

SOP Backup dan Recovery Server / Database

1. Tujuan

Menetapkan standar operasional untuk melakukan backup (pencadangan) dan recovery (pemulihan) data pada server kampus agar menjamin keamanan, integritas, dan ketersediaan data penting, baik pada level aplikasi, database, maupun sistem keseluruhan.

2. Ruang Lingkup

SOP ini mencakup:

- Backup data aplikasi dan database menggunakan Restic ke Wasabi Cloud Storage (region: Singapore).
- Backup sistem penuh menggunakan snapshot VPS (dikelola oleh penyedia layanan server).
- Prosedur pemulihan (restore) baik sebagian maupun total.
- Verifikasi hasil backup dan jadwal pengujian restore.

3. Penanggung Jawab

Jabatan	Tanggung Jawab
System Administrator / DevOps	Konfigurasi dan monitoring backup Restic, pengujian restore
Kepala STK	Persetujuan kebijakan backup, alokasi penyimpanan
Database Administrator (DBA)	Backup dan pemulihan data database
Vendor/Unit Penyedia VPS	Snapshot dan restore di level virtualisasi

4. Referensi

- Kebijakan Keamanan Informasi Kampus (Data Retention & Availability).
- Dokumentasi resmi Restic (<https://restic.net/>)
- Dokumentasi Wasabi Cloud Storage (<https://wasabi.com/>)

5. Media dan Teknologi Backup

Jenis Backup	Teknologi	Lokasi	Retensi
Aplikasi & Database	Restic	Wasabi (Singapore)	52 minggu
Konfigurasi Sistem & File Server	Restic	Wasabi (Singapore)	52 minggu
Seluruh VPS (Full Image)	Snapshot via panel virtualisasi (KVM)	Cloud Provider	7 hari (rolling)

6. Prosedur Backup

6.1 Backup Level Aplikasi dan Database (Restic)

1. Persiapan

- Pastikan Restic telah terinstal (`curl -L https://restic.net/...` atau via Centminmod custom script).

- Pastikan akses ke bucket Wasabi berfungsi (AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY).
- Direktori penting:
 - /home/nginx/domains/ → file web & konfigurasi
 - /usr/local/nginx/conf/ → konfigurasi Nginx
 - /root/scripts/ → script otomatisasi
 - /var/lib/mysql/ atau dump database → data DB
- 2. Eksekusi Backup
 - Jalankan perintah:
 - `restic -r s3:https://s3.ap-southeast-1.wasabisys.com/uss-backup \`
 - `backup /home/nginx /var/lib/mysql /etc /root --verbose`
 - Gunakan cronjob harian (misal pukul 02:00 WIB):
 - `0 2 * * * /usr/local/bin/backup.sh >> /var/log/backup.log 2>&1`
- 3. Verifikasi
 - Jalankan:
 - `restic check`
 - `restic snapshots`
 - Pastikan snapshot harian muncul dan tidak ada error integrity.
- 4. Retensi Otomatis
 - Atur kebijakan retensi:
 - `restic forget --keep-daily 7 --keep-weekly 4 --keep-monthly 3 --prune`
 - Log hasil disimpan di `/var/log/backup.log`.

6.2 Backup Level Sistem (Snapshot VPS)

1. Backup snapshot dilakukan oleh tim penyedia VPS (unit kerja lain dalam grup perusahaan).
2. Permintaan snapshot rutin dijadwalkan otomatis setiap minggu malam (Minggu, 23:00 WIB).
3. Snapshot tambahan dapat diminta sebelum perubahan besar (upgrade OS, update aplikasi, dsb).
4. Snapshot disimpan di storage virtualisasi KVM dengan masa retensi 7 hari.

7. Prosedur Recovery

7.1 Pemulihan Data dari Restic

1. Pastikan akses ke repository Wasabi dan password Restic tersedia.
2. Daftar snapshot:
3. `restic snapshots`
4. Pilih snapshot dan lakukan restore:
5. `restic restore <snapshot-id> --target /restore`
6. Verifikasi file hasil restore, lalu pindahkan ke direktori aktif.
7. Untuk database, lakukan restore dump:
8. `mysql -u root -p database_name < /restore/db.sql`
9. Setelah selesai, hapus direktori `/restore` untuk menghemat ruang.

7.2 Pemulihan Level VPS (Snapshot)

1. Ajukan permintaan ke penyedia VPS melalui kanal resmi (chat internal atau tiket).
2. Sertakan:
 - o Nama server,
 - o IP Address,
 - o Tanggal snapshot yang akan direstore.
3. Tim penyedia melakukan restore snapshot di panel virtualisasi.
4. Setelah restore, System Admin melakukan:
 - o Verifikasi layanan (systemctl status semua service),
 - o Cek integritas database dan aplikasi web.

8. Jadwal Backup

Jenis	Frekuensi	Media	Pelaksana
Aplikasi & Database	Harian (02:00 WIB)	Restic → Wasabi	System Admin
Sistem & Konfigurasi	Mingguan	Restic → Wasabi	System Admin
Snapshot VPS	Mingguan (Minggu 23:00 WIB)	Virtualisasi KVM	Unit Penyedia VPS

9. Pengujian Backup dan Restore

1. Uji restore minimal 1x per bulan dengan data acak.
2. Simulasi disaster recovery dilakukan setiap 6 bulan.
3. Hasil pengujian dilaporkan ke Kepala Divisi Infrastruktur TI.

10. Dokumentasi

- Log backup harian (/var/log/backup.log).
- Daftar snapshot Restic dan VPS.
- Catatan uji restore.
- Template permintaan restore snapshot.
- Rekapitulasi kapasitas bucket Wasabi.

11. Catatan Tambahan

- Semua kredensial Wasabi dan password Restic disimpan terenkripsi di password manager internal.
- Pastikan timezone server sudah Asia/Jakarta sebelum backup otomatis berjalan.
- Backup Restic berjalan di atas sistem Centminmod stable.
- Notifikasi hasil backup (sukses/gagal) dikirim otomatis via Telegram/Email admin.