

Rsyslog+ssl

```
openssl genrsa 2048 > ca-key.pem  
openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca-cert.pem
```

```
openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out server-req.pem  
openssl rsa -in server-key.pem -out server-key.pem  
openssl x509 -req -in server-req.pem -days 3600 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out server-cert.pem
```

.pem */etc/ssl/certs*

/etc/rsyslog.conf (*!*)

```
$DefaultNetstreamDriver gtls  
$DefaultNetstreamDriverCAFile /etc/ssl/certs/ca-cert.pem  
$DefaultNetstreamDriverCertFile /etc/ssl/certs/server-cert.pem  
$DefaultNetstreamDriverKeyFile /etc/ssl/certs/server-key.pem  
$ModLoad imtcp  
$InputTCPServerStreamDriverMode 1  
$InputTCPServerStreamDriverAuthMode anon  
$InputTCPServerRun 514
```

rsyslog

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

ca-cert.pem */etc/ssl/certs*

rsyslog-gnutls

```
apt-get install rsyslog-gnutls
```

/etc/rsyslog.conf (*!*)

```
$DefaultNetstreamDriverCAFile /etc/ssl/certs/ca-cert.pem  
$DefaultNetstreamDriver gtls  
$ActionSendStreamDriverMode 1  
$ActionSendStreamDriverAuthMode anon  
*. * @@192.168.1.1
```

(192.168.1.1 —)

rsyslog

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

```
tcpdump
```

```
apt-get install tcpdump
```

```
tcpdump -A > tcp.txt
```

```
sudo login test
```

```
exit
```

```
grep test tcp.txt
```