University College

Remote log server with rsyslog

By Per Dahlstrøm

The audience outcome

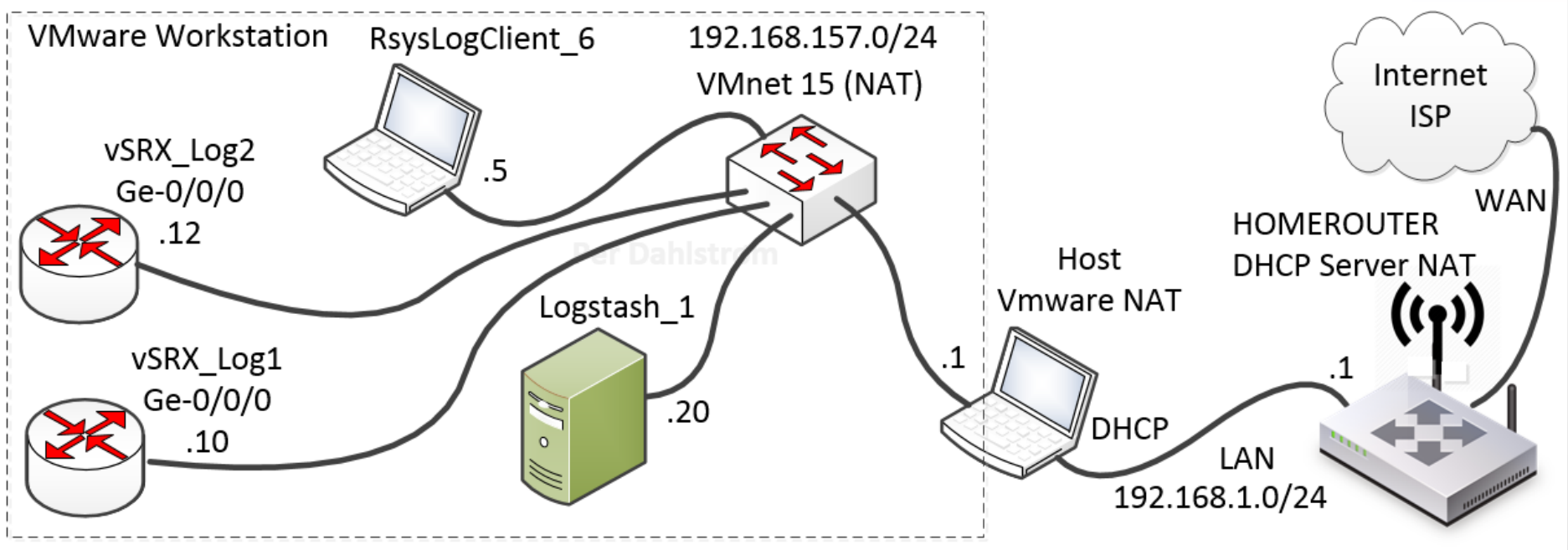
After this presentation the audience should understand:

- What a remote log server is and can do.
- Why we would want to set up a remote log server.
  What the use cases for a remote log server are.
- How to set up a remote log server on Linux.

Audience prerequisites:

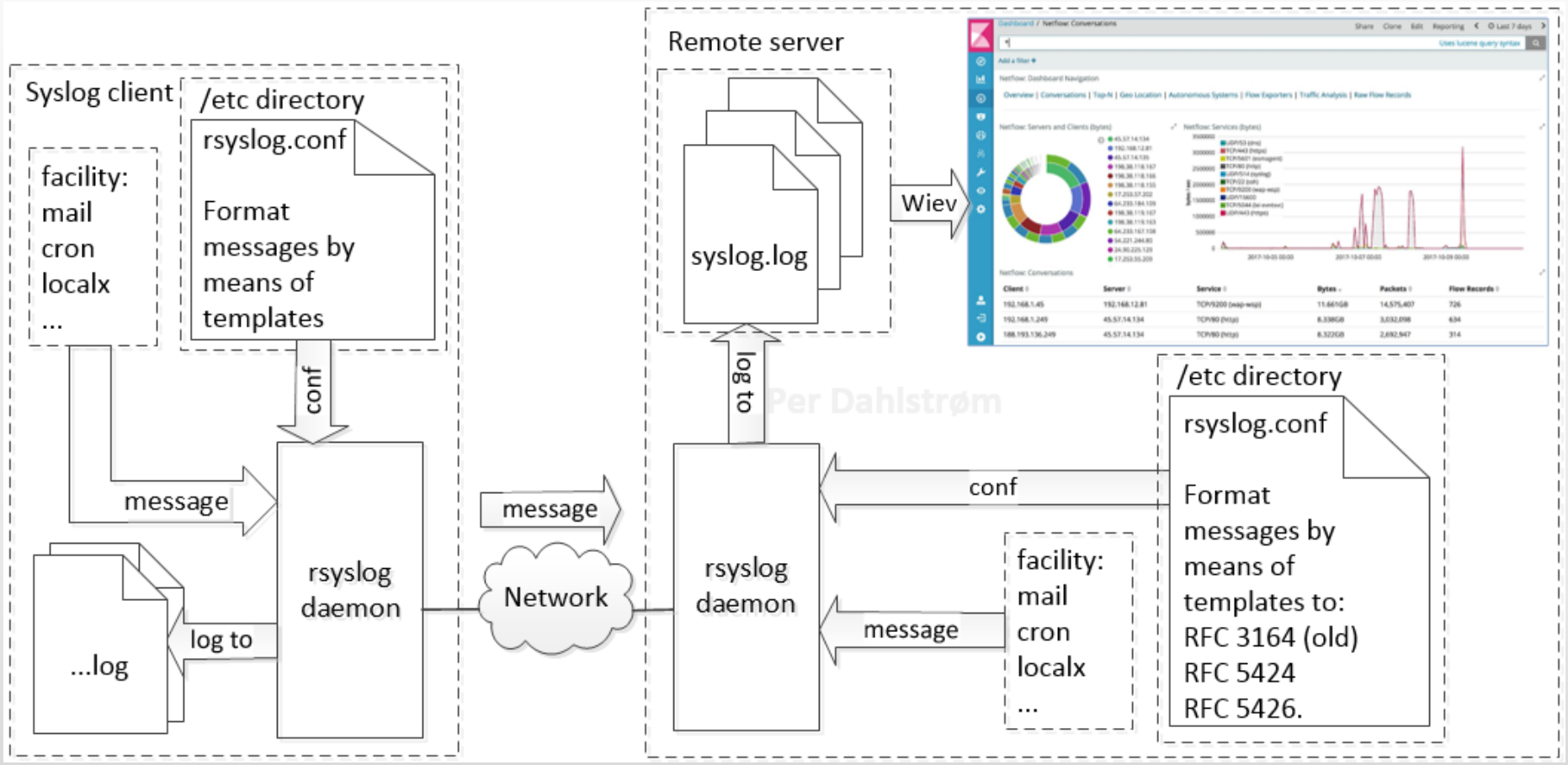
- 150 hours working with Linux.
- Have set up local logging on Linux.
  Have used rsyslog to do the local logging.

Scenario

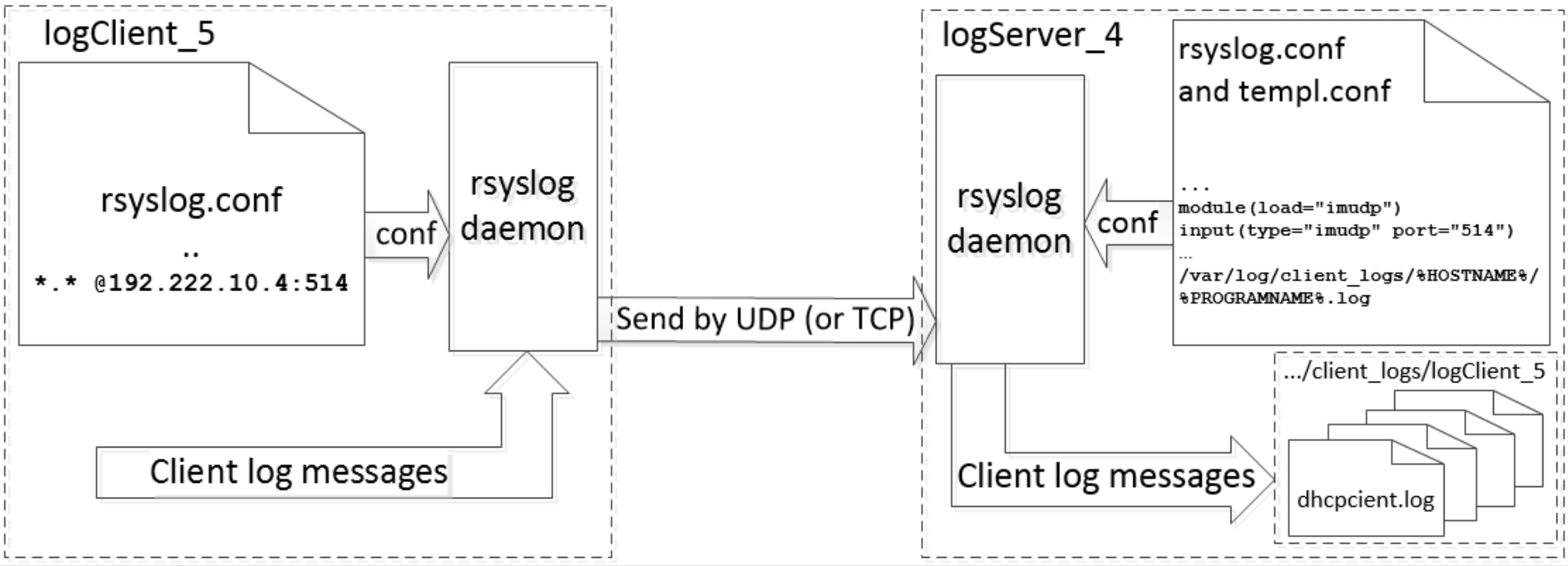

VMware Workstation
RsysLogClient_6
192.168.157.0/24
VMnet 15 (NAT)
.5
vSRX_Log2
Ge-0/0/0
.12
vSRX_Log1
Ge-0/0/0
.10
Logstash_1
.20
.1
Host
Vmware NAT
DHCP
LAN
192.168.1.0/24
.1
HOMEROUTER
DHCP Server NAT
WAN
Internet
ISP

Syslog remote log server overview

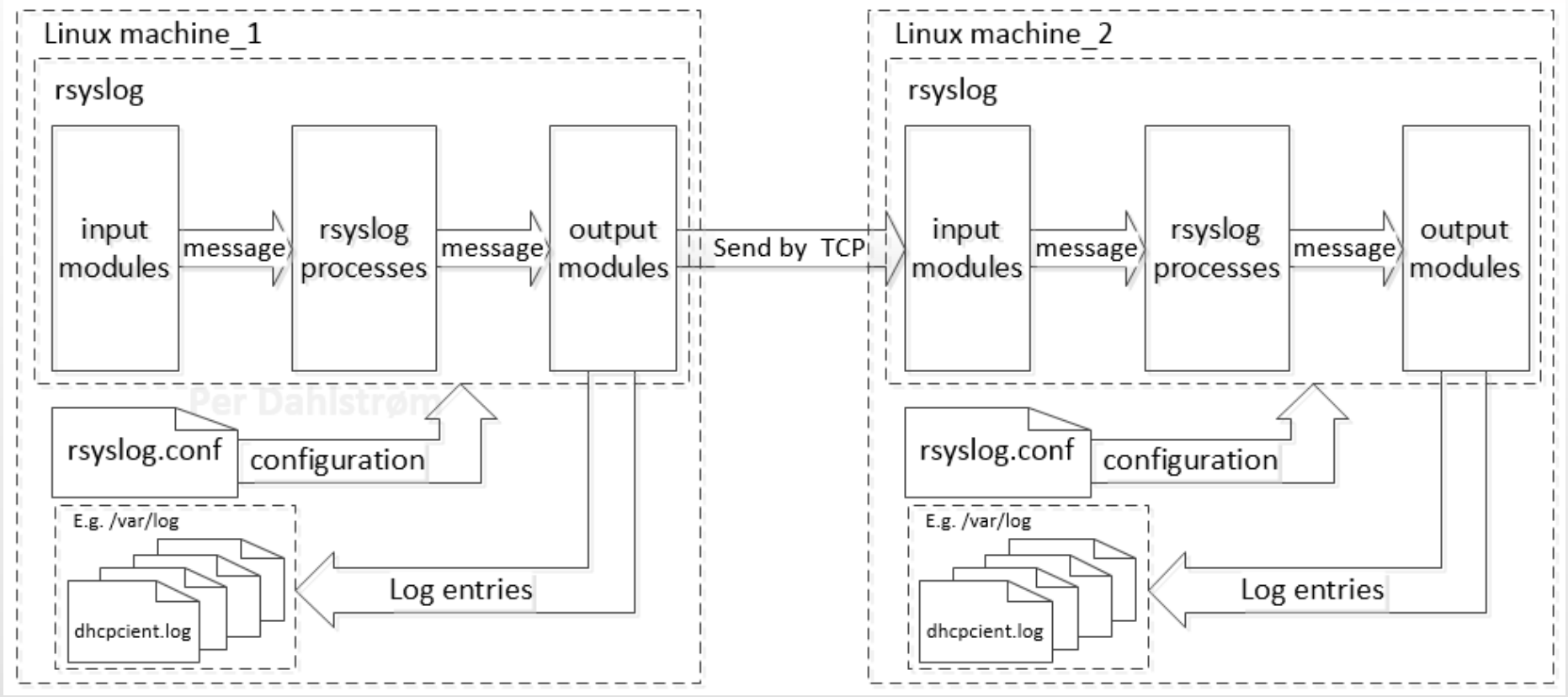
Nagios.
Kibana. ELK stack.



Remote log client and server overview



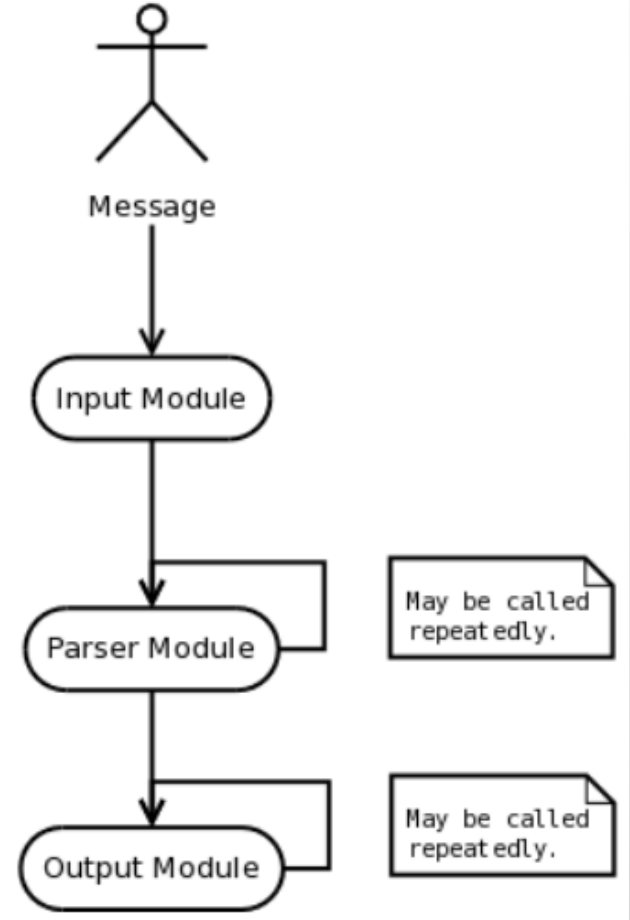
Rsyslog modules



rsyslog modules

There exist different classes of loadable modules:

Output Modules
Input Modules
Parser Modules
Message Modification Modules
String Generator Modules
Library Modules



https://www.rsyslog.com/doc/v8-stable/configuration/modules/workflow.html

rsyslog example output modules

omelasticsearch: Elasticsearch Output Module
omfile: File Output Module
omfwd: syslog Forwarding Output Module
omhdfs: Hadoop Filesystem Output Module
omhiredis: Redis Output Module
omhttpfs: Hadoop HTTPFS Output Module
omjournal: Systemd Journal Output
ommail: Mail Output Module
ommongodb: MongoDB Output Module
ommysql: MySQL Database Output Module
PostgreSQL Database Output Module (ompgsql)
omprog: Program integration Output module
omrelp: RELP Output Module
omsnmp: SNMP Trap Output Module
omstdout: stdout output module (testbench tool)
omudpspoof: UDP spoofing output module
omusrmsg: notify users

http://www.rsyslog.com/doc/v8-stable/configuration/modules/idx_output.html

rsyslog input modules (2018)

im3195: RFC3195 Input Module
imfile: Text File Input Module
imgssapi: GSSAPI Syslog Input Module
imjournal: Systemd Journal Input Module
imkafka: read from Apache Kafka
imklog: Kernel Log Input Module
imkmsg: /dev/kmsg Log Input Module
impstats: Generate Periodic Statistics of Internal Counters
imptcp: Plain TCP Syslog
imrelp: RELP Input Module
imsolaris: Solaris Input Module
imtcp: TCP Syslog Input Module
imudp: UDP Syslog Input Module
imuxsock: Unix Socket Input Module

If you need something not on the list: Write your own module.

http://www.rsyslog.com/doc/v8-stable/configuration/modules/idx_input.html

Set filters and formats in 50-default.conf

Selector	Action
Facility.Priority	What to do with message
`local4.=info`	`/var/log/local4info.log`
`mail.warn`	`@192.222.10.4:514`

@: UDP
@@: TCP

```
# Examples by Per Dahlstrøm
local4.=info     /var/log/local4info.log
mail.warn        /var/log/mail.log
*.*              @@logserver.myDomain:6514 (?)
```

Whenever the rsyslogd daemon receives a logging message, it acts or filters based on the message type (Facility) and a Level (Priority).

rsyslog overview client