RANCANG BANGUN SYSTEM DAEMON UNTUK MONITORING LOG SECARA OTOMATIS PADA LINUX

Dosen Pengampu :

Ferdi Chahyadi, S.Kom., M.Cs

Disusun oleh :

1. Fachrezi Bachry (2401020010)
2. Willy Hadipermana (2401020019)
3. Haikal Fachry Akbar (2401020027)
4. Muhammad Faiz (241020040)

FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN

UNIVERTAS MARITIM RAJA ALI HAJI

1. Latar Belakang

Administrasi sistem modern menuntut efisiensi dan keandalan operasional yang tinggi. Dalam lingkungan sistem operasi Linux, automasi menjadi kunci untuk mencapai tujuan tersebut, memungkinkan tugas-tugas rutin dan krusial berjalan tanpa intervensi manual. Salah satu aspek terpenting dari pemeliharaan sistem adalah monitoring log, di mana catatan aktivitas sistem, keamanan, dan aplikasi direkam secara berkelanjutan. Log ini merupakan sumber informasi vital untuk mendeteksi anomali, mengidentifikasi serangan keamanan, dan melakukan troubleshooting 1.

Secara tradisional, administrator sistem sering kali melakukan monitoring log secara manual, yaitu dengan membaca atau mencari pola tertentu dalam file log menggunakan perintah seperti tail, grep, atau less. Pendekatan manual ini sangat tidak efisien, rentan terhadap human error, dan tidak praktis untuk sistem dengan volume log yang tinggi atau yang memerlukan pemantauan 24/7. Permasalahan inefisiensi ini menyoroti kebutuhan mendesak akan sebuah mekanisme yang dapat menjalankan tugas monitoring log secara otomatis dan berkelanjutan.

Kebutuhan ini dapat dijawab melalui implementasi daemon atau service yang berjalan di latar belakang. Daemon memiliki peran fundamental dalam menjaga layanan sistem tetap berjalan secara otomatis, terlepas dari status login pengguna. Dalam ekosistem Linux modern, systemd telah menjadi standar init system dan service manager yang dominan, menggantikan sistem lama seperti SysVinit. systemd menawarkan kerangka kerja yang kuat dan terstruktur untuk mendefinisikan, mengelola, dan memastikan keandalan service sistem, termasuk fitur penting seperti auto-restart dan manajemen dependensi.

Oleh karena itu, proyek ini bertujuan untuk merancang dan membangun sebuah system daemon yang memanfaatkan kapabilitas systemd untuk melakukan monitoring log secara otomatis. Dengan mengintegrasikan skrip monitoring ke dalam unit systemd, sistem akan memiliki layanan yang mandiri, dapat berjalan otomatis saat boot, dan mampu memulihkan diri (self-healing) jika terjadi kegagalan, sehingga

secara signifikan meningkatkan efisiensi dan proaktifitas administrasi sistem.

2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah yang akan dijawab melalui proyek ini adalah:

1. Bagaimana merancang dan mengimplementasikan sebuah system daemon (layanan) yang mampu berjalan secara otomatis segera setelah sistem Linux selesai booting?
2. Bagaimana daemon dapat dikonfigurasi untuk melakukan monitoring terhadap file log tertentu (misalnya /var/log/auth.log) secara real-time atau berkala?
3. Bagaimana memastikan service yang menjalankan daemon monitoring log ini dapat tetap berjalan (auto-restart) dan pulih secara otomatis jika terjadi kegagalan atau error pada skrip monitoring?
4. Bagaimana memanfaatkan fitur logging dan status reporting dari systemd untuk memverifikasi bahwa proses monitoring log berjalan dengan stabil dan benar?

3. Tujuan Proyek

Tujuan utama dari pelaksanaan proyek ini adalah:

1. Membangun layanan otomatis (daemon) berbasis systemd yang berfungsi sebagai log monitor di lingkungan sistem operasi Linux.
2. Memonitor file log tertentu secara berkelanjutan dan menyimpan hasil pemantauan (misalnya, baris log yang mengandung kata kunci tertentu) ke dalam file output yang terpisah.
3. Mengimplementasikan konfigurasi service systemd yang memastikan layanan monitoring log berjalan secara otomatis (auto-run) saat sistem boot dan diaktifkan (enabled).
4. Menguji stabilitas dan keandalan daemon melalui fitur auto-restart dan manajemen log (journalctl) yang disediakan oleh systemd.

4. Manfaat Proyek

Proyek ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Akademis, Memberikan pemahaman praktis dan mendalam mengenai mekanisme kerja systemd, khususnya dalam pembuatan service unit dan manajemen proses daemon di Linux.
2. Operasional, Mengurangi pekerjaan manual yang berulang dalam membaca dan menganalisis log sistem, sehingga administrator dapat fokus pada tugas yang lebih strategis.
3. Pengembangan, Menjadi fondasi dan proof-of-concept yang solid untuk pengembangan layanan automasi yang lebih kompleks di masa depan, seperti sistem notifikasi real-time atau integrasi dengan alat analisis log eksternal.
4. Keamanan, Membantu administrator sistem dalam mendeteksi aktivitas penting, mencurigakan, atau kegagalan sistem secara otomatis dan lebih cepat.

5. Batasan Masalah

Untuk menjaga fokus proyek dan memastikan pencapaian tujuan dalam lingkup waktu yang tersedia, batasan masalah yang ditetapkan adalah:

- **Target Monitoring**: Sistem daemon hanya akan melakukan monitoring pada 1 hingga 2 file log utama sistem (misalnya, /var/log/auth.log untuk aktivitas otentikasi atau /var/log/syslog untuk pesan sistem umum).
- **Fungsi Analisis**: Proyek ini tidak membahas analisis log tingkat lanjut seperti machine learning, log parsing kompleks, atau visualisasi data log. Fokus utama adalah pada mekanisme triggering dan persistence layanan monitoring.
- **Lingkungan Implementasi**: Proyek akan dibangun dan diuji pada distribusi Linux yang menggunakan systemd sebagai init system standar (misalnya, Ubuntu Server, Debian, atau Fedora).

- **Cakupan Laporan**: Laporan proyek akan fokus pada proses pembuatan skrip monitoring, konfigurasi service unit systemd, dan hasil pengujian stabilitas daemon, bukan pada arsitektur server skala besar.

6. Landasan Teori

Proyek ini didasarkan pada beberapa konsep teoritis kunci dalam administrasi sistem Linux:

6.1 Linux Daemon

Daemon adalah program komputer yang berjalan sebagai proses latar belakang (background process), tidak terikat pada terminal kontrol, dan sering kali dimulai secara otomatis saat sistem boot. Karakteristik utama daemon meliputi:

- Proses Latar Belakang: Berjalan tanpa antarmuka pengguna.
- Tanpa Terminal: Tidak memiliki terminal kontrol (controlling terminal).
- Otomatis: Dirancang untuk berjalan secara terus-menerus dan otomatis.

6.2 systemd

systemd adalah init system dan service manager untuk sistem operasi Linux. Ia bertanggung jawab untuk menginisialisasi komponen sistem, mengelola service, dan mengawasi proses setelah kernel selesai booting. Komponen utama systemd yang relevan dengan proyek ini adalah:

- Service Unit: File konfigurasi (.service) yang mendefinisikan bagaimana sebuah layanan harus dimulai, dihentikan, dan dikelola.
- Target: Unit yang mengelompokkan unit-unit lain (mirip dengan runlevel tradisional).
- Journal: Sistem logging terpusat (journald) yang mengumpulkan log dari kernel, init system, dan aplikasi.
- File Service: Struktur file .service dibagi menjadi tiga bagian utama:

- [Unit]: Berisi metadata dan informasi dependensi (Requires, After).
- [Service]: Berisi instruksi eksekusi layanan (Type, ExecStart, Restart).
- [Install]: Berisi informasi instalasi (WantedBy).

6.3 Log System Linux

Log sistem adalah catatan kronologis dari semua aktivitas dan peristiwa yang terjadi pada sistem. Lokasi log standar umumnya berada di direktori /var/log/. Contoh log penting yang akan menjadi fokus proyek ini meliputi:

- /var/log/syslog atau /var/log/messages: Log umum sistem.
- /var/log/auth.log: Log yang mencatat upaya otentikasi dan otorisasi pengguna.

6.4 Shell Script

Skrip akan digunakan sebagai inti dari daemon monitoring. Skrip ini akan memanfaatkan perintah dasar Linux (seperti tail -f atau looping dengan grep) atau bahasa pemrograman seperti Python untuk:

- Membaca baris baru dari file log.
- Memfilter baris log berdasarkan kriteria tertentu (kata kunci).
- Menulis hasil yang difilter ke file output yang ditentukan.

7. Metodologi Perancangan

Metodologi yang akan digunakan dalam proyek ini mengikuti siklus pengembangan sistem yang terstruktur, memastikan setiap tahapan dilakukan secara sistematis.

7.1 Analisis Kebutuhan

Tahap awal ini berfokus pada pendefinisian secara spesifik:

- Apa yang dimonitor? Identifikasi file log target (/var/log/auth.log dan/atau /var/log/syslog) dan kata kunci spesifik yang harus dipantau (misalnya, "Failed password" atau "error").

- Output apa yang dihasilkan? Tentukan format dan lokasi file output yang akan menyimpan hasil monitoring (misalnya, /var/log/monitored_output.log).

7.2 Perancangan Workflow

Perancangan alur kerja daemon akan mencakup:

1. **Inisiasi**: systemd memulai service saat boot.
2. **Eksekusi Skrip**: Skrip monitoring dieksekusi oleh systemd.
3. **Pembacaan Log**: Skrip membaca stream log secara berkelanjutan (misalnya, menggunakan tail -f).
4. **Penyaringan**: Skrip memproses setiap baris log, memfilter berdasarkan kriteria yang ditentukan.
5. **Penyimpanan Output**: Baris log yang relevan disimpan ke file output.
6. **Looping/Kontinuitas**: Skrip dirancang untuk berjalan terus-menerus hingga dihentikan oleh systemd.
7. **Logging**: Semua aktivitas dan error skrip dicatat ke journald melalui stdout dan stderr

7.3 Perancangan Struktur File

Struktur file yang akan dibuat meliputi:

- File Skrip Monitoring: Skrip Shell (.sh) atau Python (.py) yang berisi logika monitoring log (misalnya, /usr/local/bin/log_monitor.sh).
- File Service systemd: File unit layanan yang mendefinisikan daemon (misalnya, /etc/systemd/system/log-monitor.service).

7.4 Implementasi

Tahap ini melibatkan penulisan kode skrip monitoring dan konfigurasi file service unit systemd.

- Skrip Monitoring: Penulisan skrip yang efisien untuk membaca, memfilter, dan menulis log.
- Service Unit: Konfigurasi parameter [Service] seperti Type=simple atau Type=forking, ExecStart, dan yang paling penting, Restart=always untuk memastikan auto-restart.

7.5 Testing

Pengujian akan dilakukan untuk memverifikasi fungsionalitas dan stabilitas daemon:

- Pengujian Fungsional: Menggunakan perintah systemctl start log-monitor.service dan systemctl status log-monitor.service untuk memverifikasi eksekusi dan status.
- Pengujian Auto-Run: Menggunakan systemctl enable log-monitor.service dan menguji reboot sistem untuk memastikan layanan dimulai secara otomatis.
- Pengujian Stabilitas: Secara sengaja menghentikan atau menyebabkan error pada skrip monitoring untuk memverifikasi bahwa fitur Restart=always berfungsi dengan baik dan layanan pulih secara otomatis.

7.6 Evaluasi Hasil

Evaluasi akan menilai keberhasilan proyek berdasarkan tujuan yang ditetapkan:

- Apakah monitoring log berjalan secara otomatis dan berkelanjutan?
- Seberapa stabil daemon saat menghadapi kegagalan?
- Apakah output yang dihasilkan akurat dan sesuai dengan kriteria filter?

8. Penutup

Proposal ini menguraikan rencana untuk merancang dan mengimplementasikan system daemon yang efektif untuk monitoring log otomatis menggunakan systemd. Proyek ini tidak hanya akan menghasilkan solusi praktis untuk meningkatkan efisiensi administrasi sistem, tetapi juga akan memberikan pemahaman teknis yang mendalam tentang manajemen layanan modern di Linux. Dengan fokus pada automasi, keandalan (auto-restart), dan integrasi dengan systemd, proyek ini diharapkan dapat menjadi kontribusi yang signifikan dalam studi administrasi sistem berbasis Linux.