joe@logger:~$ sudo apt install syslog-ng syslog-ng-core
cd /etc/syslog-ng/
ls

echo "Change settings in the conf file"

Change settings in the conf file
We will create a config file for a machine that we would like to gather logs for.
# My config file to configure logs coming from ns1.thegummibear.com
# Anything put in the options section will override defaults

options {

    create_dirs(yes);
    owner(root);
    group(root);
    perm(0664);
    dir_owner(root);
    dir_group(root);
    dir_perm(0755);
}

# My config file to configure logs coming from ns1.thegummibear.com
# Anything put in the options section will override defaults

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

# Now to apply a filter
# The logger machine will receive logs from multiple hosts
# We need to filter out the stream that this config file applies to
# filter is a reserved word f_ns1 is not

filter f_ns1 {
    host("144.38.199.50");  # this is the ip of the ns1 machine
};
create_dirs(yes);
owner(root);
group(root);
perm(0664);
dir_owner(root);
dir_group(root);
dir_perm(0755);

#
# Now to apply a filter
# The logger machine will receive logs from multiple hosts
# We need to filter out the stream that this config file applies to
# filter is a reserved word f_ns1 is not

filter f_ns1 {
    host("144.38.199.50");  #this is the ip of the ns1 machine
};

#
# Specify the output file
# This will control where the file is written to
# destination is a reserved word, d_ns1 is not
destination d_ns1 {
    file("/var/log/ns1/$YEAR-$MONTH-$DAY.ns1.log");
};
group(root);
perm(0664);
dir_owner(root);
dir_group(root);
dir_perm(0755);

# Now to apply a filter
# The logger machine will receive logs from multiple hosts
# We need to filter out the stream that this config file applies to
# filter is a reserved word f_ns1 is not

filter f_ns1 {
  host("144.38.199.50");  # this is the ip of the ns1 machine
}

# Specify the output file
# This will control where the file is written to
# destination is a reserved word, d_ns1 is not
destination d_ns1 {
  file("/var/log/ns1/$YEAR-$MONTH-$DAY.ns1.log");
}

# finally the next lines will put everything together
log {
  source(s_udp);  # s_udp is defined in global file
  filter(f_ns1);
  destination(d_ns1);
}

"ns1.thegummibear.com.conf" 36L, 874C written
joe@logger:/etc/syslog-ng/conf.d$ ls
ns1.thegummibear.com.conf
joe@logger:/etc/syslog-ng/conf.d$ cd ..
joe@logger:/etc/syslog-ng$ ls
conf.d patterndb.d scl.conf syslog-ng.conf
joe@logger:/etc/syslog-ng$  

Let's verify that s_udp exists. We may have to create it.
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();
};

I guess only the system and internal sources were specified
I will add the udp source here

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)); }

Destinations

First some standard logfile

destination d_auth { file("/var/log/auth.log"); };
"syslog-ng.conf" 168L, 6043C written
Let's try running syslog-ng in the foreground.

```
root@desdemona:~ $ echo "Lets try running syslog-ng in the foreground"

root@desdemona:~ $ sudo syslog-ng

root@desdemona:~ $ ps aux | grep syslog
```

```
message+  382  0.0  0.9  50064  4440 ?  Ss  Jan03  0:00 /usr/bin/dbus-daemon --systemd --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root    12383  0.0  2.0  277492 10200 ?  Ss  09:57  0:00 /usr/sbin/syslog-ng -F
root    12486  0.0  0.1  48936   532 ?  Ss  10:09  0:00 supervising syslog-ng
root    12487  0.0  1.9  286072  9428 ?  Ss  10:09  0:00 syslog-ng
joe    12494  0.0  0.2  14428 1032 pts/0  S+  10:09  0:00 grep --color=auto syslog

joe@desdemona:~ $ echo "looks like it is running"

looks like it is running
```