

 **ONE IDENTITY™**

Syslog-ng 101, part 7: Networking

Peter Czanik

RFC3164

```
<123>Aug  1 10:28:22 host syslog-ng[12446]: syslog-ng  
starting up; version='4.0.1'
```

- Three parts: <PRI>HEADERS MESSAGE
- PRI=8*Facility+Severity
- HEADERS: timestamp, hostname, process and process ID
e.g.,
Aug 1 10:28:22 host syslog-ng[12446]:
- MSG: the log message itself
 - For example: syslog-ng starting up; version='4.0.1'

RFC5424

- Well standardized format right from the beginning
- Can forward name-value pairs
- Not widely used
- More often: RFC3164 header + JSON message

Modes of operation

- Client mode: collecting logs from the client and sending them to the remote server (directly or through a relay)
- Relay mode: collecting logs from the clients (through the network) and sending them to the remote server (directly or through another relay)
- Server mode: collecting logs from the clients and storing them locally or in a non-syslog destination

Why relays?

UDP source

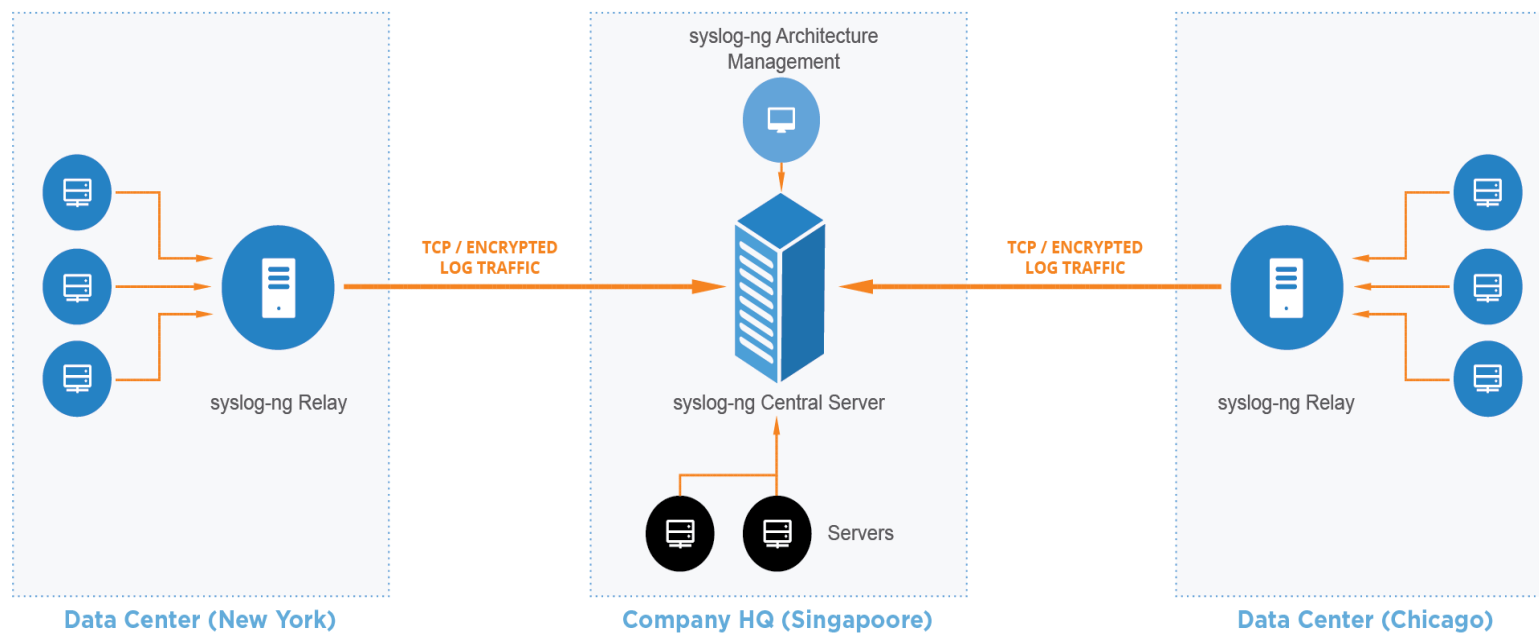
Collect as close as possible

Scalability

Distributing processing

Structure

A relay for each site or department



syslog-ng.conf: netsource.conf

- Simple server: saves incoming logs to a file

```
@version:3.38
```

```
source s_tcp { tcp(port(514)); };
```

```
destination d_file { file("/var/log/fromnet"); };
```

```
log { source(s_tcp); destination(d_file); };
```

Using logger with a network source

- logger can generate network messages
- `logger -T -n 127.0.0.1 -P 514 bla bla bla bla bla`
- Important options
 - -T: TCP
 - -n: hostname or IP
 - -P: port
 - Log message

 **ONE IDENTITY™**