PERTEMUAN 13 · SUB-CPMK 4.1

Backup, Restore & Disaster Recovery

Strategi backup, rsync & tar, RTO/RPO, dan rencana pemulihan bencana

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

Target hari ini

Sub-CPMK 4.1

Mahasiswa mampu melakukan backup, restore, dan menyusun rencana pemulihan bencana (disaster recovery) dasar pada server.

- Memahami jenis strategi backup
- Menggunakan rsync & tar
- Menyusun kerangka DRP sederhana

Alur pertemuan

1	Mengapa & aturan 3-2-1	15'
2	Strategi backup	25'
3	rsync, tar & otomasi	30'
4	DRP, RTO/RPO & studi kasus	30'
5	Praktikum lab	170'

Data hilang bukan soal “jika”, tapi “kapan”



Kegagalan hardware

Disk rusak, server terbakar, banjir di ruang server



Kesalahan manusia

rm -rf di direktori yang salah, salah edit konfigurasi



Serangan siber

Ransomware mengenkripsi seluruh berkas dan menuntut tebusan

> *Backup yang tidak pernah diuji pemulihannya sama saja dengan tidak memiliki backup.*
>
> — Prinsip utama Bab 12

Aturan 3-2-1: pegangan praktis backup

3

salinan data

1 data asli + 2 backup

2

media berbeda

mis. disk server + NAS/disk eksternal

1

di luar lokasi

gedung lain atau cloud — selamat dari kebakaran

+1

offline / immutable

tidak bisa dijangkau ransomware

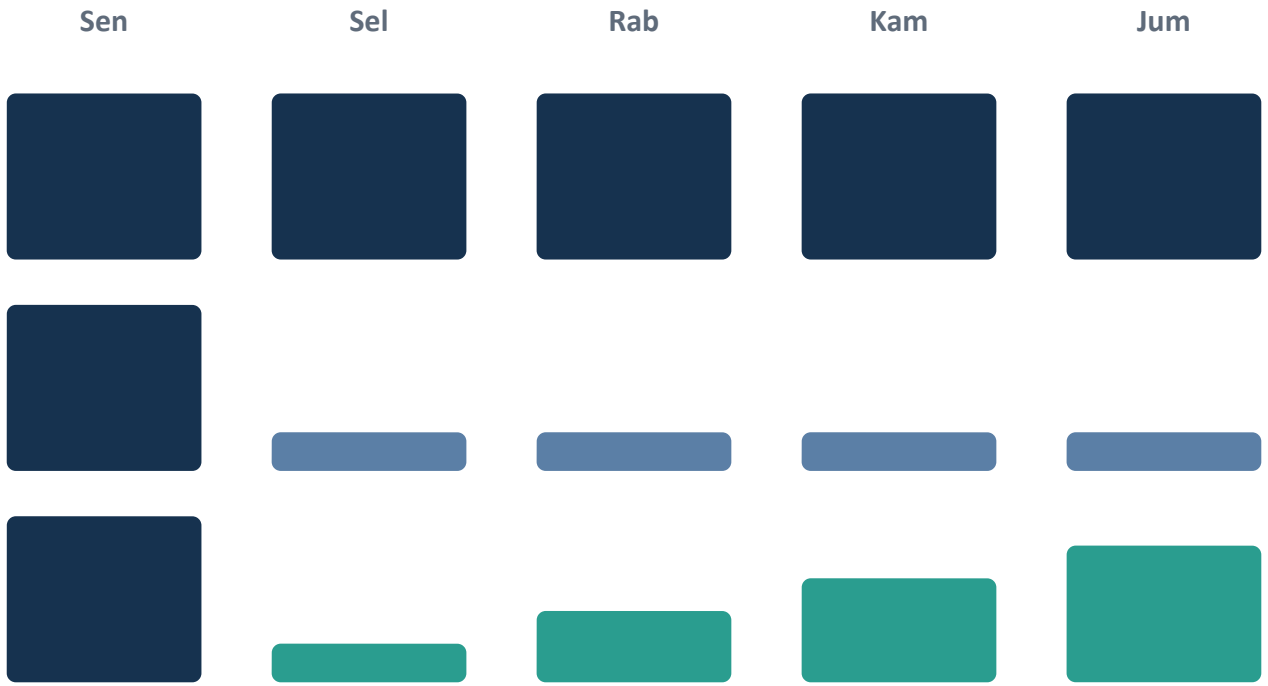
RAID dan sinkronisasi bukan backup: jika berkas terhapus atau terenkripsi, kerusakannya ikut tersalin seketika.

01

Strategi: full, incremental, differential

Tiga cara memilih apa yang disalin setiap hari — dan konsekuensinya saat restore

Apa yang disalin setiap hari?



Full

semua data, setiap hari

Incremental

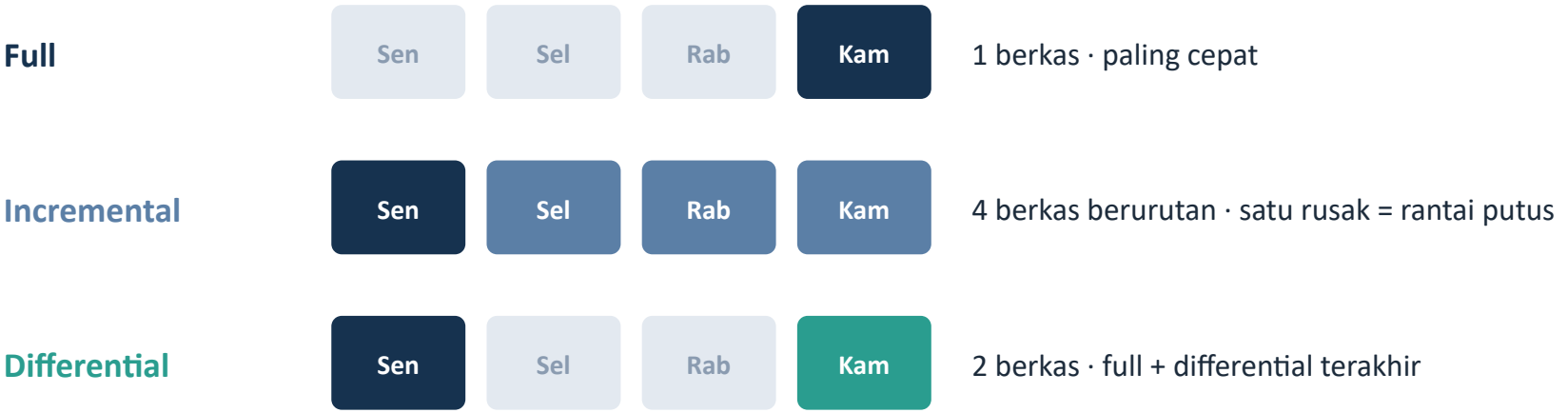
berubah sejak backup terakhir

Differential

berubah sejak full terakhir

Tinggi balok = ukuran data yang disalin hari itu. Senin selalu full backup sebagai titik awal.

Server rusak Jumat pagi — apa yang perlu di-restore?



Jenis	Ruang	Waktu backup	Waktu restore
Full	Besar	Lambat	Cepat
Incremental	Kecil	Cepat	Lambat
Differential	Sedang	Sedang	Sedang

02

Tools: tar dan rsync

Dua alat bawaan Linux yang cukup untuk kebanyakan kebutuhan backup server kecil

tar: arsip backup yang ringkas & portabel

```
# buat arsip terkompresi (c=create z=gzip f=file)
sudo tar -czf /backup/etc_$(date +%F).tar.gz /etc

# lihat isi tanpa mengekstrak (t=list)
tar -tzf /backup/etc_2026-10-06.tar.gz | head

# restore ke folder uji, bukan langsung ke /etc!
sudo tar -xzf /backup/etc_2026-10-06.tar.gz -C /restore

# incremental dengan GNU tar
sudo tar -czf /backup/data_full.tar.gz \
  --listed-incremental=/backup/data.snar /data
sudo tar -czf /backup/data_inc1.tar.gz \
  --listed-incremental=/backup/data.snar /data
```

`$(date +%F)`

Nama berkas otomatis berisi tanggal hari ini

`-C /restore`

Ekstrak ke lokasi uji dulu, bandingkan, baru salin yang perlu

`.snar`

Berkas catatan: tar tahu mana yang sudah disalin

rsync: hanya menyalin yang berubah

```
# lokal: -a arsip (izin, owner, waktu) · -v · -h
sudo rsync -avh /data/ /backup/data/

# ke server backup lewat SSH (kunci dari Pertemuan 12)
sudo rsync -avh -e ssh /data/ \
  backup@192.168.10.40:/backup/web01/data/

# selalu coba dulu dengan --dry-run
sudo rsync -avh --delete --dry-run /data/ /backup/data/
```

Jebakan garis miring: /data/ menyalin isinya; /data (tanpa /) membuat folder data/ di dalam tujuan.



Delta transfer

Run pertama menyalin semuanya. Run berikutnya hanya mengirim bagian berkas yang berubah — cepat dan hemat bandwidth.

`--delete` membuat tujuan identik dengan sumber — termasuk menghapus. Itu cermin, bukan riwayat.

Apa yang perlu di-backup dari server?

Backup

`/etc`	konfigurasi DNS, DHCP, web, Samba, SSH
`/home, /srv`	data pengguna & folder share
`/var/www`	situs web (Pertemuan 10)
Dump database	mysqldump / pg_dump, bukan salin berkas mentah
Daftar paket	dpkg --get-selections > paket.txt

Lewati

`/proc, /sys, /dev`
dibuat kernel saat boot

`/tmp, /var/cache`
sementara, bisa dibuat ulang

Folder /backup itu sendiri
agar tidak menyalin diri sendiri

Otomatis, bertanggal, dan diverifikasi

```
#!/bin/bash
# /usr/local/bin/backup_harian.sh
set -euo pipefail
exec >> /var/log/backup.log 2>&1
TGL=$(date +%F)
DEST=/backup/$TGL
mkdir -p "$DEST"

tar -czf "$DEST/etc.tar.gz" /etc
tar -czf "$DEST/www.tar.gz" /var/www
sha256sum "$DEST"/*.tar.gz > "$DEST/SHA256SUMS"
rsync -a "$DEST" backup@192.168.10.40:/backup/web01/
find /backup -maxdepth 1 -type d -mtime +14 \
  -exec rm -rf {} +
echo "$(date) backup OK"
```

Jadwalkan via crontab (Pertemuan 15)

```
0 2 * * * /usr/local/bin/backup_harian.sh
```

Tiap hari 02:00 · log di /var/log/backup.log

Uji restore rutin

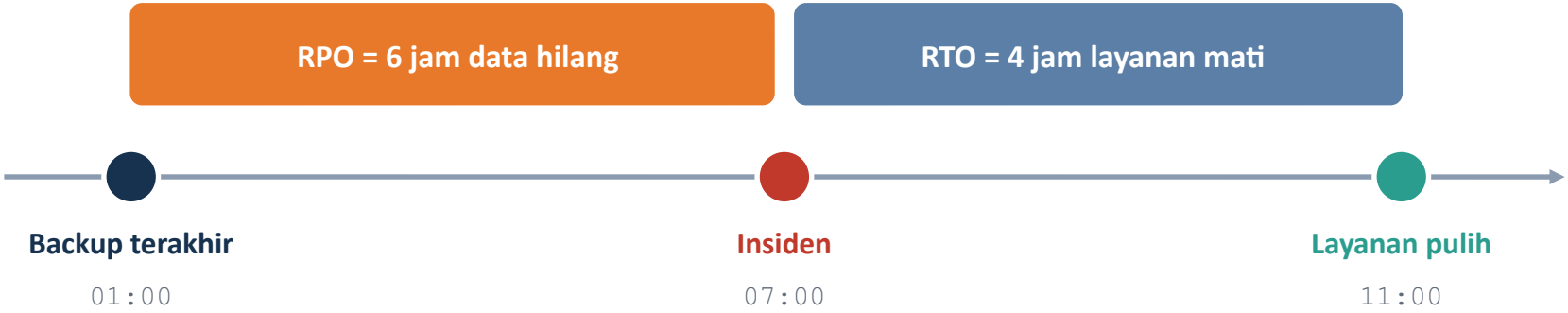
1. **Cek integritas**
   `sha256sum -c SHA256SUMS`
2. **Ekstrak ke /restore**
   bandingkan: `diff -r`
3. **Catat waktu restore**
   itulah RTO nyata Anda

03

Disaster Recovery Plan

Backup adalah bahan; DRP adalah resep untuk memulihkan layanan saat krisis

RPO & RTO: dua angka kunci DRP



RPO · Recovery Point Objective

Berapa banyak data (diukur dalam waktu) yang boleh hilang? Ditentukan oleh seberapa sering backup.

RTO · Recovery Time Objective

Berapa lama layanan boleh mati sampai pulih? Ditentukan oleh kecepatan restore & kesiapan prosedur.

Dari target RPO ke pilihan teknologi

Target RPO	Strategi	Contoh layanan	Biaya
24 jam	**Backup harian (tar/rsync via cron)**	Situs profil, berkas arsip	Rendah
1 jam	**Incremental per jam + log transaksi database**	Basis data pelanggan, SIAKAD	Sedang
≈ 0	**Replikasi real-time ke server kedua**	Transaksi bank, e-commerce besar	Tinggi

Semakin kecil RPO/RTO, semakin mahal infrastrukturnya — pilih sesuai nilai data, bukan "sebisa mungkin nol".

Isi minimal dokumen DRP

Aset kritikal & prioritas

Layanan mana dipulihkan lebih dulu (mis. DNS → DHCP → web)

Target RTO & RPO

Per layanan, disepakati dengan pimpinan

Prosedur langkah demi langkah

Bisa diikuti admin lain tanpa bertanya

Penanggung jawab

Siapa melakukan apa, termasuk cadangannya

Lokasi & akses backup

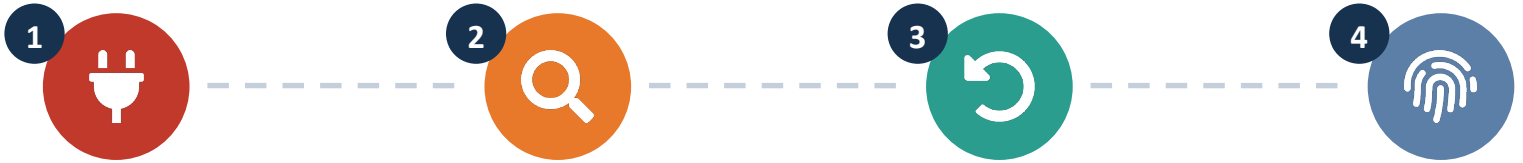
Di mana salinan off-site, siapa pegang kuncinya

Jadwal uji & revisi

DRP diuji rutin dan diperbarui setiap ada perubahan

Studi kasus: ransomware di kantor cabang

Seluruh data file server terenkripsi; pelaku meminta tebusan. Organisasi punya backup harian di server terpisah yang tidak terhubung ke jaringan saat tidak dipakai.



Isolasi

Cabut server terdampak dari jaringan agar tidak menyebar

Cari backup bersih

Pilih backup sebelum infeksi, cek checksum

Restore

Bangun ulang server & pulihkan data, bukan bayar tebusan

Akar masalah

Tinjau celah masuk & hardening (Pertemuan 12)

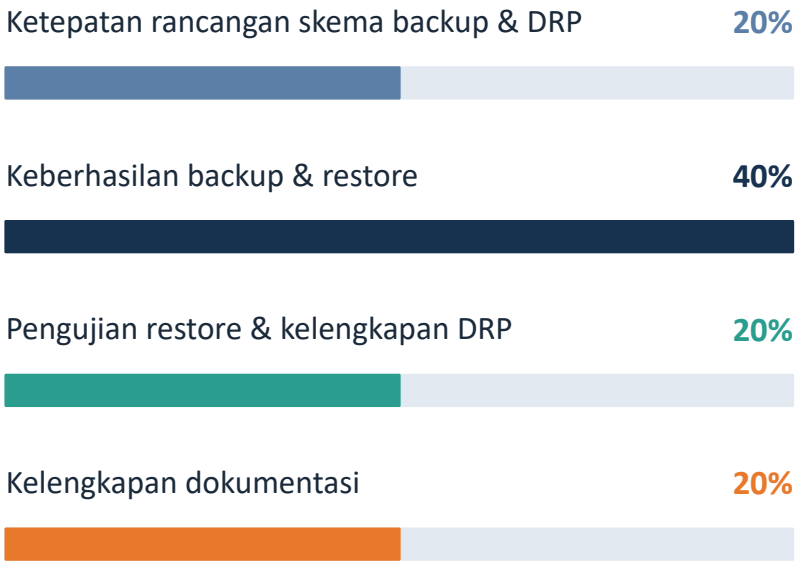
Mengapa berhasil? Backup tidak terjangkau ransomware (air-gapped). Data yang hilang hanya perubahan sejak backup terakhir — sesuai RPO yang sudah disepakati.

Praktikum & penilaian (170 menit)

Tugas lab

1. Backup full /etc & /var/www dengan tar + checksum
1. Replikasi ke VM backup dengan rsync via SSH
1. Jadwalkan skrip backup harian dengan cron
1. Simulasi bencana: hapus situs web, lalu restore & catat waktunya
1. Susun dokumen DRP 1–2 halaman untuk server kelompok

Rubrik Pertemuan 13 · bobot 1,5% nilai akhir



Cek pemahaman

1	**Backup perubahan sejak backup terakhir apa pun?**	Incremental backup
2	**Alat sinkronisasi dengan delta transfer?**	rsync
3	**Target maksimum data yang boleh hilang?**	RPO (Recovery Point Objective)
4	**Incremental vs differential?**	Inc: backup cepat, restore butuh semua rantai; Diff: restore cukup full + 1
5	**RPO 1 jam untuk basis data pelanggan?**	Incremental/log per jam atau replikasi + full harian off-site

Rangkuman

Strategi

Full, incremental, differential — trade-off ruang, waktu backup & restore; ikuti 3-2-1.

Tools

tar untuk arsip bertanggal, rsync untuk replikasi efisien; selalu verifikasi.

DRP

RPO & RTO menentukan strategi; prosedur tertulis dan diuji rutin.

Pertemuan 14

Monitoring Kinerja Sistem & Manajemen Log. Baca Bab 13 Buku Ajar sebelum kelas.

Referensi: Buku Ajar Bab 12 · Nemeth et al. (2021) · Frisch (2002) · Sobell (2015)