Configuring the sending of logs on Debian/Ubuntu

To centralise logs to a log server (port 514 UDP or TCP). Simply edit the “/etc/rsyslog.conf” file

copy

```
nano /etc/rsyslog.conf
```

At the end of the file you can add this line:

copy

```
*.*     @<ip>:514
```

This will redirect all the logs from your server to the syslog server. This is likely to do a lot because the debug and info levels are captured by the star.

You can specify the levels that interest you by modifying our line with this:

copy

```
*.notice,warn,err,crit,alert,emerg    @<ip>:514
```

The server will only send logs greater than or equal to the notice level. After each modification, the service must be restarted

copy

```
/etc/init.d/rsyslog restart
```

You can test logging with the following commands:

copy

```
logger -p auth.info "test link to syslog server. lvl info"
logger -p auth.crit "test link to syslog server. lvl crit"
```

The 2 command lines will generate 2 entries: one at “info” level and the other at critical level