Day 2-3-1
logging and monitoring

status of infrastructure

syslog, timestamp,
snmp, visualization, nms

in your network

- traffic/access trend of this month
- packets discarded yesterday
- reason of the recent outage
- person who changed the configuration

... and so on

back traceable

- what's happened in the past
- syslog

  to record messages from software
- snmp

  to monitor resources
- netflow

  to monitor packet flows

syslog messages

```
Nov  9 15:19:14.390 UTC: config[65775]:
   %MGBL-SYS-5-CONFIG_I : Configured
   from console by maz on vty0
   (2001:db8:120:100:e1dd:97f3:fd98:a51f)
```

```
Nov 12 13:53:38 maz sudo:      maz : user
   NOT in sudoers ; TTY=pts/3 ; PWD=/
   home/maz ; USER=root ; COMMAND=/
   bin/bash
```

timestamp

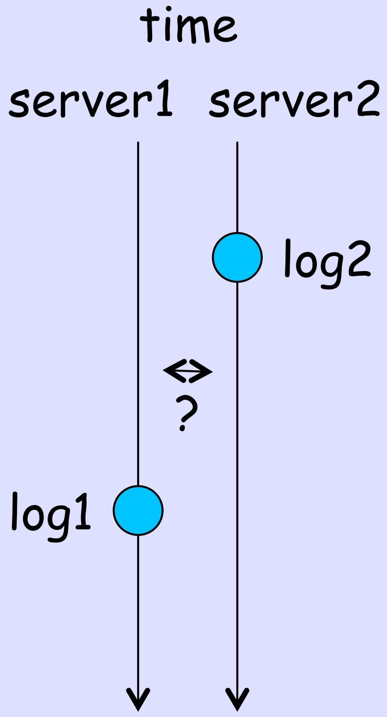
useful if system clock is synchronized

ntp (network time protocol)

- ntpd

timezone

- UTC/GMT is scalable



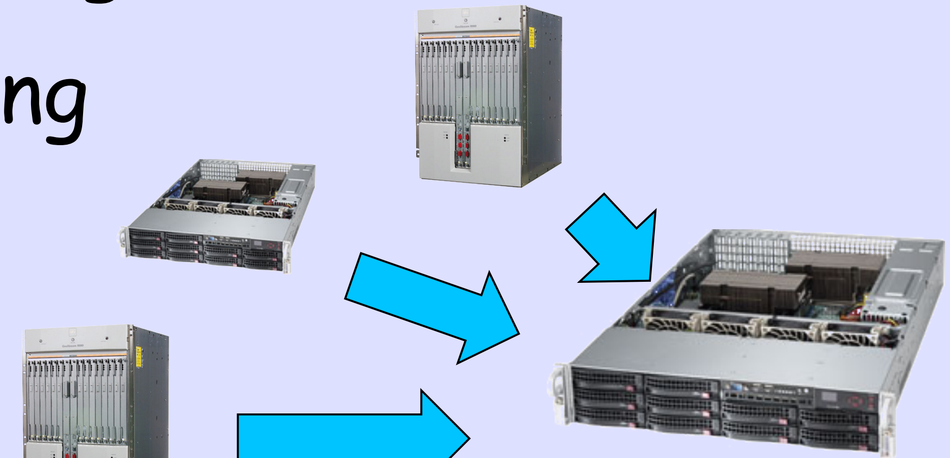
remote logging

log messages could be modified/deleted

- if the system is compromised

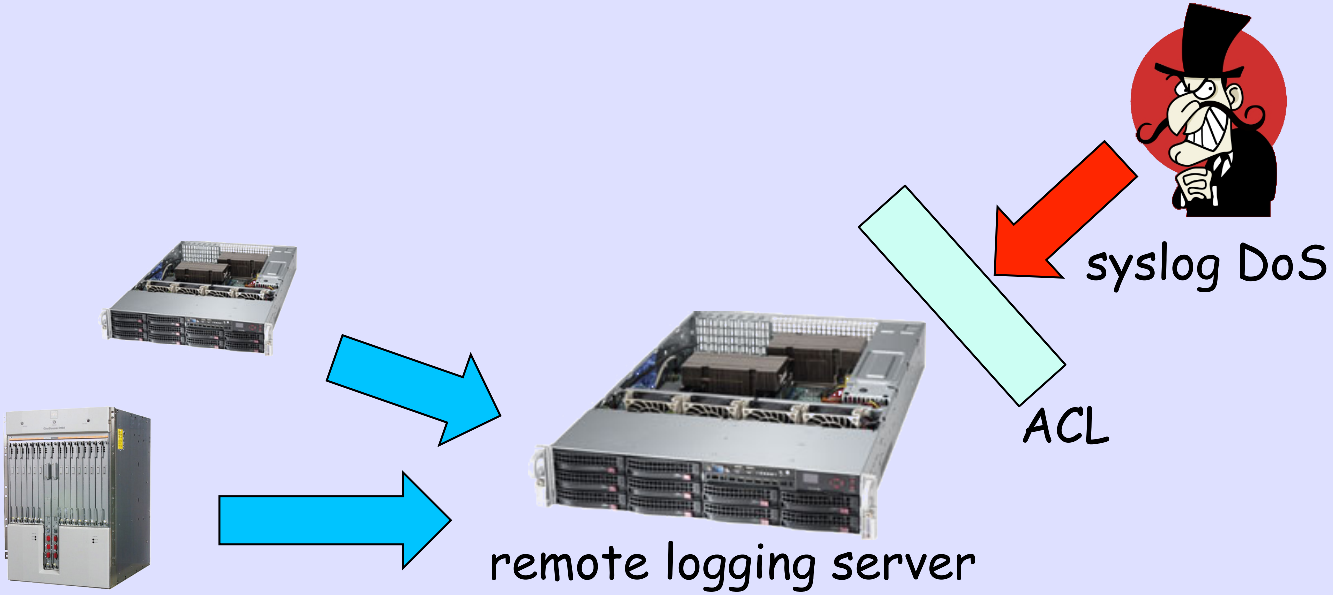
remote logging servers

- receive log messages from other devices
- syslogd/syslog-ng



remote logging server

protecting syslog



syslog DoS

ACL

remote logging server

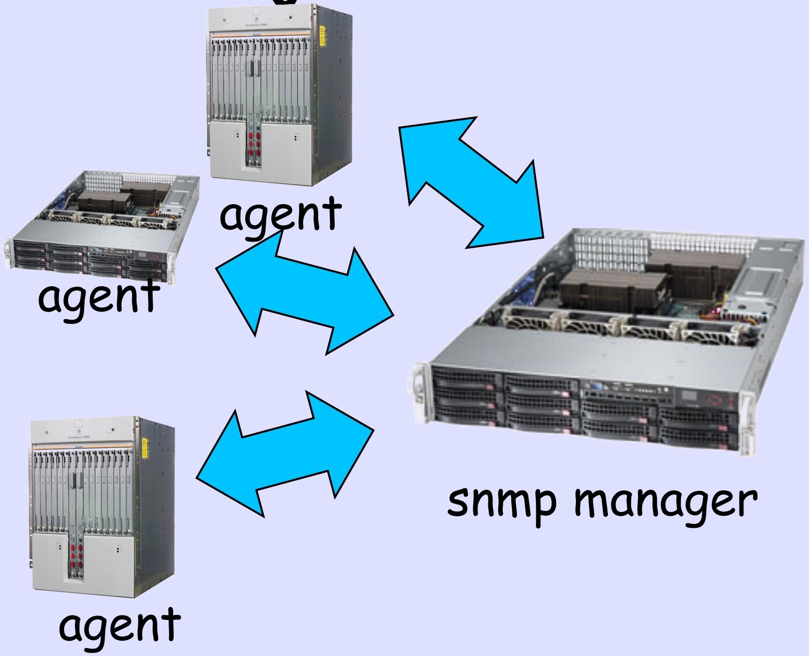
ensure the correctness of log entries

snmp

can read/write information and send a trap

- use version 3, and set password
- prevent 'write' function, or just disable it on agents
- snmp agent/manager

  net-snmp/bsnmpd



snmp MIB

Management information base

- MIB-2, IF-MIB, vender-specific MIB
- you can get information if an agent supports the MIB you want

you can specify the information by OIDs

ifHCinOctets = .1.3.6.1.2.1.31.1.1.1.6

ifHCOutOctets = .1.3.6.1.2.1.31.1.1.1.10

snmp counters

frequency of updating counters

- depends on agents (0-30sec)
- 5min is widely used as snmp polling time

counter overflow

- 32bit counters(ifIn/OutOctets) could wrap in 5.7min at 100Mbps
- consider 64bit counters(ifHCInOctets) for 1Gbps or more interfaces

visualization

helps to understand a trend

- cpu load, disk space, bps, pps, etc
- also helps to convince your boss to upgrade ;)

visualization tools

- MRTG
- RRDtool

Network Monitoring Systems

provide monitoring your devices, and notify you in case of troubles

- even if you are sleeping ☺
- syslog, snmp, ping, service(http, smtp, dns)

many implementations

- Nagios, Cacti, etc.