Monitoring Koneksi Aktif ke Server

Untuk melihat koneksi aktif ke server Anda, termasuk IP yang terhubung, gunakan `netstat`:
secara real time setiap 2 detik:

`watch -n 2 netstat -ntu`

contoh hasil:

```
Every 2.0s: netstat -ntu                    kominfos-0B: Tue Jun 24 21:28:23 2025  Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          127.0.0.1:47308         ESTABLISHED
tcp        0      0 127.0.0.1:57164         127.0.0.1:556           ESTABLISHED
tcp        0      0 127.0.0.1:38366         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:556           127.0.0.1:57164         ESTABLISHED
tcp        0      0 192.168.80.51:22        196.251.70.166:57154    ESTABLISHED
tcp        0      0 192.168.80.51:41344     91.189.91.48:80         TIME_WAIT
tcp        0      0 192.168.80.51:2014      222.124.78.211:59143    ESTABLISHED
tcp        0      0 127.0.0.1:47308         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:3306          127.0.0.1:38366         ESTABLISHED
tcp        0      0 192.168.80.51:22        222.124.78.211:59160    ESTABLISHED
tcp6       0      0 192.168.80.51:443       114.125.120.16:41242    TIME_WAIT
tcp6       0      0 192.168.80.51:80        45.82.76.192:41150      SYN_RECV
tcp6       0     25 192.168.80.51:443       177.93.63.18:45129      CLOSING
udp        0      0 192.168.80.51:68        192.168.80.1:67         ESTABLISHED
udp        0      0 169.254.95.120:68       169.254.95.118:67       ESTABLISHED
```

Daftar Status Koneksi TCP & Penjelasannya

State	Penjelasan
ESTABLISHED	Koneksi telah terbentuk dan aktif digunakan untuk komunikasi data. Ini adalah koneksi yang “normal” dan siap untuk transfer data dua arah.
SYN_SENT	Klien telah mengirim paket SYN ke server dan sedang menunggu balasan (SYN-ACK). Ini adalah tahap awal dari koneksi outbound (keluar).
SYN_RECV	Server telah menerima SYN dari klien, membalas dengan SYN-ACK, dan sedang menunggu ACK dari klien untuk menyelesaikan proses handshake.
FIN_WAIT1	Aplikasi telah menutup koneksi, dan sistem telah mengirim FIN (permintaan tutup koneksi) ke pihak lain.

State	Penjelasan
FIN_WAIT2	Setelah menerima ACK dari FIN pertama, sistem menunggu FIN dari pihak lawan.
TIME_WAIT	Koneksi ditutup, tapi sistem menunggu selama periode waktu tertentu (biasanya 2x waktu maksimum segment life) untuk memastikan semua paket terlambat tidak akan menyebabkan kebingungan.
CLOSE_WAIT	Server menerima FIN dari klien, dan menunggu aplikasinya untuk menutup koneksi juga.
CLOSING	Kedua sisi telah mengirim FIN, tapi belum semua ACK diterima.
LAST_ACK	Sistem telah mengirim FIN (balasan), menunggu ACK dari pihak lain sebelum sepenuhnya menutup koneksi.
CLOSED	Koneksi telah ditutup sepenuhnya, tidak ada komunikasi lebih lanjut.
LISTEN	Server menunggu koneksi masuk pada port tertentu (passive open). Biasanya terlihat pada server seperti web server, SSH, dll.

Contoh Alur Normal TCP (3-way handshake + closing)

Pembukaan koneksi:

1. Klien: `SYN_SENT`
2. Server: `SYN_RECV`
3. Keduanya: `ESTABLISHED`

Penutupan koneksi:

1. Pengirim: `FIN_WAIT1`
2. Penerima: `CLOSE_WAIT`
3. Pengirim: `FIN_WAIT2`
4. Penerima: `LAST_ACK`
5. Keduanya: `TIME_WAIT`
6. Akhir: `CLOSED`

Status yang Perlu Diwaspadai

- **SYN_RECV** banyak → kemungkinan *SYN flood attack*
- **TIME_WAIT** banyak → bisa akibat skrip web atau API client yang membuka-tutup koneksi terus-menerus
- **CLOSE_WAIT** menggantung → aplikasi Anda tidak menutup koneksi dengan benar (potensi memory leak)

Revisi #4
Dibuat 24 Juni 2025 21:25:21 oleh Friscia Anthony

Diperbaharui 12 Oktober 2025 00:14:58 oleh Friscia Anthony