CheatSheet 6: Utilizzo di `strace` per il Monitoraggio dei Socket

Laboratorio di Reti e Sistemi Distribuiti @ UniME

5 marzo 2025

Sommario

Il documento descrive l'utilizzo dello strumento `strace` per l'analisi delle operazioni sui socket attraverso il tracciamento delle system call.

1 Installazione

```
# Debian/Ubuntu
sudo apt install strace

# RHEL/Fedora/CentOS
sudo dnf install strace
```

2 System Call Principali per i Socket

Le principali system call da monitorare includono:

- `socket`: Creazione di nuovi socket
- `bind`: Associazione a indirizzi specifici
- `connect`: Connessione a socket remoti
- `send/recv`: Trasmissione e ricezione dati

3 Configurazione di `strace`

3.1 Tracciamento di Rete

```
strace -e trace=network -o output.log ./applicazione
```

3.2 Filtro Avanzato

```
strace -e trace=connect,accept,sendto,recvfrom -s 512 -v
```

4 Esempi di Analisi

4.1 Connessione TCP

```
connect(3, {sa_family=AF_INET, sin_port=htons(80),
sin_addr=inet_addr("93.184.216.34")}, 16) = 0
```

Dove:

- `3`: File descriptor del socket
- `AF_INET`: Protocollo IPv4
- `93.184.216.34:80`: Indirizzo remoto

4.2 Monitoraggio in Tempo Reale

```
sudo strace -p $(pidof nginx) -e trace=network -y -s 1024
```

5 Interpretazione degli Output

La Tabella 1 riassume i codici d'errore comuni:

Tabella 1: Codici d'errore frequenti

Codice	**Significato**
EACCES	Permessi insufficienti
ECONNREFUSED	Connessione rifiutata
ETIMEDOUT	Timeout di connessione

6 Ottimizzazione

Per ridurre l'overhead:

- Limitare il tracciamento alle sole system call di rete
- Utilizzare l'opzione `-c` per statistiche aggregate
- Filtrare per PID specifici con `-p`