.log
joe@logger:/etc/syslog-ng$ echo "yay, it created a timestamped log file for me"
yay, it created a timestamped log file for me
joe@logger:/etc/syslog-ng$ echo "look in it"
look in it
joe@logger:/etc/syslog-ng$ cat /var/log/ns1/2019-01-07.ns1.log
Jan  7 10:18:34 144.38.199.50 syslog-ng[6547]: syslog-ng starting up; version='3.5.6'
Jan  7 10:18:34 144.38.199.50 sudo: pam_unix(sudo:session): session closed for user root
Jan  7 10:19:13 144.38.199.50 joe: this command sends and entry to the syslog file
Jan  7 10:19:26 144.38.199.50 sudo:      joe : TTY=pts/0 ; PWD=/etc/syslog-ng ; USER=root
; COMMAND=/usr/bin/tail -n1 /var/log/syslog
Jan  7 10:19:26 144.38.199.50 sudo: pam_unix(sudo:session): session opened for user root b
y joe(uid=0)
Jan  7 10:19:26 144.38.199.50 sudo: pam_unix(sudo:session): session closed for user root
joe@logger:/etc/syslog-ng$ echo "it appears to work!, yay"
-bash: !,: event not found
joe@logger:/etc/syslog-ng$ echo "Well, it's there"
Well, it's there
joe@logger:/etc/syslog-ng$ 
```