

# 20 strumenti da riga di comando indispensabili per monitorare le prestazioni di Linux

---

Essere un amministratore di sistema o di rete incaricato di monitorare e debuggare i problemi di prestazioni del sistema Linux su base giornaliera è una responsabilità immensamente impegnativa.

Richiede una dedizione incrollabile, una profonda comprensione dei sistemi Linux e un impegno costante per garantire prestazioni e affidabilità ottimali.

Dopo aver dedicato un decennio a lavorare come amministratore Linux nel settore IT, ho imparato ad apprezzare veramente l'arduo compito di monitorare e garantire il funzionamento continuo dei sistemi.

Alla luce di ciò, abbiamo curato un elenco completo dei 20 migliori strumenti di monitoraggio della riga di comando utilizzati di frequente. Questi strumenti inestimabili possono rivelarsi indispensabili per ogni amministratore di sistema Linux/Unix, consentendogli di monitorare, diagnosticare e mantenere in modo efficiente la salute e le prestazioni dei propri sistemi.

Questi strumenti di monitoraggio sono disponibili in tutte le versioni di **Linux** e possono essere utili per monitorare e trovare le cause effettive dei problemi di prestazioni. Questo elenco di comandi illustrato di seguito è sufficiente per scegliere quello adatto allo scenario di monitoraggio.

## 1. Top – Monitoraggio dei processi Linux

Linux **top** command è un programma di monitoraggio delle prestazioni che viene utilizzato frequentemente da molti amministratori di sistema per monitorare le prestazioni di Linux ed è disponibile in molti sistemi operativi **Linux/Unix-like**.

Il comando top viene utilizzato per visualizzare tutti i processi in esecuzione e attivi in tempo reale in un elenco ordinato e lo aggiorna regolarmente. Visualizza **l'utilizzo della CPU, l'utilizzo della memoria, la memoria di scambio, la dimensione della cache, la dimensione del buffer, il PID del processo, l'utente, i comandi** molto altro.

Mostra anche un elevato utilizzo della memoria e della CPU dei processi in esecuzione. Il comando top è molto utile per gli amministratori di sistema per monitorare e intraprendere azioni correttive quando necessario. Vediamo il comando top in azione.

```
# top
```

```
top - 09:49:45 up 4:55, 4 users, load average: 0.01, 0.02, 0.00
Tasks: 133 total, 1 running, 132 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 99.3 id, 0.0 wa, 0.3 hi, 0.3 si,
MiB Mem : 1070.8 total, 268.2 free, 253.5 used, 549.1 buff/ca
MiB Swap: 9216.0 total, 9174.0 free, 42.0 used. 648.0 avail M
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	C
37345	root	20	0	64512	4944	4064	R	0.3	0.5	0:00.07	t
1	root	20	0	264232	10916	7052	S	0.0	1.0	0:05.32	s
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	k
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	r
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	r
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	k
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	m
9	root	20	0	0	0	0	S	0.0	0.0	0:00.86	k
10	root	20	0	0	0	0	I	0.0	0.0	0:00.76	r
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	m
12	root	rt	0	0	0	0	S	0.0	0.0	0:00.02	w
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00	c
15	root	20	0	0	0	0	S	0.0	0.0	0:00.00	k
16	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	n
17	root	20	0	0	0	0	S	0.0	0.0	0:00.00	k
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	k
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	c
20	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	w
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00	k
22	root	25	5	0	0	0	S	0.0	0.0	0:00.00	k
23	root	39	19	0	0	0	S	0.0	0.0	0:00.37	k
24	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	c
25	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	k
26	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	k
27	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	t
28	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	m
29	root	0	-20	0	0	0	T	0.0	0.0	0:00.00	c

## 2. VmStat – Statistiche sulla memoria virtuale

Il comando **Linux VmStat** viene utilizzato per visualizzare le statistiche della **memoria virtuale**, **i thread del kernel**, **i dischi**, **i processi di sistema**, **i blocchi I/O**, **gli interrupt**, **l'attività della CPU** e molto altro.

Installa VmStat su Linux

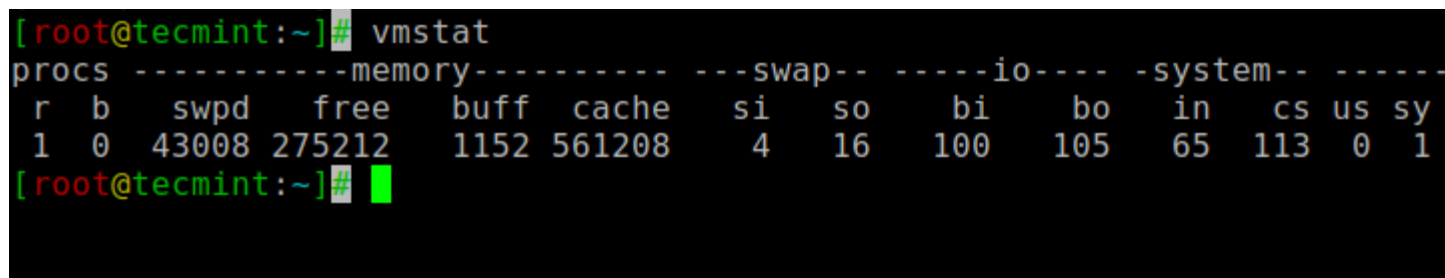
Per impostazione predefinita, il comando `vmstat` non è disponibile nei sistemi Linux: è necessario installare un pacchetto chiamato **sysstat** (un potente strumento di monitoraggio) che include un programma `vmstat`.

```
$ sudo yum install sysstat      [On Older CentOS/RHEL & Fedora]
sudo dnf install sysstat      [On CentOS/RHEL/Fedora/Rocky Linux & AlmaLinux]
sudo apt-get install sysstat  [On Debian/Ubuntu & Mint]
sudo pacman -S sysstat       [On Arch Linux]
```

L'uso comune del formato del comando `vmstat` è.

```
# vmstat
```

```
procs -----memory----- ---swap-- -----io----- -system-- -----cpu-----
 r  b  swpd  free  buff  cache   si   so   bi   bo   in   cs  us  sy  id  wa  st
 1  0  43008 275212  1152 561208    4   16  100  105   65  113  0   1  96  3   0
```



```
[root@tecmint:~]# vmstat
procs -----memory----- ---swap-- -----io----- -system-- -----
 r  b  swpd  free  buff  cache   si   so   bi   bo   in   cs  us  sy
 1  0  43008 275212  1152 561208    4   16  100  105   65  113  0  1
```

### 3. Lsof – Elenca i file aperti

Il **comando lsof** viene utilizzato in molti sistemi **Linux/Unix-like** per visualizzare un elenco di tutti i file e i processi aperti. I file aperti inclusi sono **file su disco, socket di rete, pipe, dispositivi e processi**.

Uno dei motivi principali per l'utilizzo di questo comando è quando un disco non può essere smontato e visualizza l'errore che i file vengono utilizzati o aperti. Con questo comando, puoi facilmente identificare quali file sono in uso.

Il formato più comune per **il comando lsof** è.

```
# lsof
```

COMMAND	PID	TID	TASKCMD	USER	FD	TYPE	DEVICE
systemd	1			root	cwd	DIR	8,2
224	128	/					
systemd	1			root	rtd	DIR	8,2
224	128	/					
systemd	1			root	txt	REG	8,2
1567768	134930842		/usr/lib/systemd/systemd				
systemd	1			root	mem	REG	8,2
2714928	134261052		/usr/lib64/libm-2.28.so				
systemd	1			root	mem	REG	8,2
628592	134910905		/usr/lib64/libudev.so.1.6.11				
systemd	1			root	mem	REG	8,2
969832	134261204		/usr/lib64/libsepol.so.1				



```
# tcpdump -i enp0s3
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:19:34.635893 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq
2840044824:2840045032, ack 4007244093
10:19:34.636289 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 208, win 11768,
options
10:19:34.873060 IP _gateway.57682 > tecmint.netbios-ns: NBT UDP PACKET(137): QUERY;
REQUEST; UNICAST
10:19:34.873104 IP tecmint > _gateway: ICMP tecmint udp port netbios-ns unreachable,
length 86
10:19:34.895453 IP _gateway.48953 > tecmint.netbios-ns: NBT UDP PACKET(137): QUERY;
REQUEST; UNICAST
10:19:34.895501 IP tecmint > _gateway: ICMP tecmint udp port netbios-ns unreachable,
length 86
10:19:34.992693 IP 142.250.4.189.https > 192.168.0.124.38874: UDP, length 45
10:19:35.010127 IP 192.168.0.124.38874 > 142.250.4.189.https: UDP, length 33
10:19:35.135578 IP _gateway.39383 > 192.168.0.124.netbios-ns: NBT UDP PACKET(137):
QUERY; REQUEST; UNICAST
10:19:35.135586 IP 192.168.0.124 > _gateway: ICMP 192.168.0.124 udp port netbios-ns
unreachable, length 86
10:19:35.155827 IP _gateway.57429 > 192.168.0.124.netbios-ns: NBT UDP PACKET(137):
QUERY; REQUEST; UNICAST
10:19:35.155835 IP 192.168.0.124 > _gateway: ICMP 192.168.0.124 udp port netbios-ns
unreachable, length 86
...
```

```
[root@tecmint:~]# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol deco
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 by
10:21:05.119045 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 284
10:21:05.128704 IP tecmint.47556 > _gateway.domain: 13517+ PTR? 159.0.16
10:21:05.128986 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq 1:
10:21:05.129152 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 209
10:21:05.134483 IP _gateway.domain > tecmint.47556: 13517 NXDomain 0/1/0
10:21:05.135404 IP tecmint.47761 > _gateway.domain: 3697+ PTR? 124.0.168
10:21:05.153782 IP _gateway.domain > tecmint.47761: 3697 NXDomain 0/1/0
10:21:05.154517 IP tecmint.52148 > _gateway.domain: 14980+ PTR? 1.0.168.
10:21:05.154762 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq 20
10:21:05.154948 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 417
10:21:05.157361 IP _gateway.domain > tecmint.52148: 14980 NXDomain 0/1/0
10:21:05.158060 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq 41
10:21:05.158401 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 161
10:21:05.158623 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq 16
10:21:05.158823 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 198
10:21:05.159003 IP tecmint.ssh > 192.168.0.124.45611: Flags [P.], seq 19
10:21:05.159138 IP 192.168.0.124.45611 > tecmint.ssh: Flags [.], ack 235
```

## 5. Netstat – Statistiche di rete

**netstat** è uno strumento a riga di comando per monitorare le statistiche dei pacchetti di rete **in entrata** e **in uscita**, nonché le statistiche dell'interfaccia. È uno strumento

molto utile per ogni amministratore di sistema per monitorare le prestazioni della rete e risolvere i problemi relativi alla rete.

```
# netstat -a | more
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp      0      0 tecmint:domain        0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:ssh            0.0.0.0:*               LISTEN
tcp      0      0 localhost:postgres    0.0.0.0:*               LISTEN
tcp      0      0 tecmint:ssh           192.168.0.124:45611    ESTABLISHED
tcp6     0      0 [::]:sunrpc           [::]:*                  LISTEN
tcp6     0      0 [::]:ssh               [::]:*                  LISTEN
tcp6     0      0 localhost:postgres    [::]:*                  LISTEN
udp      0      0 0.0.0.0:mdns           0.0.0.0:*               *
udp      0      0 localhost:323          0.0.0.0:*               *
udp      0      0 tecmint:domain        0.0.0.0:*               *
udp      0      0 0.0.0.0:bootps        0.0.0.0:*               *
udp      0      0 tecmint:bootpc        _gateway:bootps        ESTABLISHED
...
```

```
[root@tecmint:~]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         Stat
tcp      0      0 0.0.0.0:sunrpc          0.0.0.0:*               LIST
tcp      0      0 tecmint:domain        0.0.0.0:*               LIST
tcp      0      0 0.0.0.0:ssh            0.0.0.0:*               LIST
tcp      0      0 localhost:postgres    0.0.0.0:*               LIST
tcp      0      0 tecmint:ssh           192.168.0.124:45611    ESTA
tcp6     0      0 [::]:sunrpc           [::]:*                  LIST
tcp6     0      0 [::]:ssh               [::]:*                  LIST
tcp6     0      0 localhost:postgres    [::]:*                  LIST
udp      0      0 0.0.0.0:mdns           0.0.0.0:*               *
udp      0      0 localhost:323          0.0.0.0:*               *
udp      0      0 tecmint:domain        0.0.0.0:*               *
udp      0      0 0.0.0.0:bootps        0.0.0.0:*               *
udp      0      0 tecmint:bootpc        _gateway:bootps        ESTA
```

Mentre al giorno d'oggi netstat è stato deprecato a favore del comando ss, è ancora possibile scoprire netstat nel proprio toolkit di rete.

## 6. Htop – Monitoraggio dei processi Linux

**htop** è uno strumento di monitoraggio dei processi Linux interattivo e in tempo reale molto avanzato, che è molto simile al **comando top di Linux** ma ha alcune funzionalità ricche come **un'interfaccia user-friendly per gestire i processi, tasti di scelta rapida, viste verticali e orizzontali dei processi** e molto altro.

```
# htop
```



Per impostazione predefinita, il comando **iotop** non è disponibile in Linux ed è necessario installarlo come mostrato.

```
$ sudo yum install iotop          [On Older CentOS/RHEL & Fedora]
sudo dnf install iotop          [On CentOS/RHEL/Fedora/Rocky Linux & AlmaLinux]
sudo apt-get install iotop      [On Debian/Ubuntu & Mint]
sudo pacman -S iotop           [On Arch Linux]
```

L'uso comune del formato del comando iotop è.

```
# iotop
```

Total DISK READ :		0.00 B/s		Total DISK WRITE :		0.00 B/s	
Actual DISK READ:		0.00 B/s		Actual DISK WRITE:		0.00 B/s	
TID	PRIO	USER	DISK READ	DISK WRITE	SWAPIN	IO>	COMMAND
1	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	systemd --
2	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kthreadd]
3	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_gp]
4	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_par_g
6	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kworker/0
8	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[mm_percpu
9	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[ksoftirqd
10	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_sched
11	rt/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[migration
12	rt/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[watchdog/
13	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[cpuhp/0]
15	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kdevtmpfs
16	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[netns]
17	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kauditd]
18	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[khungtask
19	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[oom_reape
20	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[writeback
21	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kcompactd
22	be/5	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[ksmd]
23	be/7	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[khugepage
24	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[crypto]
25	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kintegrit
26	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kblockd]

## 8. Iostat – Statistiche di input/output

**IOSTAT** è uno strumento semplice che raccoglierà e mostrerà le statistiche del dispositivo di archiviazione **di input** e **output** del sistema. Questo strumento viene spesso utilizzato per tenere traccia dei problemi di prestazioni dei dispositivi di archiviazione, inclusi **dispositivi**, **dischi locali** e **dischi remoti** come **NFS**.

Installa Iostat su Linux

Per ottenere il comando **iostat**, è necessario installare un pacchetto chiamato **sysstat** come mostrato.

```
$ sudo yum install sysstat      [On Older CentOS/RHEL & Fedora]
sudo dnf install sysstat      [On CentOS/RHEL/Fedora/Rocky Linux & AlmaLinux]
sudo apt-get install sysstat  [On Debian/Ubuntu & Mint]
sudo pacman -S sysstat       [On Arch Linux]
```

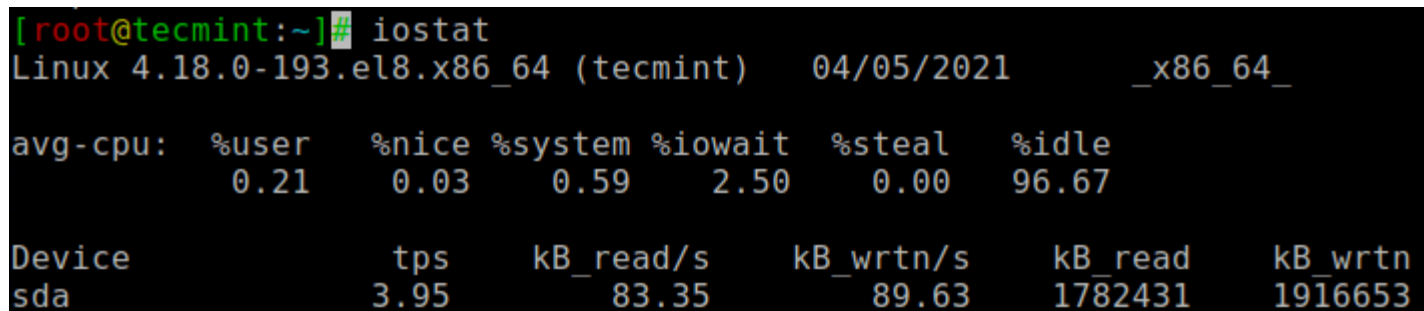
L'uso comune del formato del comando iostat è.

```
# iostat
```

```
Linux 4.18.0-193.el8.x86_64 (tecmint)  04/05/2021    _x86_64_      (1 CPU)
```

```
avg-cpu:  %user  %nice %system %iowait  %steal   %idle
           0.21   0.03   0.59   2.50    0.00   96.67
```

```
Device            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda                 3.95         83.35         89.63     1782431     1916653
```



```
[root@tecmint:~]# iostat
Linux 4.18.0-193.el8.x86_64 (tecmint)  04/05/2021    _x86_64_

avg-cpu:  %user  %nice %system %iowait  %steal   %idle
           0.21   0.03   0.59   2.50    0.00   96.67

Device            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda                 3.95         83.35         89.63     1782431     1916653
```

## 9. IPTraf – Monitoraggio LAN IP in tempo reale

**IPTraf** è un'utilità di monitoraggio della rete in tempo reale (**IP LAN**) open source basata su console per **Linux**. Raccoglie una serie di informazioni, ad esempio il monitoraggio del traffico IP che passa sulla rete, tra cui le informazioni sui flag TCP, i dettagli ICMP, le suddivisioni del traffico TCP/UDP, i pacchetti di connessione TCP e il conteggio dei byte.

Raccoglie inoltre informazioni sulle statistiche generali e dettagliate dell'interfaccia di TCP, UDP, IP, ICMP, non-IP, errori di checksum IP, attività dell'interfaccia, ecc.



```
[root@tecmint:~]# ac
total 18.77
[root@tecmint:~]# ac -d
Jul 4 total 0.24
Today total 18.54
[root@tecmint:~]# ac -p
osboxes 6.26
tecmint 2.47
root 10.05
total 18.78
[root@tecmint:~]# ac tecmint
total 2.47
[root@tecmint:~]# ac -d tecmint
Today total 2.47
[root@tecmint:~]# █
```

## 11. Monit – Monitoraggio dei processi e dei servizi Linux

**Monit** è un'utilità gratuita di supervisione dei processi open source e basata sul Web che monitora e gestisce automaticamente i processi di sistema, i programmi, i file, le directory, le autorizzazioni, i checksum e i file system.

Monitora servizi come Apache, MySQL, Mail, FTP, ProFTP, Nginx, SSH e così via. Lo stato del sistema può essere visualizzato dalla riga di comando o utilizzando la propria interfaccia web.

Monit: tecmint x +

← → ↻ Not secure | 192.168.0.159:2812/tecmint

Home > tecmint Use [M/Monit](#) to manage all your Monit instances

## System status

Parameter	Value
Name	tecmint
Status	OK
Monitoring status	Monitored
Monitoring mode	active
On reboot	start
Load average	[0.00] [0.02] [0.00]
Cpu	0.0%us 0.1%sy 0.0%wa
Memory usage	223.7 MB [20.9%]
Swap usage	41.8 MB [0.5%]
Uptime	6h 30m
Boot time	Mon, 05 Apr 2021 04:53:55
Data collected	Mon, 05 Apr 2021 11:24:03

[Disable monitoring](#)

Copyright © 2001-2019 [Tildeslash](#). All rights reserved. [Monit web site](#) | [Monit Wiki](#) | [M/Monit](#)

Per l'installazione e la configurazione, leggi il nostro articolo - Come installare e configurare il programma Monit (Linux Process and Services Monitoring).

## 12. NetHogs – Monitoraggio della larghezza di banda della rete per processo

**NetHogs** è un piccolo programma open-source (simile al **comando superiore** di Linux) che tiene sotto controllo ogni attività di rete del processo sul tuo sistema. Tiene inoltre traccia della larghezza di banda del traffico di rete in tempo reale utilizzata da ciascun programma o applicazione.

```
# nethogs
```

```
NetHogs version 0.8.5
```

PID	USER	PROGRAM	DEV	SENT	RECEIVED
37256	root	sshd: root@pts/0	enp0s3	0.180	0.000
?	root	..2.168.0.159:2812-192.16		0.000	0.000
?	root	unknown TCP		0.000	0.000
TOTAL				0.180	0.000

Per l'installazione e l'utilizzo, leggi il nostro articolo: [Monitora la larghezza di banda della rete Linux utilizzando NetHogs](#)

### 13. iftop – Monitoraggio della larghezza di banda della rete

**iftop** è un'altra utility di monitoraggio del sistema open source gratuita basata su terminale che visualizza un elenco aggiornato frequentemente dell'utilizzo della larghezza di banda di rete (host di origine e di destinazione) che passa attraverso l'interfaccia di rete del sistema.

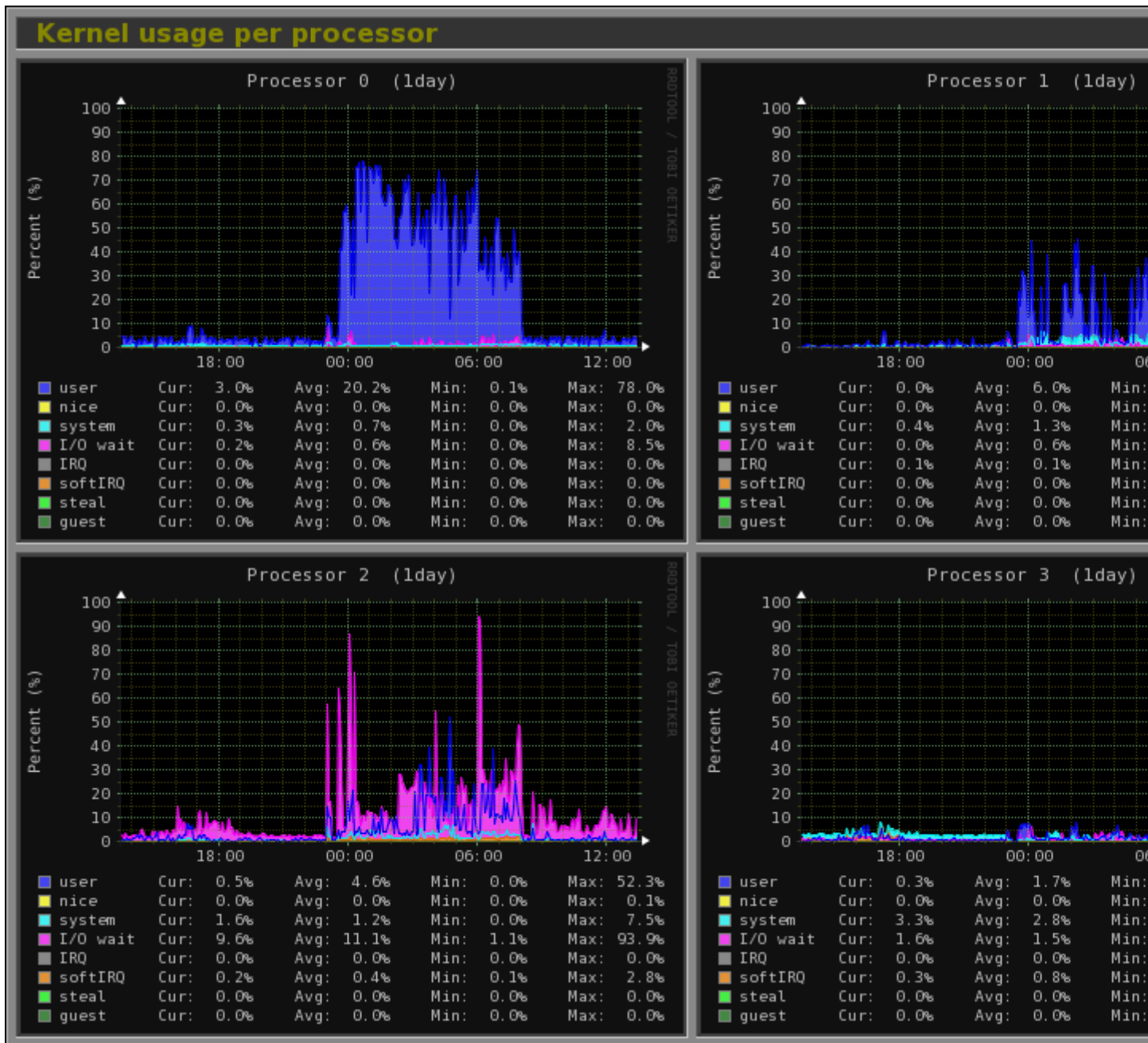
**iftop** è analogo a **'top'** nel contesto dell'utilizzo della rete, proprio come **'top'** fornisce informazioni sull'utilizzo della CPU.

**iftop** appartiene alla stimata famiglia "top" di strumenti di monitoraggio della rete. Progettato specificamente per osservare un'interfaccia di rete selezionata dall'utente, esegue il rendering dei dati in tempo reale sull'utilizzo corrente della larghezza di banda tra due host specificati.

```
# iftop
```



È progettato per monitorare le prestazioni complessive del sistema e aiuta a rilevare guasti, colli di bottiglia, attività anomale, ecc.



Per l'installazione e l'utilizzo, leggi il nostro articolo: [Monitorix uno strumento di monitoraggio del sistema e della rete per Linux](#)

### 15. Arpwatch – Monitoraggio dell'attività Ethernet

**Arpwatch** è un tipo di programma progettato per monitorare la risoluzione degli indirizzi (modifiche degli indirizzi **MAC** e **IP**) del traffico **di rete Ethernet** su una rete Linux.

Tiene costantemente d'occhio il traffico Ethernet e produce un registro delle modifiche alle coppie di indirizzi **IP** e **MAC** insieme a un timestamp su una rete. Ha anche una funzione per inviare avvisi e-mail agli amministratori, quando viene aggiunto o modificato un abbinamento. È molto utile per rilevare lo spoofing **ARP** su una rete.

```
[root@tecmint:~]# arpwatch -i enp0s3
[root@tecmint:~]# tail -f /var/log/messages
Apr  5 11:40:42 osboxes systemd[1]: Started Network Manager Script Dispa
rvice.
Apr  5 11:42:33 osboxes systemd[1]: Started /usr/bin/systemctl start man
e-update.
Apr  5 11:42:33 osboxes systemd[1]: Starting man-db-cache-update.service
Apr  5 11:42:33 osboxes systemd[1]: Reloading.
Apr  5 11:42:48 osboxes kernel: device enp0s3 entered promiscuous mode
Apr  5 11:42:48 osboxes arpwatch[41055]: listening on enp0s3
Apr  5 11:42:52 osboxes systemd[1]: Started man-db-cache-update.service.
Apr  5 11:43:00 osboxes arpwatch[41055]: new station 192.168.0.1 98:da:c
4c
Apr  5 11:43:00 osboxes arpwatch[41055]: new station 192.168.0.124 38:b1
8:c7
Apr  5 11:43:05 osboxes arpwatch[41055]: new station 192.168.0.159 08:00
```

Per l'installazione e l'utilizzo, leggi il nostro articolo: Arpwatch per monitorare l'attività Ethernet

#### 16. Suricata – Monitoraggio della sicurezza della rete

**Suricata** è un **sistema di monitoraggio** della **sicurezza di rete** e della prevenzione delle **intrusioni** open source ad alte prestazioni per **Linux**, **FreeBSD** e **Windows**.

È stato progettato e di proprietà di una fondazione senza scopo di lucro, **OISF (Open [Information Security](#) Foundation)**.

Per l'installazione e l'utilizzo, leggi il nostro articolo: Suricata – Un sistema di rilevamento e prevenzione delle intrusioni di rete

#### 17. VnStat PHP – Monitoraggio della larghezza di banda della rete

**VnStat PHP** è un'applicazione frontend basata sul web per lo strumento di rete più popolare chiamato "**vnstat**". **VnStat PHP monitora l'utilizzo** del traffico di rete in modalità grafica.

Visualizza l'utilizzo totale del traffico di rete **IN** e **OUT** in report di **riepilogo orario, giornaliero, mensile** e **completo**.

Per l'installazione e l'utilizzo, leggi il nostro articolo: Monitoraggio dell'utilizzo della larghezza di banda della rete

## 18. Nagios – Monitoraggio di rete/server

Nagios è un potente sistema di monitoraggio open source leader del settore che consente agli amministratori di rete/sistema di identificare e risolvere i problemi relativi al server prima che influiscano sui principali processi aziendali.

Con il sistema Nagios, gli amministratori possono monitorare Linux, Windows, switch, router e stampanti remoti su un'unica finestra. Mostra avvisi critici e indica se qualcosa è andato storto nella rete/server, il che aiuta indirettamente l'utente ad avviare i processi di correzione prima che si verifichino.

Per l'installazione, la configurazione e l'utilizzo, leggi il nostro articolo - Installa il sistema di monitoraggio Nagios per monitorare gli host Linux/Windows remoti

## 19. Nmon: Monitora le prestazioni di Linux

**Nmon** (acronimo di Nigel's Performance Monitor), che viene utilizzato per monitorare tutte le risorse Linux come CPU, memoria, utilizzo del disco, rete, processi principali, NFS, kernel e molto altro. Questo strumento è disponibile in due modalità: Modalità online e Modalità di acquisizione.

La modalità online viene utilizzata per il monitoraggio in tempo reale e la modalità di acquisizione viene utilizzata per archiviare l'output in formato CSV per un'elaborazione successiva.



```

Terminal
16  4 1068 2403  0  0  0  0  3  19  1  10
48  1 1081 1862  0  0  0  0  2  7  0  6
70  1 1138 2556  0  0 120 10  1  2  0  2
50  3 1001 3042  0  0  0  0  0  0  0  0
28  5  938 2799  0  0  0  0  1  1  0  1
33  3 1119 3213 572 32  12  3 20 27  4 34
36  2 1191 3534  12  3 176  3 48 48  4 43
35  7 1351 4495 1392 17 388 26 10 25  4 32
29  5 1327 5127 1384 21  0  0 114 89  6 66
17  5  808 1415  0  0 276  3  1  1  0  1
29  3  804 1285  0  0  0  0  1  2  0  2
23  2  799 1136  0  0  0  0  2  8  1  7
16  2  769 1177  0  0 348 26  1  1  0  1
35  6 1053 4322  52  7  0  0  1  2  0  3
#<-----CPU-----><-----Disks-----><-----Network----->
#cpu sys inter  ctxsw KRead  Reads KBWrit Writes  KBin  PktIn  KOut  PktOut
19  2  927 2352  0  0  0  0  1  4  1  7
22  5  926 2177  0  0  0  0  1  1  0  1
34  6 1261 4487  0  0 136  3  1  5  3  6
18  2 1022 2103  0  0 1164 159  1  5  1  7
27  4 1024 2742  0  0  0  0  1  7  1  7
20  4  844 1699  0  0  72  2  1  1  0  1
16  3  854 2093  0  0  4  1  3 12  0  5

```

Per l'installazione e l'utilizzo, leggi il nostro articolo: [Installa lo strumento Collectl \(All-in-One Performance Monitoring\) in Linux](#)

Vorremmo sapere che tipo di **programmi di monitoraggio** utilizzate per **monitorare le prestazioni dei vostri server Linux**. Se ci siamo persi uno strumento importante che vorresti includere in questo elenco, ti preghiamo di informarci tramite commenti e non dimenticare di condividerlo.