joe@ns1:~$ echo "Here is the client I want to send logs from"
Here is the client I want to send logs from
joe@ns1:~$ sudo apt install syslog-ng syslog-ng-core
Create our config file for the client

Create our config file for the client

Create our config file for the client
# First to configure the destination address and port

# destination IS a keyword, loghost is NOT

destination loghost { udp("144.38.201.39" port(514)); };
# First to configure the destination address and port

# destination IS a keyword, loghost is NOT

destination loghost { udp("144.38.201.39" port(514)); }; 

# note that s_src is defined in the global options

log { source(s_src); destination(loghost); };
joe@ns1:/etc/syslog-ng/conf.d$ ls
joe@ns1:/etc/syslog-ng/conf.d$ echo "Create our config file for the client"
Create our config file for the client
joe@ns1:/etc/syslog-ng/conf.d$ sudo vi client.conf
joe@ns1:/etc/syslog-ng/conf.d$ sudo service syslog-ng restart
joe@ns1:/etc/syslog-ng/conf.d$
joe@ns1:/etc/syslog-ng/conf.d$ logger "This command sends and entry to the syslog file"

joe@ns1:/etc/syslog-ng/conf.d$ tail -n1 /var/log/syslog
Jan 9 14:48:57 ns1 joe: This command sends and entry to the syslog file

joe@ns1:/etc/syslog-ng/conf.d$ echo "Told you!"
Told you!

joe@ns1:/etc/syslog-ng/conf.d$
We should also see a similar entry back on our logging server if everything is working correctly.
joe@logger:~$ ls /var/log/
alternatives.log  btmp           dpkg.log  kern.log  ns1
apt             cron.log         faillog    lastlog    syslog
auth.log        dist-upgrade     fsck       lxd        unattended-upgrades
bootstrap.log   dmesg           installer  messages  wtmp
joe@logger:~$ echo "Yay, it created the ns1 directory for us"
Yay, it created the ns1 directory for us
joe@logger:~$
joe@logger:/var/log/ns1$ ls
2018-01-09.ns1.log

joe@logger:/var/log/ns1$ cat 2018-01-09.ns1.log
Jan  9 14:49:41 144.38.201.34 syslog-ng[13410]: Syslog connection broken; fd='17', server='AF_INET(144.38.201.39:514)', time_reopen='60'
Jan  9 14:50:37 144.38.201.34 joe: This command sends and entry to the syslog file
Jan  9 14:50:41 144.38.201.34 syslog-ng[13410]: Syslog connection established; fd='16', server='AF_INET(144.38.201.39:514)', local='AF_INET(0.0.0.0:0)'

joe@logger:/var/log/ns1$
joe@logger:/var/log/ns1$ echo "Awesome, it works!"
Awesome, it works!
joe@logger:/var/log/ns1$