Imagine a server with the following specs:

- 4 times Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00GHz
- 64GB of ram
- 2 TB HDD disk space
- 2 x 10Gbit/s nics

The server is used for SSL offloading and proxies around 25000 requests per second. Please let us know which metrics are interesting to monitor in that specific case and how would you do that? What are the challenges of monitoring this?

Which Metrics:

- CPU Utilisation
- CPU Load average
- Memory Utilisation
- Disk Utilisation
- Network Traffic
- Network Packets in and out
- Network Packets drops
- CPU Core usage
- Process monitoring

How to do that:

- CPU Utilisation - Can be monitor by using Top/Htop commands
- CPU Load average - Can be monitor by using Top/Htop / uptime commands
- Memory Utilisation - Can be monitor by using Top/Htop / uptime commands
- Disk Utilisation - Can be monitor by using df -kh command
- Network traffic - can be monitoring by Sar tool
- Network Packets in and out - can be monitor be using ifconfig / Sar tool / tcpdump / wireshark
- Network Packets drops - can be monitor be using ifconfig / Sar tool / tcpdump / wireshark
- CPU Core usage - can be monitoring by Sar tool
- Process monitoring - can be monitoring by top / Htop / ps -ef
- All above can be monitor by using monitoring tool like prometheus , Zabbix and etc
- Syslog for OOM killer activity

What are the challenges of monitoring:

- If we use linux commands to monitor, it’s hard to maintain the history of metrics
- With 25000 requests per second it’s hard to analyse the TCP packets in sequence
- It’s makes more difficult to monitor and debug if any UDP requests are there because UDP doesn't have handshake
- Tools like prometheus or Zabbix will use some system resources as well as network resource so we need to have extra resources for these