

# **LAPORAN TUGAS BESAR PEMELIHARAAN DAN ADMINISTRASI IT**



## **NAMA KELOMPOK :**

- **Edmundt Jonathan (103092400038)**
- **Rifalina Desinta Nandari (103092400007)**
- **Naila Ayu Permatasari (103092400061)**

**Telkom University Surabaya**

**Teknologi Informasi**

**2025**

## 1. MANAJEMEN AKUN

### - Konfigurasi Grup

```
edmundcino@cinoKomputer:~$ sudo getent group developer
[sudo] password for edmundcino:
developer:x:1004:rifa
edmundcino@cinoKomputer:~$ getent group | grep -E 'rifa|naila|edmundcino'
adm:x:4:syslog,edmundcino
cdrom:x:24:edmundcino
sudo:x:27:edmundcino,edmundt
dip:x:30:edmundcino
plugdev:x:46:edmundcino
users:x:100:edmundcino,edmundt,edmundt,rifa,naila,alya
lpadmin:x:114:edmundcino
edmundcino:x:1000:
developer:x:1004:rifa
rifa:x:1002:
naila:x:1005:
```

**sudo getent group developer** (Perintah ini digunakan untuk menampilkan informasi detail tentang grup bernama "developer"), dengan menambahkan sudo, pengguna mendapatkan hak akses administratif untuk melihat detail grup yang mungkin memerlukan izin khusus. Hasilnya menunjukkan bahwa grup "developer" memiliki GID (Group ID) 1004 dan hanya beranggotakan satu user, yaitu "rifa". **getent group | grep -E 'rifa|naila|edmundcino'** (getent group akan menampilkan seluruh daftar grup beserta anggotanya di sistem). **grep -E 'rifa|naila|edmundcino'** menyaring hasil hanya untuk baris yang mengandung salah satu dari tiga nama tersebut. Hasilnya, kita dapat melihat grup-grup mana saja yang diikuti oleh masing-masing user tersebut, baik sebagai anggota utama maupun tambahan. Contohnya, "edmundcino" tergabung di beberapa grup seperti adm, cdrom, sudo, dip, plugdev, users, lpadmin, sedangkan "rifa" dan "naila" tergabung di grup users dan memiliki grup masing-masing sesuai namanya

### - Permission Folder

```
edmundcino@cinoKomputer:~$ getfacl /srv/projects
getfacl: Removing leading '/' from absolute path names
# file: srv/projects
# owner: root
# group: developer
# flags: -s-
user::rwx
group::rwx
other::---
```

**getfacl /srv/projects** digunakan untuk menampilkan Access Control List (ACL) dari sebuah file atau direktori. ACL memungkinkan pengaturan hak akses yang lebih detail dibandingkan dengan permission standar (rwx) pada Linux. Hanya pemilik (root) dan anggota grup developer yang dapat mengakses dan memodifikasi isi direktori /srv/projects. User lain tidak memiliki akses sama sekali. Dengan menggunakan ACL, administrator dapat memastikan file dan folder baru yang dibuat di dalam /srv/projects otomatis mengikuti aturan grup yang sudah ditetapkan.

## - Hasil ID dan Grup

```
edmundcino@cinoKomputer:~$ id edmundcino
uid=1000(edmundcino) gid=1000(edmundcino) groups=1000(edmundcino),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114(lpadmin)
edmundcino@cinoKomputer:~$ groups edmundcino
edmundcino : edmundcino adm cdrom sudo dip plugdev users lpadmin
edmundcino@cinoKomputer:~$ id rifa
uid=1002(rifa) gid=1002(rifa) groups=1002(rifa),100(users),1004(developer)
edmundcino@cinoKomputer:~$ groups rifa
rifa : rifa users developer
edmundcino@cinoKomputer:~$ id naila
uid=1005(naila) gid=1005(naila) groups=1005(naila),100(users)
edmundcino@cinoKomputer:~$ groups naila
naila : naila users
```

Pada output ini menunjukkan bahwa uid=1000, gid = 1000 (edmundcino) adalah user dengan hak akses paling tinggi, termasuk sudo (akses administrator), dan anggota banyak grup sistem. uid = 1002, gid = 1002 (rifa) merupakan anggota grup users dan developer dan memiliki akses standar pengguna serta tambahan sebagai anggota developer, yang mungkin digunakan untuk pengembangan perangkat lunak. Uid 1005 (naila) adalah pengguna biasa tanpa hak akses khusus (hanya anggota grup users).

## - Hasil ls -l (Untuk verifikasi hak akses)

```
edmundcino@cinoKomputer:~$ sudo ls -l /srv/projects
total 20
-rw-r--r-- 1 root developer 17 Jun 17 11:34 males.txt
-rw-r--r-- 1 root developer 11 Jun 17 11:36 pati.txt
-rw-rw---- 1 root developer  0 Jun 15 22:21 tes.txt
-rw-r--r-- 1 root developer 15 Jun 17 12:17 tubespati.txt
-rw-r--r-- 1 root developer 10 Jun 17 11:31 tubes.txt
-rw-r--r-- 1 root developer 11 Jun 17 11:30 tugas.txt
```

Perintah ls -l digunakan untuk menampilkan daftar file dan direktori beserta detail informasinya dalam format long listing. Dengan tambahan sudo, perintah dijalankan dengan hak akses administrator untuk memastikan semua file dapat ditampilkan, termasuk yang mungkin dibatasi untuk user biasa. Semua file di dalam /srv/projects dimiliki oleh user root dan tergabung dalam grup developer. **-rw-rw-r--** menunjukkan file tersebut dapat dibaca dan ditulis oleh owner dan grup, serta hanya dapat dibaca oleh user lain.

## 2. FOLDER SHARING

### - Folder data/dev dan Folder data/public

```
edmundcino@cinoKomputer:~$ ls -ld /data/dev
drwxrwx--- 2 root developer 4096 Jun 17 13:54 /data/dev
edmundcino@cinoKomputer:~$ ls -ld /data/public
drwxr-xr-x 2 root root 4096 Jun 17 10:45 /data/public
```

Pada output di data/ dev :

drwxrwx---:

- rwx (owner: root) → root bisa membaca, menulis, dan masuk direktori
- rwx (group: developer) → anggota grup developer juga bisa baca, tulis, dan masuk

- --- (others) → pengguna lain tidak punya hak akses sama sekali

Hak kepemilikannya root sebagai owner, developer sebagai grup dan hanya user root dan anggota grup developer yang bisa mengakses isi direktori ini.

Pada output data/public :

- rwxr-xr-x:
  - rwx (owner: root) → root bisa baca, tulis, dan masuk
  - r-x (group: root) → grup root bisa baca dan masuk, tapi tidak menulis
  - r-x (others) → semua pengguna bisa membaca dan masuk, tapi tidak menulis

Hak kepemilikannya root sebagai owner dan grup. Direktori ini bisa diakses oleh semua pengguna (public), tapi hanya root yang bisa menulis.

### 3. MONITORING SERVER

Skrip ini digunakan untuk mengambil data penggunaan **CPU, memori, dan disk**, lalu menyimpannya dalam format prometheus metrics ke file. Untuk monitoring server, menggunakan akses **sudo nano /usr/local/bin/monitor.sh**. Proses pemantauan dilakukan menggunakan script shell custom bernama **monitor.sh**. Script ini dijalankan secara otomatis setiap 10 menit menggunakan cron job.

```
#!/bin/bash

timestamp=$(date "+%Y-%m-%d %H:%M:%S")

cpu_usage=$(top -bn1 | awk '/Cpu/ {print 100 - $8}')
mem_usage=$(free -m | awk '/Mem:/ {printf "%.2f", $3/$2 * 100}')
disk_usage=$(df / | awk 'END {print $5}' | tr -d '%')

cat <<EOF > /opt/prometheus/monitor.prom
# HELP custom_cpu_usage CPU usage in percent
# TYPE custom_cpu_usage gauge
custom_cpu_usage $cpu_usage

# HELP custom_memory_usage Memory usage in percent
# TYPE custom_memory_usage gauge
custom_memory_usage $mem_usage

# HELP custom_disk_usage Disk usage in percent
# TYPE custom_disk_usage gauge
custom_disk_usage $disk_usage
EOF
```

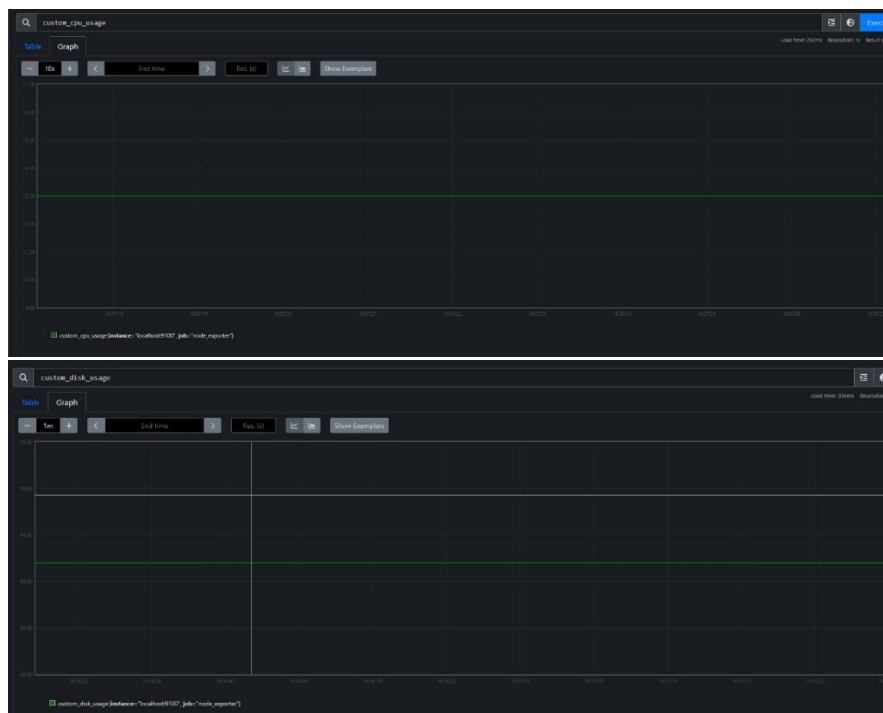
Selanjutnya Sistem menyimpan data ke dalam **file log /var/log/sysmon.log**. Setiap entri log memuat timestamp, presentase penggunaan CPU, penggunaan RAM dalam persen maupun MB, serta penggunaan disk. Dengan pencatatan berkala ini, administrator dapat memantau performa server secara konsisten, mendeteksi lonjakan pemakaian sumber daya, serta melakukan evaluasi sistem jika perlu.

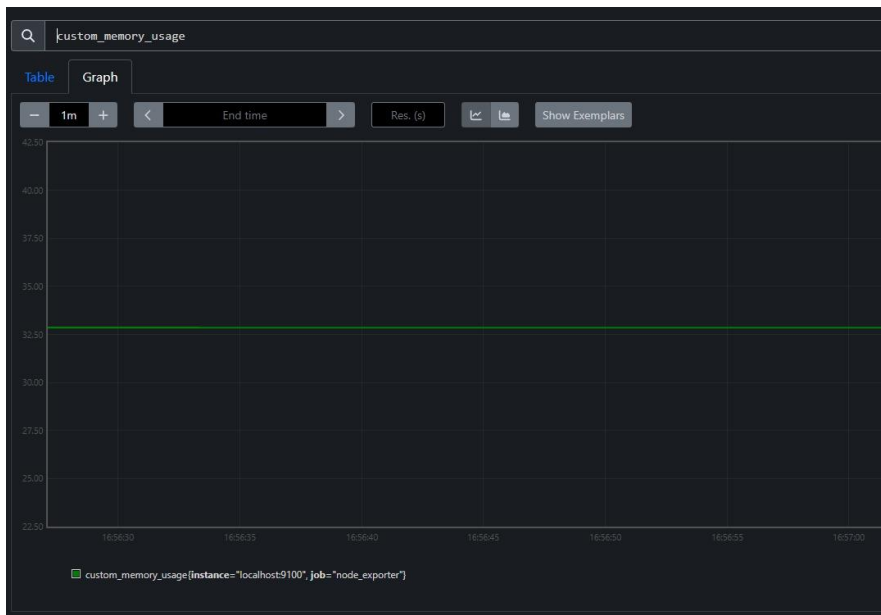
```

edmundtcino@cinoKomputer:~$ sudo /usr/local/bin/monitor.sh
edmundtcino@cinoKomputer:~$ cat /var/log/sysmon.log
2025-06-16 00:14:44 | CPU: 12% | RAM: 1260/3866 MB | DISK: 40%
2025-06-16 00:20:01 | CPU: 16% | RAM: 3016/3866 MB | DISK: 41%
2025-06-16 00:30:01 | CPU: 13% | RAM: 3091/3866 MB | DISK: 41%
2025-06-16 00:40:01 | CPU: 24% | RAM: 2883/3866 MB | DISK: 41%
2025-06-16 17:50:01 | CPU: 9% | RAM: 813/3866 MB | DISK: 41%
[2025-06-16 18:00:01] CPU: 8.3% | RAM: 31.69% | Disk: 41%
2025-06-16 18:00:01 | CPU: 9% | RAM: 1225/3866 MB | DISK: 41%
[2025-06-16 18:10:01] CPU: 11.5% | RAM: 31.53% | Disk: 41%
2025-06-16 18:10:02 | CPU: 9% | RAM: 1219/3866 MB | DISK: 41%
[2025-06-16 18:20:01] CPU: 8.3% | RAM: 31.30% | Disk: 41%
2025-06-16 18:20:01 | CPU: 5% | RAM: 1211/3866 MB | DISK: 41%
[2025-06-16 18:30:01] CPU: 22.2% | RAM: 31.35% | Disk: 41%
2025-06-16 18:30:01 | CPU: 56% | RAM: 1212/3866 MB | DISK: 41%
[2025-06-16 18:31:17] CPU: 12.5% | RAM: 31.38% | Disk: 41%
2025-06-16 18:31:17 | CPU: 9% | RAM: 1213/3866 MB | DISK: 41%
[2025-06-16 18:40:01] CPU: 13% | RAM: 32.31% | Disk: 41%
2025-06-16 18:40:01 | CPU: 12% | RAM: 1249/3866 MB | DISK: 41%
[2025-06-16 18:50:01] CPU: 8.3% | RAM: 31.66% | Disk: 41%
2025-06-16 18:50:02 | CPU: 5% | RAM: 1224/3866 MB | DISK: 41%
[2025-06-16 19:00:01] CPU: 12% | RAM: 31.66% | Disk: 41%
2025-06-16 19:00:01 | CPU: 12% | RAM: 1224/3866 MB | DISK: 41%
[2025-06-16 19:10:01] CPU: 13.3% | RAM: 32.54% | Disk: 42%

```

Berikut adalah tampilan dari dasbor data metrik Prometheus dengan query **custom\_cpu\_usage** untuk melihat penggunaan cpu saat ini, **custom\_disk\_usage** untuk melihat penggunaan disk saat ini, dan **custom\_ram\_usage** untuk melihat penggunaan ram saat ini.





Grafik menampilkan garis hijau horizontal yang menunjukkan penggunaannya dalam rentan waktu tertentu, jika menunjukkan stabil berarti tidak banyak aktivitas berat. Query yang digunakan ini adalah metrik kustom yang berasal dari **file .prom** yang di generate oleh script **monitor.sh**

## 4. DNS CACHING SERVER

Untuk mengatur agar server DNS lokal bisa meneruskan permintaan DNS ke **Google DNS**, perlu mengedit konfigurasi BIND di file `named.conf.options`. File ini bisa diakses dengan perintah **sudo nano /etc/bind/named.conf.options**. Selengkapnya sebagai berikut.

```
Options {
    directory "/var/cache/bind";

    recursion yes;
    allow-query { any; };
    listen-on port 53 { any; };

    forwarders {
        8.8.8.8;
        1.1.1.1;
    };

    dnssec-validation auto;
};
```



Konfigurasi ini membuat BIND9 bertindak sebagai **caching recursive DNS server**, dengan kemampuan meneruskan **query ke DNS eksternal dan memvalidasi DNSSEC**. Cocok untuk jaringan lokal yang ingin mempercepat akses DNS dan mengontrol permintaan DNS secara lokal.

```
edmundcino@cinoKomputer:~$ dig google.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29213
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 5       IN      CNAME   forcesafesearch.google.com.
forcesafesearch.google.com. 5       IN      A       216.239.38.120

;; Query time: 20 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jun 17 17:02:37 WIB 2025
;; MSG SIZE rcvd: 85
```

Perintah **dig.google.com** digunakan untuk mengkonfirmasi apakah **DNS lokal** berhasil meneruskan permintaan ke **DNS luar**. Sebagai contoh tampilan di atas

- DNS berjalan normal
- Domain google.com berhasil diterjemahkan
- IP yang dikembalikan adalah milik Google SafeSearch (216.239.38.120)