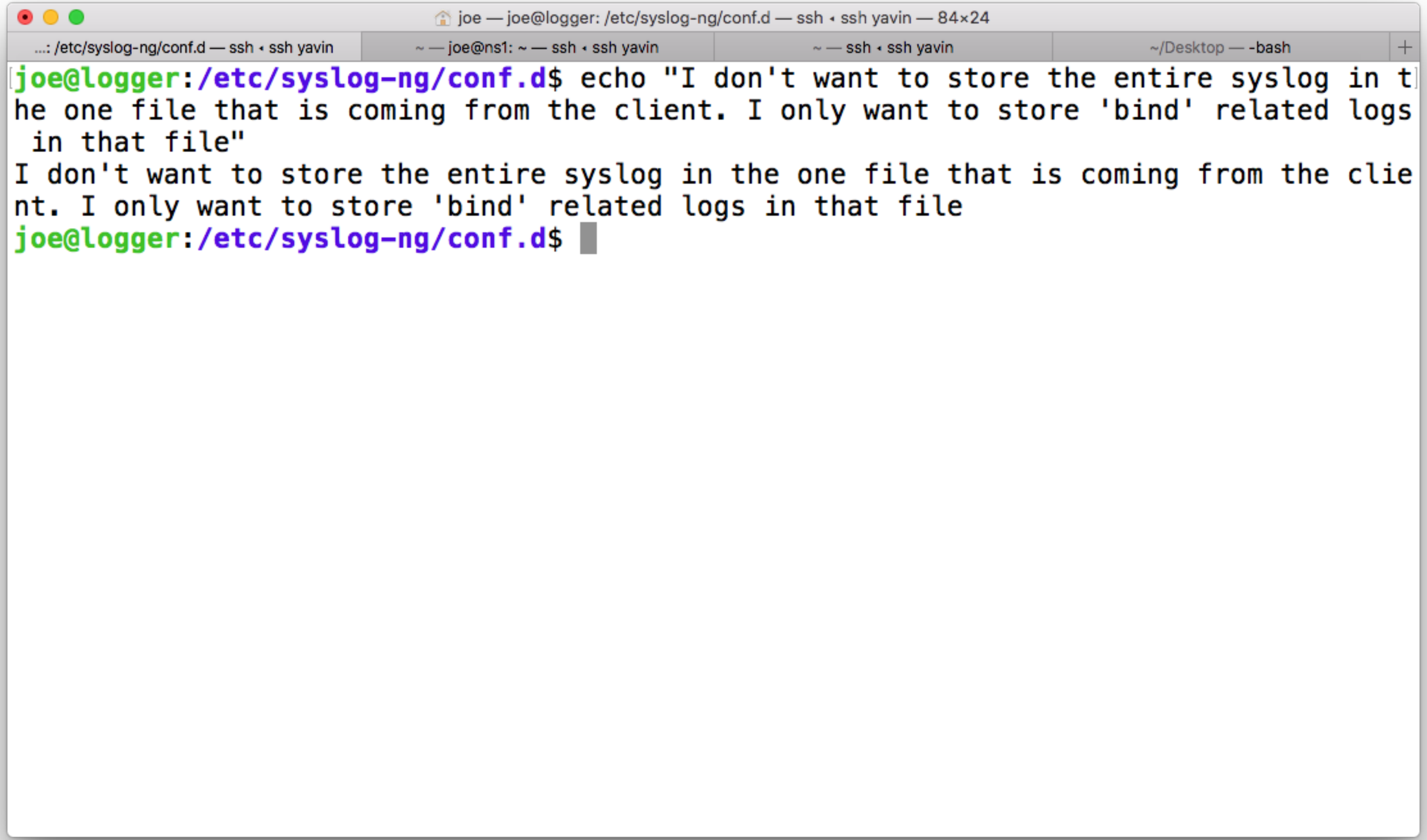

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24
...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin
~ — joe@ns1: ~ — ssh ◂ ssh yavin
~ — ssh ◂ ssh yavin
~/Desktop — -bash
joe@logger:/etc/syslog-ng/conf.d$ echo "I don't want to store the entire syslog in t
he one file that is coming from the client. I only want to store 'bind' related logs
 in that file"
I don't want to store the entire syslog in the one file that is coming from the clie
nt. I only want to store 'bind' related logs in that file
joe@logger:/etc/syslog-ng/conf.d$

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
joe@logger:/etc/syslog-ng/conf.d$ ls
ns1.mojojojo.ml.conf
joe@logger:/etc/syslog-ng/conf.d$ sudo vi ns1.mojojojo.ml.conf
```

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
};

#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

# Im changing my filter!!!
# if it matches the ip and has the string named in it.
filter f_ns1 {
        host("144.38.201.34") and match("named");
};

# Specify the output file
# Where do we want this log stream written to?
# destination is a reserved word, d_ns1 is not

#note I changed my filename too
destination d_ns1 {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.bind.log");
};

# Now put all the magic together
"ns1.mojojojo.ml.conf" 41L, 899C written                      30,31         66%
```

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

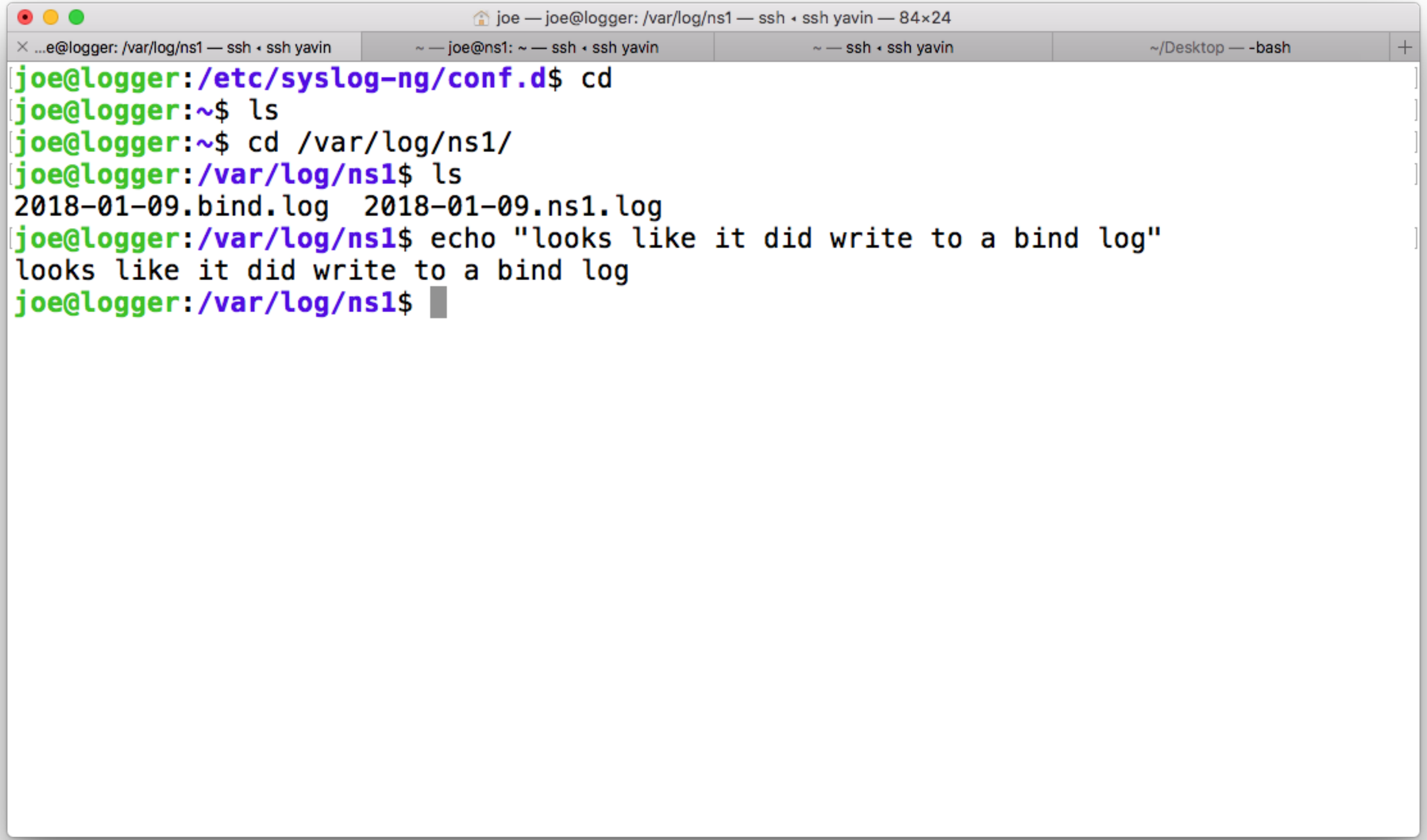
...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
joe@logger:/etc/syslog-ng/conf.d$ sudo service syslog-ng restart
joe@logger:/etc/syslog-ng/conf.d$
```

joe — joe@ns1: ~ — ssh ‹ ssh yavin — 84×24

...: /etc/syslog-ng/conf.d — ssh ‹ ssh yavin | ~ — joe@ns1: ~ — ssh ‹ ssh yavin | ~ — ssh ‹ ssh yavin | ~/Desktop — -bash

```
joe@ns1:~$ echo "Lets see if it works"
Lets see if it works
joe@ns1:~$ sudo service bind9 restart
joe@ns1:~$
```


joe — joe@logger: /var/log/ns1 — ssh ◂ ssh yavin — 84×24
...e@logger: /var/log/ns1 — ssh ◂ ssh yavin
~ — joe@ns1: ~ — ssh ◂ ssh yavin
~ — ssh ◂ ssh yavin
~/Desktop — -bash
joe@logger:/etc/syslog-ng/conf.d$ cd
joe@logger:~$ ls
joe@logger:~$ cd /var/log/ns1/
joe@logger:/var/log/ns1$ ls
2018-01-09.bind.log 2018-01-09.ns1.log
joe@logger:/var/log/ns1$ echo "looks like it did write to a bind log"
looks like it did write to a bind log
joe@logger:/var/log/ns1$

joe — joe@logger: /var/log/ns1 — ssh ◂ ssh yavin — 84×24

...e@logger: /var/log/ns1 — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
Jan  9 14:59:24 144.38.201.34 named[13477]: automatic empty zone: EMPTY.AS112.ARPA
Jan  9 14:59:24 144.38.201.34 named[13477]: configuring command channel from '/etc/b
ind/rndc.key'
Jan  9 14:59:24 144.38.201.34 named[13477]: command channel listening on 127.0.0.1#9
53
Jan  9 14:59:24 144.38.201.34 named[13477]: configuring command channel from '/etc/b
ind/rndc.key'
Jan  9 14:59:24 144.38.201.34 named[13477]: command channel listening on ::1#953
Jan  9 14:59:24 144.38.201.34 named[13477]: managed-keys-zone: journal file is out o
f date: removing journal file
Jan  9 14:59:24 144.38.201.34 named[13477]: managed-keys-zone: loaded serial 6
Jan  9 14:59:24 144.38.201.34 named[13477]: zone 0.in-addr.arpa/IN: loaded serial 1
Jan  9 14:59:24 144.38.201.34 named[13477]: zone 127.in-addr.arpa/IN: loaded serial
1
Jan  9 14:59:24 144.38.201.34 named[13477]: zone 255.in-addr.arpa/IN: loaded serial
1
Jan  9 14:59:24 144.38.201.34 named[13477]: zone localhost/IN: loaded serial 2
Jan  9 14:59:24 144.38.201.34 named[13477]: zone mojojojo.ml/IN: loaded serial 20180
10903
Jan  9 14:59:24 144.38.201.34 named[13477]: all zones loaded
Jan  9 14:59:24 144.38.201.34 named[13477]: running
Jan  9 14:59:24 144.38.201.34 named[13477]: zone mojojojo.ml/IN: sending notifies (s
erial 2018010903)
(END)
```

joe — joe@logger: /var/log/ns1 — ssh ◂ ssh yavin — 84×24

...e@logger: /var/log/ns1 — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
joe@logger:/var/log/ns1$ echo "Looks like it only had bind related stuff in it"
Looks like it only had bind related stuff in it
joe@logger:/var/log/ns1$
```

joe — joe@logger: /var/log/ns1 — ssh ◂ ssh yavin — 84×24

...e@logger: /var/log/ns1 — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
joe@logger:/var/log/ns1$ echo "Im going to create a few more filters and destination
s"
Im going to create a few more filters and destinations
joe@logger:/var/log/ns1$
```

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
filter f_ns1 {
        host("144.38.201.34") and match("named");
};

#filters everything that has CRON in it
filter f_ns1_cron {
        host("144.38.201.34") and match("CRON");
};

#filters everything that has serial and mojojojo in it
#maybe I want to log everytime that serial is loaded?
filter f_ns1_serial {
        host("144.38.201.34") and match("serial") and match("mojojojo");
};

# Specify the output file
# Where do we want this log stream written to?
# destination is a reserved word, d_ns1 is not

#note I changed my filename too
destination d_ns1 {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.bind.log");
};
```

22,14 44%

```
#maybe I want to log everytime that serial is loaded?
filter f_ns1_serial {
        host("144.38.201.34") and match("serial") and match("mojojojo");
};

# Specify the output file
# Where do we want this log stream written to?
# destination is a reserved word, d_ns1 is not

#note I changed my filename too
destination d_ns1 {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.bind.log");
};
destination d_ns1_cron {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.cron.log");
};
destination d_ns1_serial {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.serial.log");
};

# Now put all the magic together
log {
                                                          51,0-1        65%
```

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

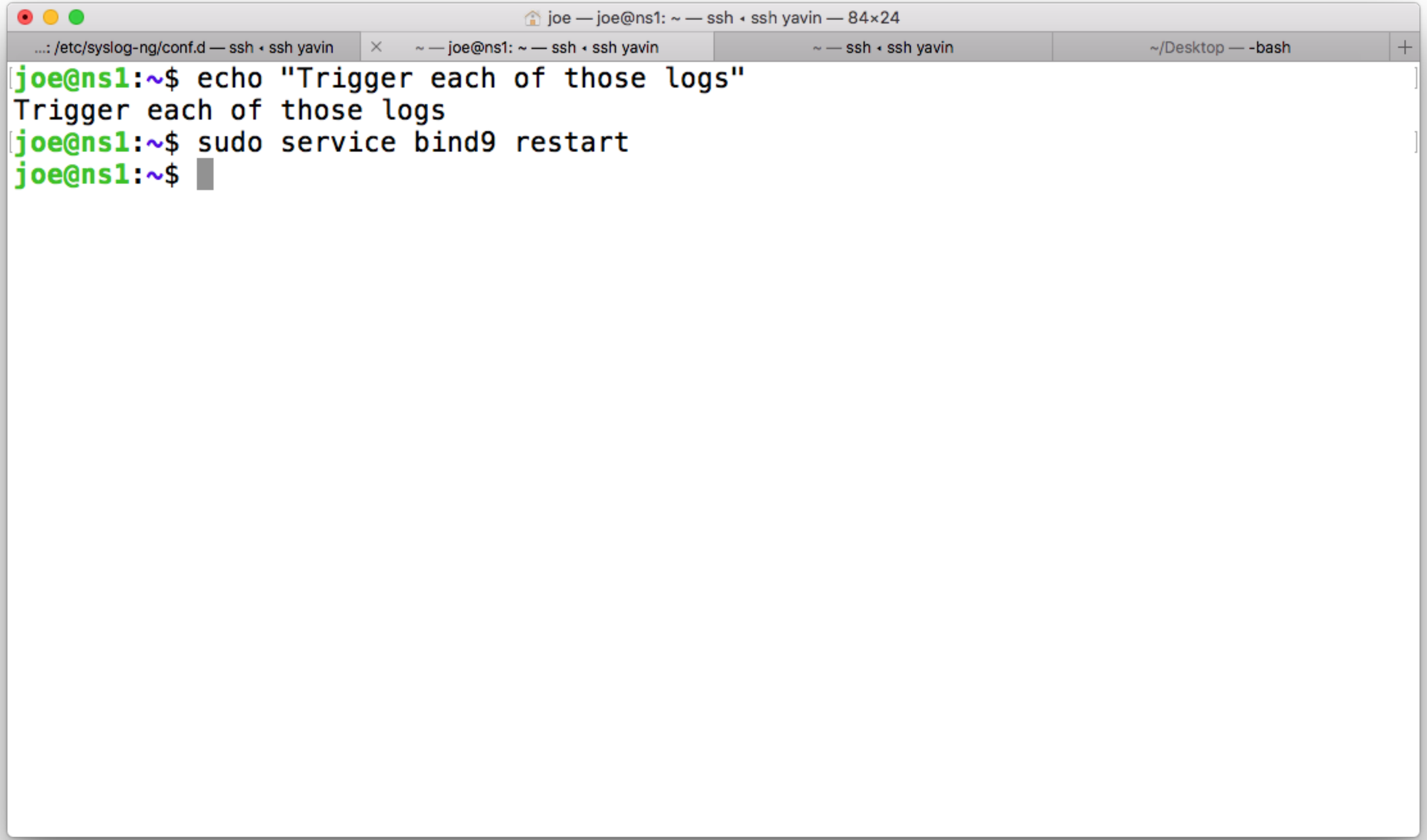
...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

```
destination d_ns1_serial {
        file("/var/log/ns1/$YEAR-$MONTH-$DAY.serial.log");
};


# Now put all the magic together
log {
        source(s_udp);
        filter(f_ns1_cron);
        destination(d_ns1_cron);
};

log {
        source(s_udp);
        filter(f_ns1_serial);
        destination(d_ns1_serial);
};

log {
        source(s_udp);
        filter(f_ns1);
        destination(d_ns1);
};
                                                              70,1          Bot
```

joe — joe@logger: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin — 84×24

…: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin | ~ — joe@ns1: ~ — ssh ◂ ssh yavin | ~ — ssh ◂ ssh yavin | ~/Desktop — -bash

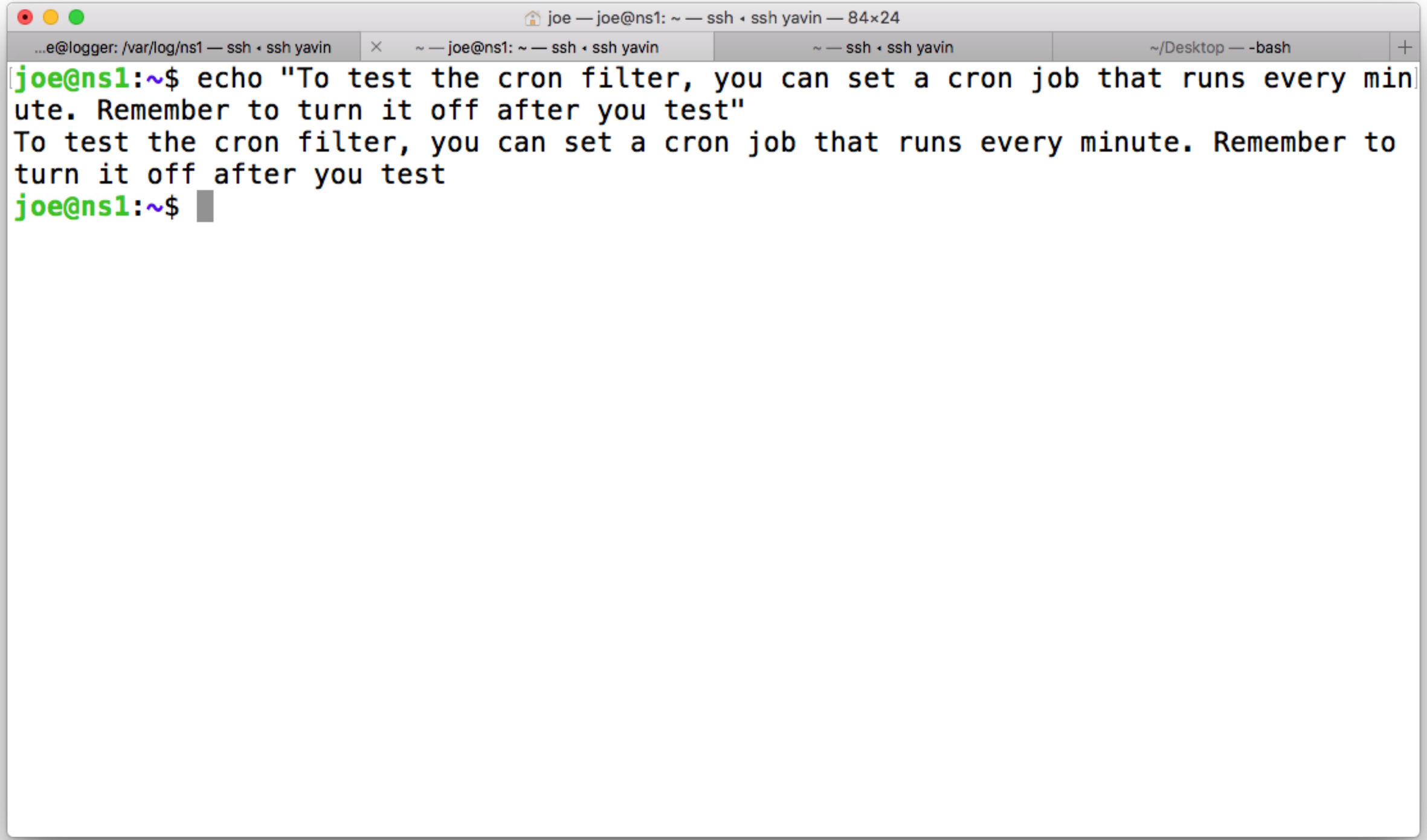
```
joe@logger:/etc/syslog-ng/conf.d$ ls
ns1.mojojojo.ml.conf
joe@logger:/etc/syslog-ng/conf.d$ sudo vi ns1.mojojojo.ml.conf
joe@logger:/etc/syslog-ng/conf.d$ !?restart
sudo service syslog-ng restart
joe@logger:/etc/syslog-ng/conf.d$
```


joe — joe@ns1: ~ — ssh ◂ ssh yavin — 84×24
...: /etc/syslog-ng/conf.d — ssh ◂ ssh yavin
~ — joe@ns1: ~ — ssh ◂ ssh yavin
~ — ssh ◂ ssh yavin
~/Desktop — -bash
joe@ns1:~$ echo "Trigger each of those logs"
Trigger each of those logs
joe@ns1:~$ sudo service bind9 restart
joe@ns1:~$

joe — joe@logger: /var/log/ns1 — ssh ‹ ssh yavin — 84×24

...e@logger: /var/log/ns1 — ssh ‹ ssh yavin | ~ — joe@ns1: ~ — ssh ‹ ssh yavin | ~ — ssh ‹ ssh yavin | ~/Desktop — -bash

```
joe@logger:/etc/syslog-ng/conf.d$ cd
joe@logger:~$ ls
joe@logger:~$ cd /var/log/ns1/
joe@logger:/var/log/ns1$ ls
2018-01-09.bind.log  2018-01-09.ns1.log  2018-01-09.serial.log
joe@logger:/var/log/ns1$ less 2018-01-09.serial.log
joe@logger:/var/log/ns1$
joe@logger:/var/log/ns1$
joe@logger:/var/log/ns1$
joe@logger:/var/log/ns1$ ls
2018-01-09.bind.log  2018-01-09.cron.log  2018-01-09.ns1.log  2018-01-09.serial.log
joe@logger:/var/log/ns1$
```


joe — joe@ns1: ~ — ssh ◂ ssh yavin — 84×24
...e@logger: /var/log/ns1 — ssh ◂ ssh yavin
~ — joe@ns1: ~ — ssh ◂ ssh yavin
~ — ssh ◂ ssh yavin
~/Desktop — -bash
joe@ns1:~$ echo "To test the cron filter, you can set a cron job that runs every minute. Remember to turn it off after you test"
To test the cron filter, you can set a cron job that runs every minute. Remember to turn it off after you test
joe@ns1:~$