Install the packages necessary for the server to receive logs
joe@logger:~$ sudo apt install syslog-ng syslog-ng-core
joe@logger:~$ cd /etc/syslog-ng/
joe@logger:/etc/syslog-ng$ ls
conf.d  patterndb.d  scl.conf  syslog-ng.conf
joe@logger:/etc/syslog-ng$ echo "Can change settings in the conf file"
Can change settings in the conf file
joe@logger:/etc/syslog-ng$
joe@logger:/etc/syslog-ng$ ls
conf.d patterndb.d scl.conf syslog-ng.conf
joe@logger:/etc/syslog-ng$ cd conf.d/
joe@logger:/etc/syslog-ng/conf.d$ echo "We will make our own configuration file for machines we want to capture logs from in this directory"
We will make our own configuration file for machines we want to capture logs from in this directory
joe@logger:/etc/syslog-ng/conf.d$
The following file, you will have to type in

joe@logger:/etc/syslog-ng/conf.d$ echo "The following file, you will have to type in"

joe@logger:/etc/syslog-ng/conf.d$ sudo vi ns1.mojojojo.ml.conf
# ns1.mojojojo.ml syslog-ng config file

# First we will override some options from the global file

options {
    create_dirs(yes);
    owner(root);
    group(root);
    perm(0664);
    dir_owner(root);
    dir_group(root);
    dir_perm(0755);
};
# First we will override some options from the global file

options {
    create_dirs(yes);
    owner(root);
    groupt(root);
    perm(0664);
    dir_owner(root);
    dir_group(root);
    dir_perm(0755);
};

# apply a filter
# Since our 'logger' machine is going to receive log streams from multiple hosts
# We need to filter out which stream this config file applies to
# filter is a reserved word f_ns1 is not
filter f_ns1 {
    host("144.38.201.34");
}

"ns1.mojojojo.ml.conf" 22L, 475C written
create_dirs(yes);
owner(root);
group(root);
perm(0664);
dir_owner(root);
dir_group(root);
dir_perm(0755);

# apply a filter
# Since our 'logger' machine is going to receive log streams from multiple hosts
# We need to filter out which stream this config file applies to
# filter is a reserved word f_ns1 is not
filter f_ns1 {
    host("144.38.201.34");
};

# Specify the output file
# Where do we want this log stream written to?
# destination is a reserved word, d_ns1 is not
destination d_ns1 {
    file("/var/log/ns1/$YEAR-$MONTH-$DAY.ns1.log");
};

"ns1.mojojojo.ml.conf" 29L, 668C written
# apply a filter
# Since our 'logger' machine is going to receive log streams from multiple hosts
# We need to filter out which stream this config file applies to
# filter is a reserved word, f_ns1 is not
filter f_ns1 {
    host("144.38.201.34");
};

# Specify the output file
# Where do we want this log stream written to?
# destination is a reserved word, d_ns1 is not
destination d_ns1 {
    file("/var/log/ns1/$YEAR-$MONTH-$DAY.ns1.log");
};

# Now put all the magic together
log {
    source(s_udp);
    filter(f_ns1);
    destination(d_ns1);
};
There is one more thing we have to do. If you noticed that s_udp line, you may wonder where it came from.

we must add it. I could have added it to that file, but since the source will be the same from various hosts, let's put it in the global config file.
sudo vi ../conf.d/patterns.conf
scl.conf syslog-ng.conf

sudo vi ../syslog-ng.conf
bad_hostname("^gconfd$";)

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

source s_udp {
    udp(port(514));
};

# 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" 167L, 6007C written

25,21
6%
Note that if it doesn't run, it may be hard to find your error. Try to run syslog-ng in the foreground like this:

```
$ syslog-ng
```

syslog-ng: Error setting capabilities, capability management disabled; error='Operation not permitted'
Error creating persistent state file; filename='/var/lib/syslog-ng/syslog-ng.persist-', error='Permission denied (13)'

```
joe@logger:/etc/syslog-ng/conf.d$ echo "But do it with sudo... you may be able to see where you have problems or missed a semicolon"

But do it with sudo... you may be able to see where you have problems or missed a semicolon

joe@logger:/etc/syslog-ng/conf.d$