PERTEMUAN 14 · SUB-CPMK 4.2

Monitoring Kinerja & Manajemen Log

Metrik CPU, memori, disk & jaringan · top/htop · ss · syslog & journalctl

Administrasi Sistem (CEN3303) · D3 Teknik Komputer · Politeknik Negeri Padang
Ir. H. A. Mooduto, M.Kom. · Semester Ganjil 2026/2027

Target hari ini

Sub-CPMK 4.2

Mahasiswa mampu memantau kinerja sistem dan mengelola log untuk mendeteksi anomali operasional.

- Memahami metrik kinerja sistem
- Menggunakan top, htop, ss/netstat
- Mengelola log: syslog & journalctl

Alur pertemuan

1	Mengapa monitoring	10'
2	Metrik & tools	35'
3	Manajemen log	35'
4	Alur troubleshoot & kasus	20'
5	Praktikum lab	170'

Reaktif vs proaktif

Tanpa monitoring



Disk penuh 09:00



Pengguna mengeluh 10:30



Admin mencari 11:00



Pulih 12:30

3,5 jam layanan terganggu

Dengan monitoring



Disk 80% pukul 06:00



Alert ke admin 06:01



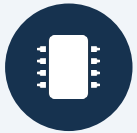
Bersihkan log 06:20



Pengguna tak terdampak

0 menit layanan terganggu

Empat sumber daya yang selalu dipantau



CPU

% pemakaian, load average

Tanda bahaya

Load terus di atas jumlah core

`top · uptime`



Memori

RAM terpakai, swap

Tanda bahaya

Swap terus naik → RAM kurang

`free -h`



Disk

Kapasitas, inode, I/O

Tanda bahaya

Di atas 80–90% → layanan bisa berhenti

`df -h · du`



Jaringan

Bandwidth, koneksi aktif

Tanda bahaya

Lonjakan tak wajar → mungkin serangan

`ss · ip -s link`

01

Membaca kondisi server

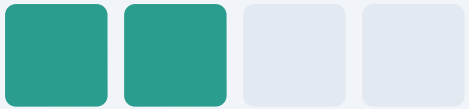
Angka-angka di layar top, free, df, dan ss — dan artinya bagi admin

Load average: antrean kerja CPU

```
$ uptime
 09:41:02 up 12 days,  load average: 3.80, 2.10, 0.95
$ nproc
4
```

1 menit · **5 menit** · **15 menit —** bandingkan dengan jumlah core (nproc). Tren naik dari 0.95 ke 3.80 = beban sedang meningkat.

Load 2 / 4 core



Santai

CPU sering menganggur

Load 4 / 4 core



Penuh

Semua core sibuk, belum antre

Load 8 / 4 core



+4 antre

Kewalahan

Separuh pekerjaan menunggu giliran

Membaca layar top / htop

```
top - 09:41:02 up 12 days,  load average: 3.80, 2.10, 0.95
Tasks: 142 total,   3 running, 139 sleeping,   0 zombie
%Cpu(s): 62.0 us,  8.1 sy,  0.0 ni, 4.5 id, 25.4 wa
MiB Mem :  3936.0 total,  210.4 free,  2984.1 used
MiB Swap:  2048.0 total, 1310.7 free,   737.3 used

  PID USER      %CPU %MEM COMMAND
 2381 root      71.3 12.4 tar
 1044 www-data 18.2  6.1 nginx
  912 mysql     9.7 31.0 mysqld
```

us / sy
waktu CPU untuk aplikasi / kernel

wa = 25.4
CPU menunggu disk — I/O jadi biang lambat

zombie
proses mati yang belum dibersihkan (Bab 5)

Swap used
737 MiB terpakai → RAM mulai sesak

Tombol di top: `P` urut CPU · `M` urut memori · `k` kill PID · `1` per core · `q` keluar

htop: versi interaktif dengan warna, mouse, dan F6 untuk memilih urutan.

Memori & disk: angka yang sering disalahpahami

```
$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       2.9Gi       210Mi       1.0Mi       700Mi       620Mi
Swap:          2.0Gi       737Mi       1.3Gi
```

Lihat kolom available, bukan free. Linux sengaja memakai RAM kosong sebagai cache; cache itu bisa dilepas saat dibutuhkan.

```
$ df -h /var
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        50G   46G  4.0G  92% /var

$ sudo du -sh /var/* | sort -h | tail -3
1.2G    /var/cache
4.8G    /var/lib
 38G    /var/log
```

`df` memberi tahu partisi mana yang penuh; `du` menunjukkan folder mana penyebabnya.

Jebakan inode: “No space left on device” padahal df -h masih lega? Cek df -i — jutaan berkas kecil bisa menghabiskan inode.

Jaringan: ss menggantikan netstat

```
$ sudo ss -tulnp
Netid State  Local Address:Port  Process
udp   UNCONN 0.0.0.0:67          dhcpd
tcp   LISTEN 0.0.0.0:53          named
tcp   LISTEN 0.0.0.0:22          sshd
tcp   LISTEN 0.0.0.0:80          nginx
tcp   LISTEN 0.0.0.0:445         smbd
```

Arti opsi -tulnp

`-t / -u`	TCP / UDP
`-l`	hanya yang listening
`-n`	angka port, bukan nama
`-p`	tampilkan proses (perlu sudo)

Ringkasan koneksi `ss -s`

Siapa yang terhubung ke web? `ss -tn state established '( sport = :80 )'`

Statistik antarmuka `ip -s link show enp0s3`

02

Log: buku harian server

Metrik memberi tahu “ada masalah”; log memberi tahu “apa masalahnya”

Peta log di /var/log

Berkas (Debian/Ubuntu)	Isi	Pertemuan
`/var/log/syslog`	Pesan umum sistem & layanan	**semua**
`/var/log/auth.log`	Login, sudo, SSH, fail2ban	**12**
`/var/log/kern.log`	Pesan kernel, driver, disk error	**1, 4**
`/var/log/nginx/`	access.log & error.log per situs	**10**
`/var/log/samba/`	Koneksi & error Samba	**11**
`/var/log/backup.log`	Hasil skrip backup harian	**13**

Pada RHEL/CentOS: /var/log/messages dan /var/log/secure. Membaca log sistem perlu sudo atau grup adm.

Tingkat keparahan pesan log (syslog)

0	**emerg**	Sistem tidak bisa dipakai
1	**alert**	Harus ditangani segera
2	**crit**	Kondisi kritis
3	**err**	Error
4	**warning**	Peringatan
5	**notice**	Normal tapi penting
6	**info**	Informasi
7	**debug**	Detail untuk debugging

```
journalctl -p err -b      # level 0–3 sejak boot terakhir
journalctl -p warning --since today
```

Semakin kecil angkanya, semakin parah. -p err menampilkan err dan semua yang lebih parah.

Resep journalctl yang paling sering dipakai

Log satu layanan hari ini

```
journalctl -u ssh --since today
```

Ikuti secara langsung

```
journalctl -u nginx -f
```

Rentang waktu tertentu

```
journalctl --since "09:00" --until "10:00"
```

Boot sebelumnya (setelah crash)

```
journalctl -b -1 -p err
```

Pesan kernel saja

```
journalctl -k
```

Ukuran & pembersihan jurnal

```
journalctl --disk-usage
sudo journalctl --vacuum-time=14d
```

Mengubah ribuan baris log menjadi jawaban

10 IP teratas yang gagal login SSH

```
sudo grep "Failed password" /var/log/auth.log \
  | grep -oE 'from [0-9.]+' | sort | uniq -c \
  | sort -rn | head
```

Halaman yang paling sering 404

```
sudo awk '$9 == 404 {print $7}' \
  /var/log/nginx/access.log | sort | uniq -c \
  | sort -rn | head
```

Pantau error secara langsung

```
sudo tail -f /var/log/syslog | grep -i error
```

Pola pipeline

`grep`

saring baris

↓

`awk / grep -o`

ambil kolom

↓

`sort | uniq -c`

hitung

↓

`sort -rn | head`

ambil teratas

logrotate: agar log tidak memenuhi disk



aktif → kemarin → dikompresi → … → dihapus setelah 8 minggu

```
# /etc/logrotate.d/backup
/var/log/backup.log {
    weekly
    rotate 8
    compress
    delaycompress
    missingok
    notifempty
}
```

weekly · rotate 8

putar tiap minggu, simpan 8 salinan

compress

salinan lama di-gzip, hemat ruang

missingok

jangan error bila berkas tidak ada

Uji tanpa menunggu

```
sudo logrotate -d /etc/logrotate.d/backup
```

Dari memantau ke diberi tahu: alert sederhana

```
#!/bin/bash
# /usr/local/bin/cek_server.sh
BATAS=80
PAKAI=$(df --output=pcent / | tail -1 | tr -dc '0-9')
if [ "$PAKAI" -gt "$BATAS" ]; then
  logger -p user.warning "DISK / sudah ${PAKAI}%"
fi

for svc in nginx named isc-dhcp-server smbd; do
  systemctl is-active --quiet "$svc" || \
    logger -p user.err "Layanan $svc MATI"
done
```



logger

Menulis pesan ke log sistem, sehingga muncul di journalctl -p warning bersama log lain.

Di industri

Prometheus + Grafana, Zabbix, Netdata: dasbor grafik & alert ke email/chat. Konsepnya sama dengan skrip ini.

Alur troubleshooting: dari gejala ke akar masalah



Gejala

"Server lambat"

`uptime`

Metrik

CPU, memori, disk, jaringan?

`top · free · df`

Proses

Proses mana penyebabnya?

`top (P/M) · ps`

Log

Mengapa proses itu begitu?

`journalctl -u`

Perbaiki & pantau

Atasi, lalu pastikan tidak berulang

`alert · cron`

Aturan emas: ukur dulu, baru ubah. Jangan langsung restart server — restart menghapus bukti (proses, isi memori) dan masalah akan kembali.

Studi kasus: server lambat tanpa sebab jelas

1 Gejala

Aplikasi sangat lambat sejak pagi; tidak ada perubahan konfigurasi.

2 Temuan htop

Proses backup yang seharusnya selesai tengah malam masih berjalan, memakan CPU & I/O.

3 Temuan log

journalctl -u backup.service: skrip gagal berhenti dan mengulang tanpa henti.

Solusi

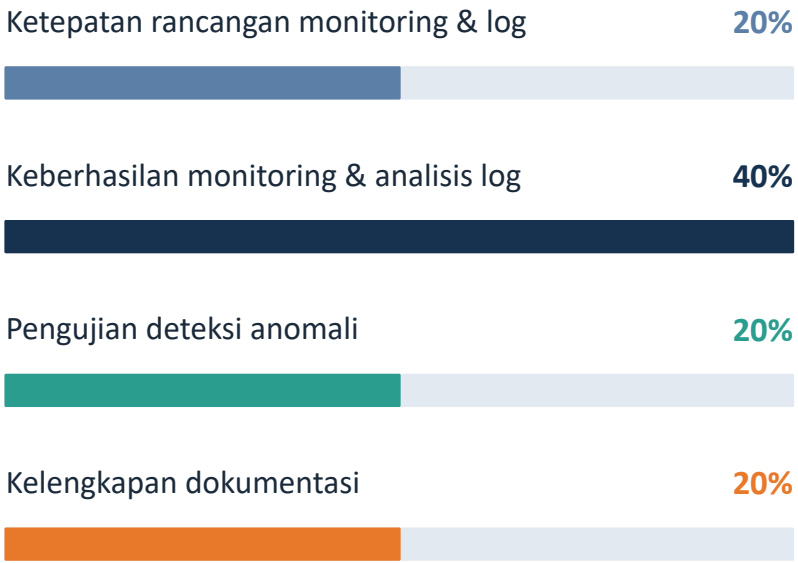
- Hentikan proses bermasalah (kill PID / systemctl stop)
- Perbaiki skrip: tambahkan batas waktu, mis. timeout 4h tar …
- Alert bila backup berjalan melebihi durasi wajar (Pertemuan 15)

Praktikum & penilaian (170 menit)

Tugas lab

1. Catat baseline: load, memori, disk, port yang listening
1. Beri beban (stress / unduhan besar), amati & jelaskan perubahan
1. Analisis auth.log & access.log: temukan anomali
1. Pasang logrotate untuk backup.log
1. Jalankan skrip cek_server.sh & buktikan alert di jurnal

Rubrik Pertemuan 14 · bobot 2% nilai akhir



Cek pemahaman

1	**Tools interaktif penggunaan CPU & memori per proses?**	htop
2	**Log layanan sshd hari ini dengan journalctl?**	journalctl -u sshd --since today
3	**Indikasi umum RAM tidak mencukupi?**	Penggunaan swap yang tinggi
4	**Beda fungsi syslog dan journalctl?**	Syslog: berkas teks per kategori; journalctl: jurnal terpusat, filter per unit/waktu/level
5	**CPU tinggi terus — langkah troubleshoot?**	uptime → top (P) → ps → journalctl -u → perbaiki → pantau

Rangkuman

Metrik

CPU (load vs core), memori (available, swap), disk (df/du/inode), jaringan (ss).

Log

/var/log & journalctl; saring per level, unit, waktu; rotasi dengan logrotate.

Troubleshooting

Gejala → metrik → proses → log → perbaiki → pantau. Ukur dulu, baru ubah.

Pertemuan 15

Otomatisasi (scripting/cron) & proyek kolaboratif. Baca Bab 14 dan bentuk kelompok 4 orang.

Referensi: Buku Ajar Bab 13 · Nemeth et al. (2021) · Sobell (2015) · systemd Journal Documentation