PRD: Audit Log & Monitoring Infrastruktur

Web Desa Sangkima

Penulis: Nabil **Tanggal:** 8 Juli 2026 **Status:** Draft v0.1

1. Ringkasan

Dokumen ini membahas rencana penambahan dua kapabilitas ke sistem web-desa-sangkima: audit log aktivitas akun, dan monitoring infrastruktur/uptime server. Keduanya sebenarnya berangkat dari masalah yang sama kewajiban maintenance 1 tahun sesuai MoU dengan pihak desa dan sponsor menuntut adanya cara untuk menelusuri aktivitas di sistem dan mengetahui masalah server lebih awal, bukan setelah ada yang melapor duluan.

2. Masalah

Sistem e-surat yang berjalan sekarang punya alur persetujuan dua level dan menyimpan data pribadi warga desa. Satu-satunya jejak aktivitas yang tersimpan saat ini adalah tabel *letterRequestLogs*, yang mencatat perubahan status pengajuan surat. Di luar dari itu tidak ada catatan apa-apa. seperti siapa yang login, siapa yang menghapus akun warga, siapa yang mengubah role admin semuanya dapat dilakukan tanpa jejak.

Masalah ini akan terasa ketika sistem telah diberikan ke pihak desa melalui serahterima. Kalau suatu hari ada pertanyaan seperti “kenapa pengajuan surat saya hilang” atau “kenapa akun saya tidak bisa dipakai lagi”, saat ini tidak ada cara menjawabnya selain menebak-nebak lewat database secara manual. Untuk sistem yang menyangkut layanan publik dan terikat kontrak maintenance, ini risiko yang sebaiknya ditutup dari awal.

Ada juga masalah di sisi operasional server. Web ini nantinya berjalan di VPS yang saya kelola sendiri, dan sejauh ini cara saya tahu server bermasalah adalah dari laporan orang lain, bukan dari sistem. Untuk layanan yang dipakai warga desa, jeda antara server down dan saya menyadarinya idealnya bisa dipangkas jadi hitungan menit, bukan menunggu ada yang komplain.

3. Solusi yang Diusulkan

Ada dua hal yang diusulkan, dan saya sengaja memisahkannya karena cara pengerjaannya beda.

Pertama, audit log aktivitas akun. Ini fitur baru yang perlu dibangun langsung di aplikasi mencatat login, perubahan akun, dan memperluas log surat yang sudah ada supaya semuanya bisa dilihat dari satu tempat.

Kedua, monitoring uptime dan resource server. Ini sebenarnya tidak perlu dibangun dari awal lagi. Karena platform deployment yang dipakai sekarang (Coolify), sudah punya monitoring bawaan (status container, disk usage, status backup). Tinggal ditambah Uptime Kuma, yang juga bisa di-deploy langsung dari Coolify dalam beberapa klik, untuk pengecekan uptime dari luar dan notifikasi otomatis. Bagian ini murni soal konfigurasi, bukan pengembangan aplikasi baru.

4. Tujuan & Ukuran Keberhasilan

Tujuan	Ukuran Keberhasilan
Aktivitas akun bisa ditelusuri	Semua aksi di daftar cakupan (bagian 7) tercatat di produksi, tanpa gap
Masalah server terdeteksi lebih cepat dari laporan manual	Notifikasi otomatis masuk maksimal 5 menit setelah server down
Ada bukti objektif kalau terjadi sengketa data	Tidak ada kasus yang berakhir “tidak bisa ditelusuri” selama masa maintenance

5. Di Luar Cakupan

Beberapa hal sengaja tidak masuk ke fase ini supaya scope-nya tetap terkendali:

- Mencatat setiap request GET / aktivitas melihat data biasa nilainya kecil dibanding beban storage dan noise yang ditimbulkan
- Audit siapa membaca data pribadi tertentu baru relevan kalau nanti ada kebutuhan compliance yang lebih spesifik dari sekarang
-

Dashboard monitoring custom dipertimbangkan lagi kalau traffic sudah jauh lebih besar

- Analytics pengunjung atau session replay di luar tujuan dokumen ini, yang fokusnya ke akuntabilitas dan ketersediaan sistem, bukan perilaku pengguna

6. Pengguna & Akses

Peran	Akses
Developer	Penuh ke audit log dan monitoring; penerima notifikasi utama
Admin desa	Tidak ada akses default; bisa diberi akses terbatas (lihat saja atau hasil export) kalau memang dibutuhkan
Petugas / warga	Tidak mengakses log mereka yang aktivitasnya dicatat, bukan yang melihat catatan

7. User Stories & Kebutuhan Fungsional

ID	User Story	Prioritas
US-1	Saya ingin setiap percobaan login (berhasil maupun gagal) tercatat, supaya saya bisa mendeteksi percobaan akses yang mencurigakan.	P0
US-2	Saya ingin setiap perubahan akun oleh admin (buat, ubah, hapus, ganti role) tercatat, supaya ada jejak tanggung jawab yang jelas.	P0
US-3	Saya ingin log approve/reject surat yang sudah ada terhubung ke log umum, supaya semua log bisa dilihat dari satu tempat.	P1
US-4	Saya ingin mendapat notifikasi otomatis kalau server down atau resource-nya kritis, supaya saya bisa menangani sebelum ada warga yang melapor.	P0

ID	User Story	Prioritas
US-5	Saya ingin bisa export sebagian log jadi file terpisah, supaya saya bisa membagikannya ke admin desa tanpa perlu memberi akses penuh ke sistem.	P2

P0 berarti wajib ada di rilis pertama, P1 penting tapi bisa menyusul, P2 nice-to-have kalau waktu memungkinkan.

8. Kebutuhan Non-Fungsional

- Retensi data minimal 12 bulan, mengikuti durasi maintenance. Kebijakan setelah itu belum diputuskan (lihat bagian 9).
- Pencatatan log tidak boleh mengganggu performa aksi utama approval surat, misalnya, harus tetap jalan meski proses logging gagal.
- Data pribadi di log (IP address, dsb.) dicatat seperlunya saja, bukan semuanya.

9. Timeline / Fase

Fase	Cakupan
Fase 1 (MVP)	Semua user story P0 dan P1, plus setup Uptime Kuma dan notifikasi Coolify
Fase 2 (lanjutan, Masih dipertimbangkan)	Audit akses data sensitif, dashboard resource lanjutan, akses granular untuk admin desa, integrasi error tracking