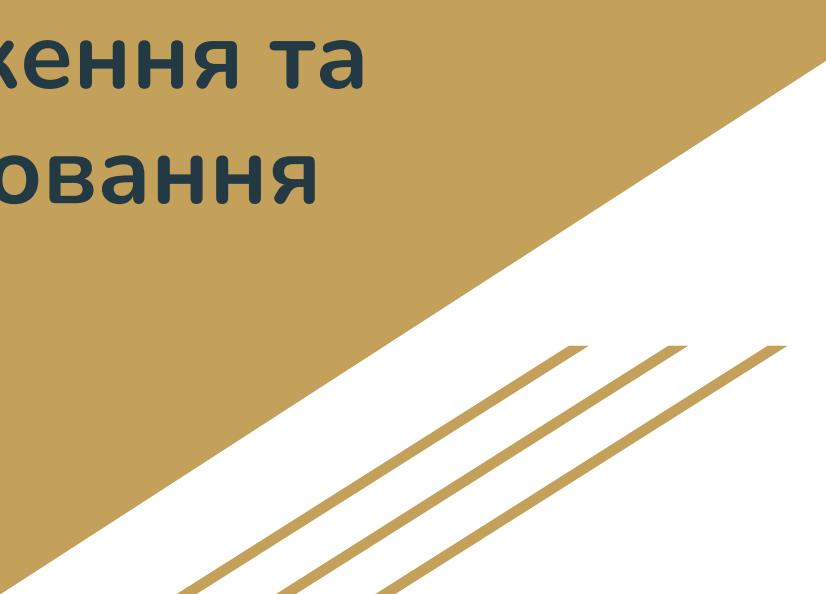




Моніторинг ОС, налагодження та журналювання



Інструменти командного рядка для моніторингу продуктивності Linux

Кожному системному чи мережевому адміністратору справді дуже важко щоденно контролювати та усувати проблеми продуктивності системи Linux. Я склав список часто використовуваних інструментів моніторингу командного рядка, які можуть бути корисними для кожного системного адміністратора Linux/Unix. Ці команди доступні в усіх версіях Linux і можуть бути корисними для моніторингу та пошуку фактичних причин проблеми з продуктивністю. Цього списку команд, наведеної тут, цілком достатньо, щоб вибрати ту, яка підходить для вашого сценарію моніторингу та налагодження.

Топ – Моніторинг процесів Linux

Команда Linux Top — це програма моніторингу продуктивності, яка часто використовується багатьма системними адміністраторами для моніторингу продуктивності Linux і доступна для багатьох операційних систем, подібних до Linux/Unix. Верхня команда використовується для відображення всіх запущених і активних процесів у реальному часі в упорядкованому списку та регулярно оновлює його. Він відображає використання процесора, використання пам'яті, пам'ять підкачки, розмір кешу, розмір буфера, PID процесу, користувача, команди та багато іншого. Він також показує високе використання пам'яті та ЦП запущеними процесами. Верхня команда є дуже корисною для системного адміністратора, щоб контролювати та вживати правильних дій, коли потрібно. Давайте подивимося на дію верхньої команди.

```
# top
```

VmStat – Статистика віртуальної пам'яті

Команда Linux VmStat використовується для відображення статистики віртуальної пам'яті, потоків ядра, дисків, системних процесів, блоків вводу/виводу, переривань, активності процесора та багато іншого. За замовчуванням команда vmstat недоступна в системах Linux, вам потрібно встановити пакет під назвою sysstat, який містить програму vmstat. Загальним

```
# vmstat

procs -----memory----- --swap-- -----io---- --system-- -----cpu-----
 r b    swpd   free  inact active   si   so    bi    bo   in   cs us sy id wa st
 1 0      0 810420  97380  70628    0    0   115     4   89   79   1   6 90   3   0
```

Lsof – Список відкритих файлів

Команда Lsof використовується в багатьох системах, подібних до Linux/Unix, і використовується для відображення списку всіх відкритих файлів і процесів. Відкриті файли включають дискові файли, мережеві сокети, канали, пристрой та процеси. Однією з головних причин використання цієї команди є те, що диск неможливо відмонтувати та відображається повідомлення про помилку, що файли використовуються або відкриваються. За допомогою цієї команди ви можете легко визначити, які файли використовуються. Найпоширеніший формат цієї команди:

```
# lsof
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
init	1	root	cwd	DIR	104,2	4096	2	/
init	1	root	rtd	DIR	104,2	4096	2	/
init	1	root	txt	REG	104,2	38652	17710339	/sbin/init
init	1	root	mem	REG	104,2	129900	196453	/lib/ld-2.5.so
init	1	root	mem	REG	104,2	1693812	196454	/lib/libc-2.5.so
init	1	root	mem	REG	104,2	20668	196479	/lib/libdl-2.5.so
init	1	root	mem	REG	104,2	245376	196419	/lib/libsep01.so.1
init	1	root	mem	REG	104,2	93508	196431	/lib/libselinux.so.1
init	1	root	10u	FIFO	0,17		953	/dev/initctl

Tcpdump – Аналізатор мережевих пакетів

Tcpdump — одна з найпоширеніших мережевих аналізаторів пакетів командного рядка або програма аналізу пакетів, яка використовується для захоплення або фільтрування пакетів TCP/IP, отриманих або переданих через певний інтерфейс через мережу. Він також надає можливість зберігати захоплені пакети у файлі для подальшого аналізу. tcpdump доступний майже у всіх основних дистрибутивах Linux.

```
# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
22:08:59.617628 IP tecmint.com.ssh > 115.113.134.3.static-mumbai.vsnl.net.in.28472: P 2532133365:2532133481(116) ack 3561562349 win 9648

22:09:07.653466 IP tecmint.com.ssh > 115.113.134.3.static-mumbai.vsnl.net.in.28472: P 116:232(116) ack 1 win 9648

22:08:59.617916 IP 115.113.134.3.static-mumbai.vsnl.net.in.28472 > tecmint.com.ssh: . ack 116 win 64347
```

Netstat – Статистика мережі

Netstat — це інструмент командного рядка для моніторингу статистики вхідних і вихідних мережевих пакетів, а також статистики інтерфейсу. Це дуже корисний інструмент для кожного системного адміністратора для моніторингу продуктивності мережі та усунення проблем, пов'

```
# netstat -a | more

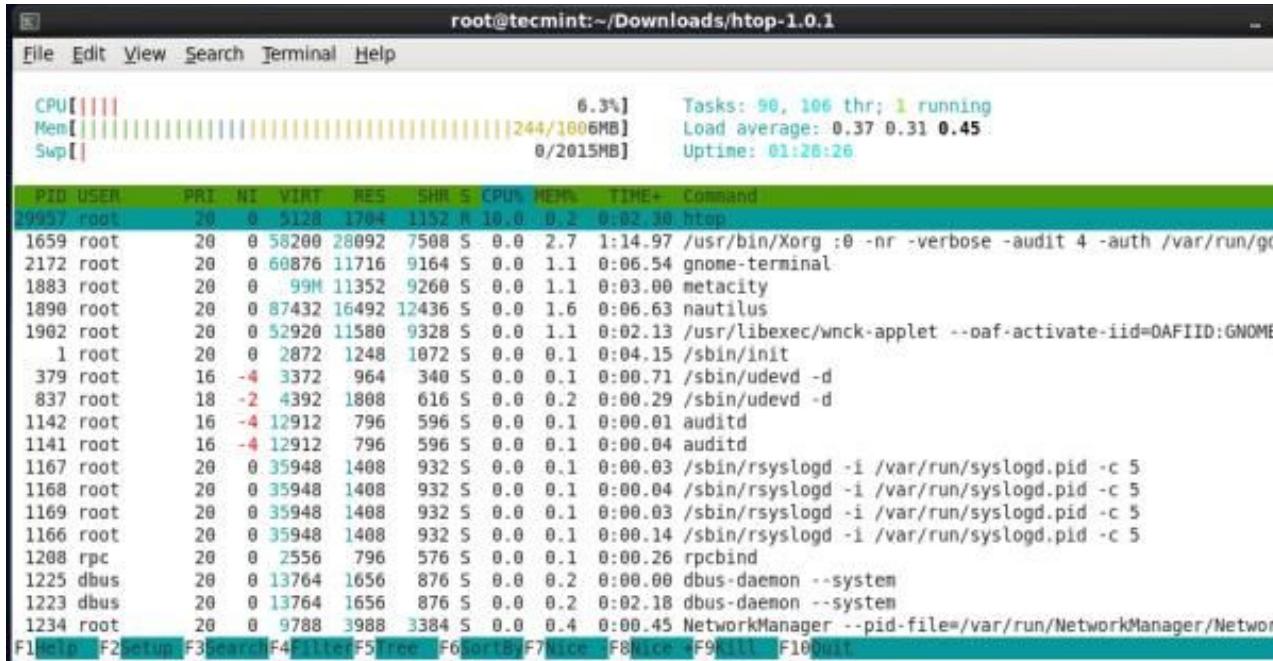
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 *:mysql                  *:*
tcp      0      0 *:sunrpc                 *:*
tcp      0      0 *:realm-rusd            *:*
tcp      0      0 *:ftp                   *:*
tcp      0      0 localhost.localdomain:ipp  *:*
tcp      0      0 localhost.localdomain:smtp *:*
tcp      0      0 localhost.localdomain:smtp localhost.localdomain:42709 TIME_WAIT
tcp      0      0 localhost.localdomain:smtp localhost.localdomain:42710 TIME_WAIT
tcp      0      0 *:http                  *:*
tcp      0      0 *:ssh                   *:*
tcp      0      0 *:https                *:*
```

Htop – Моніторинг процесів Linux

Htop – це вдосконалений інтерактивний інструмент моніторингу процесів Linux у реальному часі. Це дуже схоже на верхню команду Linux, але має деякі багаті функції, такі як зручний інтерфейс для керування процесом, комбінації клавіш, вертикальний і горизонтальний перегляд процесів і багато іншого. Htop є стороннім інструментом і не входить до систем Linux, вам потрібно встановити його за допомогою інструмента керування пакетами YUM. Щоб дізнатися більше про встановлення, прочитайте нашу статтю нижче.

```
# htop
```

Нtop – Моніторинг процесів Linux



iotop – Монітор дискового вводу-виводу Linux

iotop також багато в чому схожий на команду top і програму Htop, але він має функцію обліку для моніторингу та відображення дискового введення-виведення та процесів у реальному часі. Цей інструмент дуже корисний для пошуку точного процесу та читання/запису процесів на диск, який часто використовується.

```
# iotop
```

Total DISK READ: 0.00 B/s Total DISK WRITE: 0.00 B/s							
TID	PRIo	USER	DISK READ	DISK WRITE	SWAPIN	IO>	COMMAND
20869	be/4	mongod	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mongod -f /etc/mongod.conf
23239	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	konqueror -mimetype-ctory file:///root
7183	be/4	ubersvn	0.00 B/s	0.00 B/s	0.00 %	0.00 %	java -Djava.util.concurrent.ThreadPoolExecutor.CORE_POOL_SIZE=10 -jar /opt/ubersvn/ubersvn.jar
1805	be/3	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[cnic_wq]
1812	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[bnx2i thread/0]
7125	be/4	ubersvn	0.00 B/s	0.00 B/s	0.00 %	0.00 %	java -Djava.util.concurrent.ThreadPoolExecutor.CORE_POOL_SIZE=10 -jar /opt/ubersvn/ubersvn.jar
7152	be/4	ubersvn	0.00 B/s	0.00 B/s	0.00 %	0.00 %	java -Djava.util.concurrent.ThreadPoolExecutor.CORE_POOL_SIZE=10 -jar /opt/ubersvn/ubersvn.jar
25635	be/4	clamav	0.00 B/s	0.00 B/s	0.00 %	0.00 %	clamd
9160	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	perl /usr/libexec/bmin/miniserv.conf
18100	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	automount
8406	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	squid -D
31923	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	Xvnc :1 -desktop ~ -rfbport 5901 -pn
32127	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mm-applet --sm-disable
2125	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	xulrunner-bin ./application.ini
8355	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	crond
32168	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	gconfd-2 7
25636	be/4	clamav	0.00 B/s	0.00 B/s	0.00 %	0.00 %	clamd
31932	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	sh /usr/bin/startkde
1965	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	klauncher [kdeinit] --new-startup
2064	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	bt-applet --sm-disable
32125	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	bt-applet --sm-disable
2146	be/4	apache	0.00 B/s	0.00 B/s	0.00 %	0.00 %	php-fpm: pool www
8478	be/4	xymon	0.00 B/s	0.00 B/s	0.00 %	0.00 %	hobbitd_channel --og hobbitd_history
13846	be/4	mysql	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mysqld --basedir=/b/mysql/mysql.sock
30015	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	(ncsa auth) /etc/squid/passwd
32091	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	kdeinit Running...
13831	be/4	mysql	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mysqld --basedir=/b/mysql/mysql.sock
13832	be/4	mysql	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mysqld --basedir=/b/mysql/mysql.sock
13833	be/4	mysql	0.00 B/s	0.00 B/s	0.00 %	0.00 %	mysqld --basedir=/b/mysql/mysql.sock

lostat – Статистика введення/виведення

IoStat — це простий інструмент, який збирає та показує статистику системного введення та виводу пристрій зберігання. Цей інструмент часто використовується для відстеження проблем продуктивності пристрій зберігання даних, включаючи пристрій, локальні диски, віддалені

```
# iostat
```

```
Linux 2.6.18-238.9.1.el5 (tecmint.com)          09/13/2012

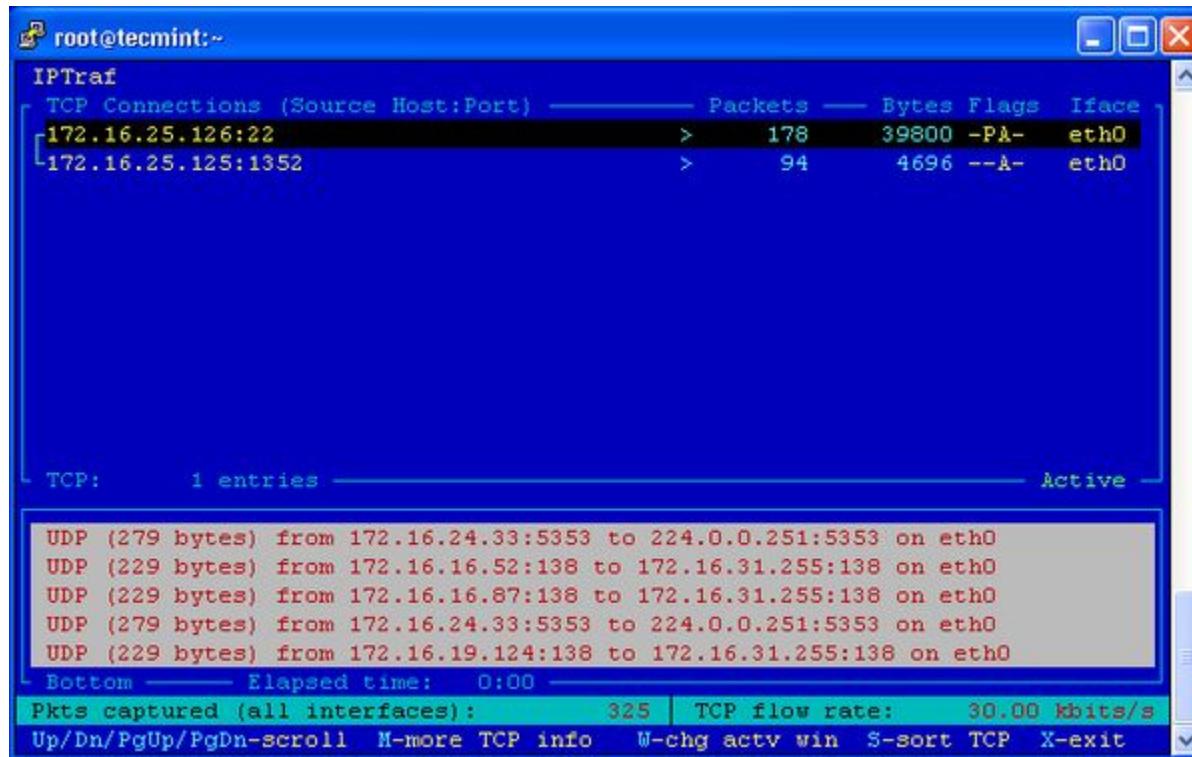
avg-cpu: %user   %nice %system %iowait  %steal   %idle
          2.60    3.65   1.04    4.29    0.00   88.42

Device:    tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
cciss/c0d0     17.79      545.80      256.52  855159769  401914750
cciss/c0d0p1     0.00       0.00       0.00      5459      3518
cciss/c0d0p2     16.45      533.97      245.18  836631746  384153384
cciss/c0d0p3     0.63       5.58       3.97     8737650    6215544
cciss/c0d0p4     0.00       0.00       0.00        8        0
cciss/c0d0p5     0.63       3.79       5.03    5936778    7882528
cciss/c0d0p6     0.08       2.46       2.34    3847771    3659776
```

IPTraf – Моніторинг IP LAN у реальному часі

IPTraf — це утиліта для моніторингу мережі в режимі реального часу (IP LAN) з відкритим вихідним кодом на основі консолі для Linux. Він збирає різноманітну інформацію, таку як монітор IP-трафіку, який проходить через мережу, включаючи інформацію про пропори TCP, деталі ICMP, збої трафіку TCP/UDP, пакети TCP-з'єднання та одиничні підрахунки. Він також збирає інформацію про загальну та детальну статистику інтерфейсу TCP, UDP, IP, ICMP, не-IP, помилки контролальної суми IP, активність інтерфейсу тощо.

IPTraf – Моніторинг IP LAN у реальному часі



Psacct or Acct – Моніторинг активності користувача

Інструменти psacct або acct дуже корисні для моніторингу активності кожного користувача в системі. Обидва демони працюють у фоновому режимі та уважно спостерігають за загальною діяльністю кожного користувача в системі, а також за тим, які ресурси вони споживають.

Ці інструменти дуже корисні для системних адміністраторів, щоб відстежувати діяльність кожного користувача, наприклад, що вони роблять, які команди вони видають, скільки ресурсів ними використовується, як довго вони активні в системі тощо.

Monit – Моніторинг процесів і служб Linux

Monit — це безкоштовна веб-утиліта з відкритим вихідним кодом для контролю процесів, яка автоматично відстежує та керує системними процесами, програмами, файлами, каталогами, дозволами, контрольними сумами та файловими системами.

Він відстежує такі служби, як Apache, MySQL, Mail, FTP, ProFTP, Nginx, SSH тощо. Статус системи можна переглянути з командного рядка або за допомогою власного веб-інтерфейсу.

Monit – Моніторинг процесів і служб Linux

The screenshot shows a web browser window displaying the Monit Service Manager interface at <http://www.tecmint.com>. The page title is "tecmin.com Monit". The main content area displays system and process monitoring information.

System Monitoring:

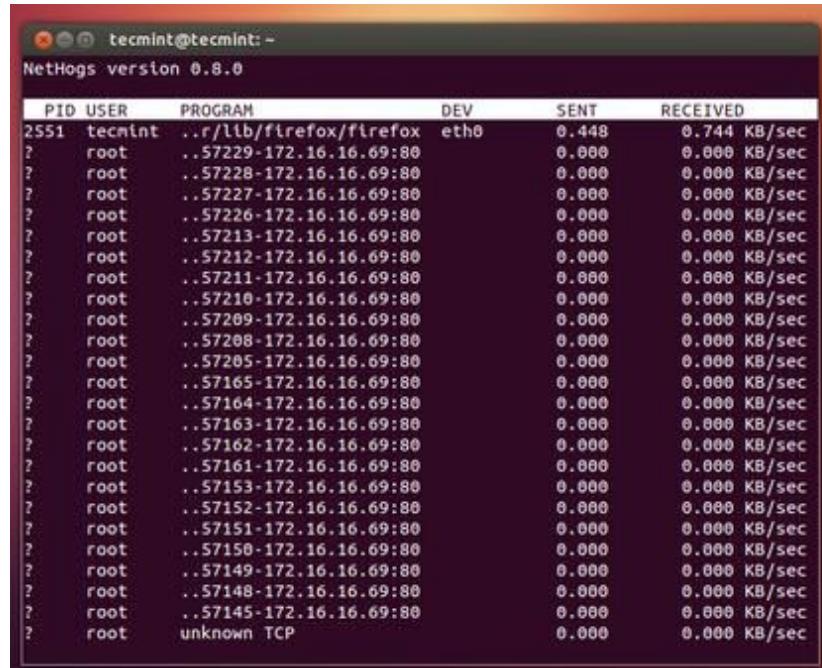
System	Status	Load	CPU	Memory
tecmint.com	running	[0.10] [0.07] [0.04]	5.0%us, 0.9%sy, 0.9%wa	34.6% [354012 kB]

Process Monitoring:

Process	Status	Uptime	CPU	Memory
sshd	running	1d 2h 42m	0.0%	0.06% [636 kB]
mysqld	running	1d 2h 42m	0.4%	2.8% [29068 kB]
proftpd	running	23m	0.0%	0.1% [1748 kB]

NetHogs – Контроль пропускної здатності мережі для кожного процесу

NetHogs — це гарна невелика програма з відкритим вихідним кодом (схожа на верхню команду Linux), яка відстежує мережеву активність кожного процесу у вашій системі. Вона також відстежує пропускну здатність мережі в режимі реального часу, яку використовує кожна програма чи додаток.



The screenshot shows a terminal window titled "tecmint@tecmint: ~" running the command "NetHogs version 0.8.0". The output displays a table of network usage statistics:

PID	USER	PROGRAM	DEV	SENT	RECEIVED
2551	tecmint	..r/lib/firefox/firefox	eth0	0.448	0.744 KB/sec
?	root	..57229-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57228-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57227-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57226-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57213-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57212-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57211-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57210-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57209-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57208-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57205-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57165-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57164-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57163-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57162-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57161-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57153-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57152-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57151-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57150-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57149-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57148-172.16.16.69:80		0.000	0.000 KB/sec
?	root	..57145-172.16.16.69:80		0.000	0.000 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec

iftop – Моніторинг пропускної здатності мережі

iftop – це ще одна термінальна безкоштовна утиліта моніторингу системи з відкритим вихідним кодом, яка відображає часто оновлюваний список використання пропускної здатності мережі (хости джерела та призначення), що проходить через мережевий інтерфейс вашої системи.

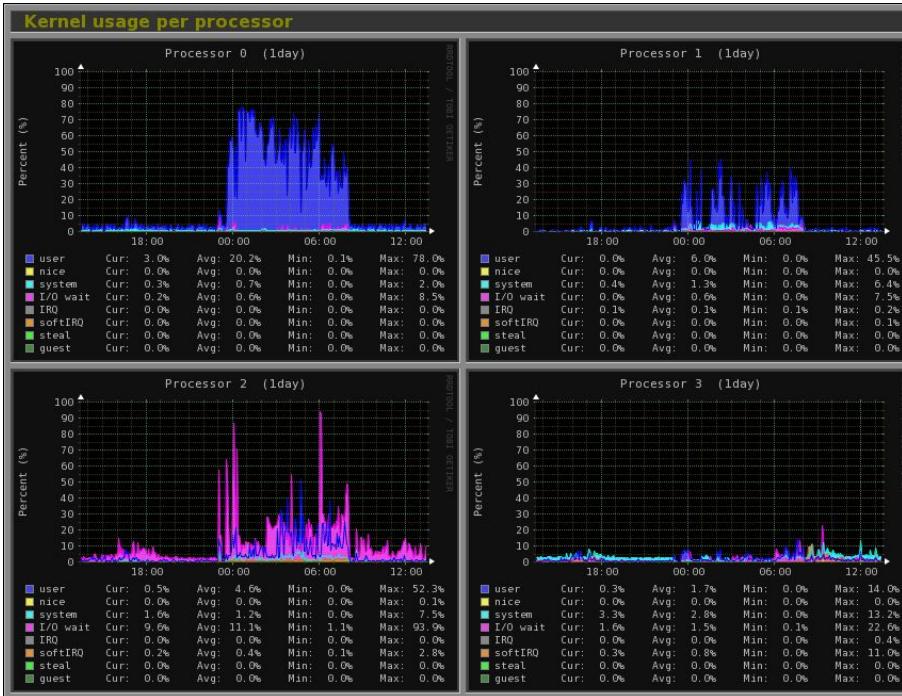
якщо top розглядається для використання мережі, що «top» робить для використання ЦП. iftop – це «верхній» сімейний інструмент, який відстежує вибраний інтерфейс і відображає поточне використання пропускної здатності між двома хостами.

172.16.25.126	=>	172.16.25.125	2.67Kb	2.84Kb	2.84Kb
	<=		160b	240b	240b
172.16.25.126	=>	mddc-01.midcorp.mid-d	284b	861b	861b
	<=		592b	1.50Kb	1.50Kb
172.16.31.255	=>	172.16.23.185	0b	0b	0b
	<=		0b	240b	240b
172.16.31.255	=>	172.16.22.152	0b	0b	0b
	<=		0b	229b	229b
172.16.31.255	=>	wsus.midcorp.mid-day.	0b	0b	0b
	<=		0b	229b	229b
172.16.31.255	=>	172.16.21.79	0b	0b	0b
	<=		916b	229b	229b
172.16.31.255	=>	172.16.18.159	0b	0b	0b
	<=		0b	156b	156b
255.255.255.255	=>	172.16.18.9	0b	0b	0b
	<=		0b	68b	68b
TX:		cumulative:	3.68KB	peak:	rates:
RX:			2.93KB	4.84Kb	2.93Kb
TOTAL:			6.60KB	9.34Kb	4.58Kb
				6.60Kb	6.60Kb

Monitorix – моніторинг системи та мережі

Monitorix – це безкоштовна легка утиліта, розроблена для запуску та моніторингу якомога більшої кількості системних і мережевих ресурсів на серверах Linux/Unix. Він має вбудований веб-сервер HTTP, який регулярно збирає інформацію про систему та мережу та відображає їх у вигляді графіків. Він відстежує середнє завантаження системи та використання, розподіл пам'яті, стан драйвера диска, системні служби, мережеві порти, статистику пошти (Sendmail, Postfix, Dovecot тощо), статистику MySQL та багато іншого. Він призначений для моніторингу загальної продуктивності системи та допомагає виявляти збої, вузькі місця, ненормальну діяльність тощо.

Monitorix – моніторинг системи та мережі



Arpwatch – монітор активності Ethernet

Arpwatch — це свого роду програма, призначена для моніторингу розпізнавання адрес (зміни MAC- та IP-адрес) мережевого трафіку Ethernet у мережі Linux. Він постійно стежить за трафіком Ethernet і створює журнал змін пар IP- і MAC-адрес разом із часовими мітками в мережі. Він також має функцію надсилання сповіщень електронною поштою адміністратору про додавання чи зміну пари. Це дуже корисно для виявлення ARP-спуфінгу в мережі.

Suricata – моніторинг безпеки мережі

Suricata — це високопродуктивна система безпеки мережі з відкритим вихідним кодом, виявлення та запобігання вторгненням для Linux, FreeBSD і Windows. Вона розроблена та належить некомерційній організації OISF (Фонд відкритої інформаційної безпеки).

VnStat PHP – моніторинг пропускної здатності мережі

VnStat PHP — веб-інтерфейс програми для найпопулярнішого мережевого інструменту під назвою «vnstat». VnStat PHP відстежує використання мережевого трафіку в чудовому графічному режимі. Він відображає загальне використання мережевого трафіку IN і OUT у погодинному, щоденному, місячному та повному зведеному звіті.

Nagios – моніторинг мережі/сервера

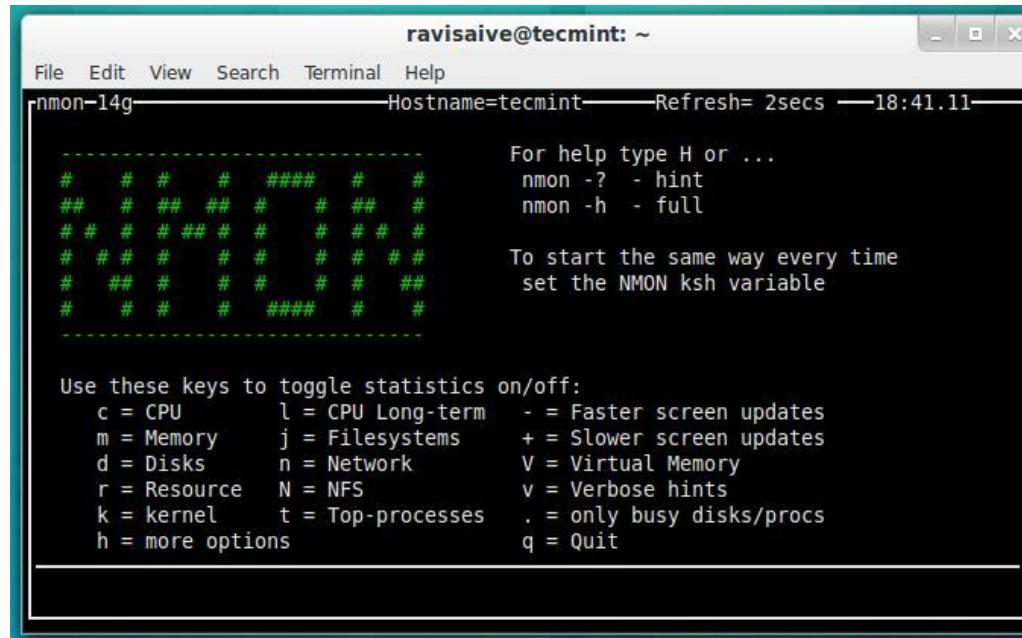
Nagios — це провідна потужна система моніторингу з відкритим кодом, яка дозволяє мережевим/системним адміністраторам виявляти та вирішувати проблеми, пов'язані з сервером, перш ніж вони вплинути на основні бізнес-процеси. За допомогою системи Nagios адміністратори можуть контролювати віддалені Linux, Windows, комутатори, маршрутизатори та принтери в одному вікні. Він показує критичні попередження та вказує, якщо щось пішло не так у вашій мережі/сервері, що опосередковано допомагає вам розпочати процеси виправлення, перш ніж вони відбудуться.

Nmon: моніторинг продуктивності Linux

Інструмент Nmon (розшифровується як монітор продуктивності Найджела), який використовується для моніторингу всіх ресурсів Linux, таких як процесор, пам'ять, використання диска, мережа, основні процеси, NFS, ядро та багато іншого. Цей інструмент доступний у двох режимах: режим онлайн і режим захоплення.

Онлайн-режим використовується для моніторингу в реальному часі, а режим захоплення використовується для збереження вихідних даних у форматі CSV для подальшої обробки.

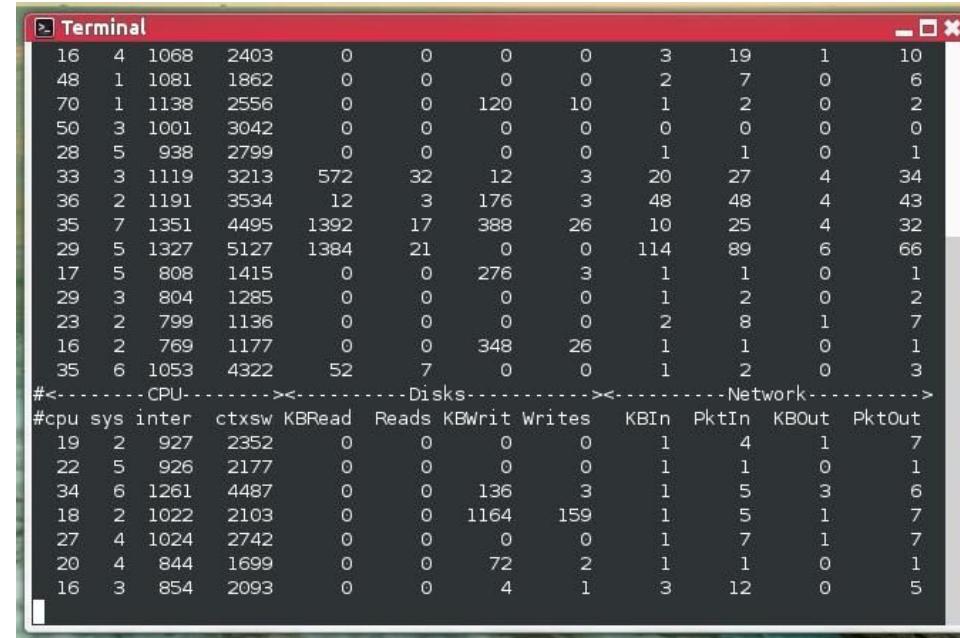
Nmon: моніторинг продуктивності Linux



Collectl: універсальний інструмент моніторингу продуктивності

Collectl — це ще одна потужна та багатофункціональна утиліта на основі командного рядка, яку можна використовувати для збору інформації про системні ресурси Linux, такі як використання процесора, пам'ять, мережа, inodes, процеси, nfs, tcp, сокети та багато іншого.

Collectl: універсальний інструмент моніторингу продуктивності



The screenshot shows a terminal window titled "Terminal" displaying performance monitoring data from the Collectl tool. The data is presented in three main sections: CPU, Disks, and Network.

CPU Data:

CPU	sys	inter	ctxsw	KBRead	Reads	KBWrite	Writes	KBIn	PktIn	KBOut	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

Disks Data:

CPU	sys	inter	ctxsw	KBRead	Reads	KBWrite	Writes	KBIn	PktIn	KBOut	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

Network Data:

CPU	sys	inter	ctxsw	KBRead	Reads	KBWrite	Writes	KBIn	PktIn	KBOut	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

/proc

/proc — віртуальна файлова система. Наприклад, якщо ви виконаете `ls -l /proc/stat`, ви помітите, що він має розмір 0 байтів, але якщо ви виконали «`cat /proc/stat`», ви побачите певний вміст у файлі.

Виконайте `ls -l /proc`, і ви побачите багато каталогів лише з числами. Ці числа представляють ідентифікатори процесів, файли в цьому пронумерованому каталозі відповідають процесу з цим конкретним PID.

Нижче наведено важливі файли, розташовані в кожному пронумерованому каталозі (для кожного процесу):

- `cmdline` – командний рядок команди.
- `environ` – змінні середовища.
- `fd` – містить дескриптори файлів, які пов'язані з відповідними файлами.
- `limits` – містить інформацію про конкретні обмеження для процесу.
- `mounts` – монтування відповідної інформації

Нижче наведено важливі посилання під кожним пронумерованим каталогом (для кожного процесу):

- `cwd` – Посилання на поточний робочий каталог процесу.
- `exe` – Посилання на виконуваний файл процесу.
- `root` – Посилання на кореневий каталог процесу.

Керування користувачами

Додавання облікових записів користувачів

Щоб додати новий обліковий запис користувача, ви можете виконати будь-яку з наступних двох команд від імені користувача root.

```
# adduser [new_account]  
# useradd [new_account]
```

Коли новий обліковий запис користувача додається до системи, виконуються наступні операції.

1. Створено його/її домашній каталог (/home/username за замовчуванням).
2. Наступні приховані файли копіюються в домашній каталог користувача та використовуватимуться для надання змінних середовища для його/її сеансу користувача.
 3. Поштовий спул створюється для користувача в /var/spool/mail/username.
 4. Створюється група, якій присвоюється таке саме ім'я, як і новому обліковому запису користувача.

```
.bash_logout  
.bash_profile  
.bashrc
```

Додавання облікових записів користувачів: Розуміння /etc/passwd

Повна інформація про обліковий запис зберігається у файлі /etc/passwd. Цей файл містить записи для кожного облікового запису користувача системи та має такий формат (поля

```
[username]:[x]:[UID]:[GID]:[Comment]:[Home directory]:[Default shell]
```

Поля [ім'я користувача] і [Коментар] не пояснюються.

- Х у другому полі означає, що обліковий запис захищено захищеним паролем (у /etc/shadow), який потрібен для входу як [ім'я користувача].
- Поля [UID] і [GID] є цілими числами, які представляють ідентифікатор користувача та ідентифікатор основної групи, до якої належить [ім'я користувача] відповідно.
- [Домашній каталог] вказує абсолютний шлях до домашнього каталогу [ім'я користувача], і
- [Оболонка за замовчуванням] — це оболонка, яка стане доступною для цього користувача, коли він або вона ввійде в систему.

Додавання облікових записів користувачів: Розуміння /etc/group

Інформація про групу зберігається у файлі /etc/group. Кожен запис має такий формат.

```
[Group name]:[Group password]:[GID]:[Group members]
```

- [Group name] - назва групи.
- X у [Group password] означає, що групові паролі не використовуються.
- [GID]: те саме, що в /etc/passwd.
- [Group members]: відокремлений комами список користувачів, які є членами [Group name].

Додавання облікових записів користувачів: Розуміння /etc/group

```
[gacanepa@dev1 ~]$ grep gacanepa /etc/passwd  
gacanepa:x:1000:1000:Gabriel Cánepa:/home/gacanepa:/bin/bash  
[gacanepa@dev1 ~]$ grep gacanepa /etc/group  
gacanepa:x:1000:gacanepa  
[gacanepa@dev1 ~]$
```

<http://www.tecmint.com>

Після додавання облікового запису ви можете редагувати наступну інформацію (щоб назвати кілька полів) за допомогою команди usermod, основний синтаксис якої такий.

```
# usermod [options] [username]
```

Додавання облікових записів користувачів: Розуміння /etc/group

Встановлення терміну дії облікового запису

Використовуйте позначку –expiredate, за якою слідує дата у форматі PPPP-ММ-ДД.

```
# usermod --expiredate 2014-10-30 tecmint
```

Використовуйте комбіновані параметри -aG або –append –groups, після яких розділений комами список груп.

```
# usermod --append --groups root,users tecmint
```

Додавання облікових записів користувачів: Розуміння /etc/group

Зміна стандартного розташування домашнього каталогу користувача

Використовуйте параметри -d або –home, а потім абсолютний шлях до нового домашнього

```
# usermod --home /tmp tecmint
```

Зміна оболонки, яку користувач використовуватиме за замовчуванням

Рішкюсторуйте –shell, а потім шлях до нової оболонки.

```
# usermod --shell /bin/sh tecmint
```

Додавання облікових записів користувачів: Розуміння /etc/group

Відображення груп, до яких входить користувач

```
# groups tecmint  
# id tecmint
```

Тепер давайте виконаємо всі наведені вище команди за один раз.

```
# usermod --expiredate 2014-10-30 --append --groups root,users --home /tmp --shell /bin/sh tecmint
```

Додавання облікових записів користувачів: Розуміння /etc/group

```
[root@dev1 ~]# adduser tecmint
[root@dev1 ~]# usermod --expiredate 2014-10-30 --append --groups root,users --home /tmp --shell /bin/sh tecmint
[root@dev1 ~]# finger tecmint
Login: tecmint          Name:      The finger command is used to look up information for an account
Directory: /tmp           Shell: /bin/sh
Never logged in.
No mail.
No Plan.
[root@dev1 ~]# groups tecmint
tecmint : tecmint root users
[root@dev1 ~]# id tecmint
uid=1001(tecmint) gid=1001(tecmint) groups=1001(tecmint),0(root),100(users)
[root@dev1 ~]#
```

The groups utility prints the names of the groups an user is in, whereas the id command also prints the corresponding UID and GIDs of those groups.

У наведеному вище прикладі ми встановимо термін дії облікового запису користувача tecmint до 30 жовтня 2014 року. Ми також додамо обліковий запис до кореневої групи та групи користувачів. Нарешті, ми встановимо sh як оболонку за замовчуванням і змінимо розташування домашнього каталогу на /tmp:

Додавання облікових записів користувачів: Розуміння /etc/group

Для наявних облікових записів ми також можемо зробити наступне.

Відключення облікового запису за допомогою пароля

Використовуйте параметр -L (великий регистр L) або параметр –lock, щоб заблокувати пароль користувача.

```
# usermod --lock tecmint
```

Розблокування пароля користувача

Використовуйте параметр –u або –unlock, щоб розблокувати пароль користувача, який раніше був заблокований.

```
# usermod --unlock tecmint
```

Додавання облікових записів користувачів: Розуміння /etc/group

```
[root@dev1 ~]# usermod --lock tecmint → root locks the password for user tecmint
[root@dev1 ~]# exit → root logs off
logout
[gacanepa@dev1 ~]$ su tecmint → User gacanepa tries to logon as tecmint. Since the
Password:                                password is locked, the authentication fails
su: Authentication failure
[gacanepa@dev1 ~]$ su - → User gacanepa logs in as root
Password:
Last login: Tue Oct 28 13:38:35 ART 2014 on pts/0
[root@dev1 ~]# usermod --unlock tecmint → root unlocks the password for user tecmint
[root@dev1 ~]# exit → root logs off
logout
[gacanepa@dev1 ~]$ su tecmint → User gacanepa logs in as tecmint
Password:
sh-4.2$ █ → The authentication succeeds and a command prompt is shown
```

Додавання облікових записів користувачів: Розуміння /etc/group

Створення нової групи для читання та запису файлів, доступ до яких має мати декілька користувачів

Виконайте наступну серію команд, щоб досягти мети.

```
# groupadd common_group # Add a new group  
# chown :common_group common.txt # Change the group owner of common.txt to common_group  
# usermod -aG common_group user1 # Add user1 to common_group  
# usermod -aG common_group user2 # Add user2 to common_group  
# usermod -aG common_group user3 # Add user3 to common_group
```

Додавання облікових записів користувачів: Розуміння /etc/group

Видалення групи

Ви можете видалити групу за допомогою такої команди.

```
# groupdel [group_name]
```

Якщо є файли, власником яких є group_name, їх не буде видалено, але власником групи буде встановлено GID групи, яку було видалено.

Права доступу до файлів Linux

Окрім основних дозволів на читання, запис і виконання, які ми обговорювали в Інструменти архівування та налаштування атрибутів файлів – Частина 3 цієї серії, існують інші менш використовувані (але не менш важливі) налаштування дозволів, які іноді називають «спеціальними дозволами».

Як і базові дозволи, які обговорювалися раніше, вони встановлюються за допомогою вісімкового файлу або за допомогою літери (symbolічного позначення), яка вказує на тип дозволу.

Видалення облікових записів користувачів

Ви можете видалити обліковий запис (разом із його домашнім каталогом, якщо він належить користувачеві, і всіма файлами, що містяться в ньому, а також спулом пошти) за допомогою команди userdel із параметром `--remove`.

```
# userdel --remove [username]
```

Управління групою

Щоразу, коли до системи додається новий обліковий запис користувача, створюється група з такою ж назвою, єдиним учасником якої є ім'я користувача. Пізніше до групи можна додати інших користувачів. Однією з цілей груп є реалізація простого контролю доступу до файлів та інших системних ресурсів шляхом встановлення правильних дозволів на ці ресурси.

Наприклад, припустимо, що у вас є такі користувачі.

- користувач1 (основна група: користувач1)
- користувач2 (основна група: користувач2)
- користувач3 (основна група: користувач3)

Усім їм потрібен доступ для читання та запису до файлу під назвою common.txt, розташованого десь у вашій локальній системі або, можливо, у мережевому ресурсі, який створив user1. У вас може виникнути спокуса

```
# chmod 660 common.txt  
OR  
# chmod u=rw,g=rw,o= common.txt [notice the space between the last equal sign and the file name]
```

Однак це надасть доступ для читання та запису лише власнику файлу та тим користувачам, які є членами групи власників файлу (user1 у цьому випадку). Знову ж таки, у вас може виникнути спокуса додати користувачів2 і користувач3 до групи user1, але це також надасть їм доступ до решти файлів, які належать користувачам user1 і групі user1.

Розуміння Setuid

Коли дозвіл setuid застосовується до виконуваного файлу, користувач, який запускає програму, успадковує ефективні привілеї власника програми. Оскільки такий підхід може викликати занепокоєння щодо безпеки, кількість файлів із дозволом setuid має бути мінімальною.

Ймовірно, ви знайдете програми з таким набором дозволів, коли користувачеві системи потрібно отримати доступ до файлу, що належить root.

Підводячи підсумок, йдеться не лише про те, що користувач може виконувати двійковий файл, але й про те, що він може робити це з правами root. Наприклад, давайте перевіримо дозволи /bin/passwd. Цей двійковий файл використовується для зміни пароля облікового запису та змінює файл /etc/shadow. Суперкористувач може змінити будь-який пароль, але всі інші користувачі повинні мати можливість змінювати лише свій.

```
[root@dev1 ~]# ls -l /bin/passwd
-rwsr-xr-x. 1 root root 27832 Jun 10 03:27 /bin/passwd
[root@dev1 ~]# This s stands for setuid
```

<http://www.tecmint.com>

Розуміння Setuid

Таким чином, будь-який користувач повинен мати дозвіл на запуск /bin/passwd, але лише root зможе вказати обліковий запис. Інші користувачі можуть змінювати лише відповідні паролі.

```
[gacanepa@dev1 ~]$ passwd tecmint
passwd: Only root can specify a user name.
[gacanepa@dev1 ~]$ passwd
Changing password for user gacanepa.
Changing password for gacanepa.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[gacanepa@dev1 ~]$ █
```

Розуміння Setuid

Коли встановлено біт setgid, ефективний GID справжнього користувача стає ідентифікатором власника групи. Таким чином, будь-який користувач може отримати доступ до файлу з привілеями, наданими власнику групи такого файла. Крім того, коли для каталогу встановлено біт setgid, новостворені файли успадковують ту саму групу, що й каталог, а новостворені підкаталоги також успадковують біт setgid батьківського каталогу. Ви, швидше за все, використовуватимете цей підхід щоразу, коли членам певної групи потрібен доступ до всіх

```
# chmod g+s [filename]
```

Щоб встановити setgid у вісімковій формі, додайте число 2 перед поточними (або бажаними) базовими дозволами.

```
# chmod 2755 [directory]
```

Розуміння Setuid

Встановлення SETGID у каталозі

```
[root@dev1 ~]# ls -l  
total 0  
drwxr-xr-x. 3 root root 21 Oct 29 22:47 backups  
[root@dev1 ~]# chmod g+s backups  
[root@dev1 ~]# ls -l  
total 0  
drwxr-sr-x. 3 root root 21 Oct 29 22:47 backups  
[root@dev1 ~]# mkdir backups/testdir  
[root@dev1 ~]# ls -ld backups/testdir  
drwxr-sr-x. 2 root root 6 Oct 29 22:48 backups/testdir  
[root@dev1 ~]# █
```

The setgid is applied to a directory (the g stands for 'group' and the s stands for 'setgid'). In other words, the setgid is a permission that only applies to groups.

Newly created directories inherit the setgid bit from the parent directory.

Розуміння Sticky Bit

Коли для файлів встановлено «*липкий біт*», Linux просто ігнорує його, тоді як для каталогів це запобігає користувачам видаляти або навіть перейменовувати файли, які містяться, якщо користувач не є власником каталогу, файлу або є адміністратором.

```
# chmod o+t [directory]
```

Щоб встановити sticky bit у вісімковій формі, додайте число 1 перед поточними (або бажаними) базовими дозволами.

```
# chmod 1755 [directory]
```

Розуміння Sticky Bit

Без закріпленого біта будь-хто, хто може писати в каталог, може видаляти або перейменовувати файли. З цієї причини закріплений біт зазвичай зустрічається в каталогах, таких як /tmp, які доступні для запису.

```
[root@dev1 ~]# ls -ld /tmp
drwxrwxrwt. 7 root root 108 Oct 30 08:59 /tmp
[root@dev1 ~]# exit
logout
[gacanepa@dev1 ~]$ touch /tmp/myfile
[gacanepa@dev1 ~]$ ls -lR /tmp
/tmp:
total 0
-rw-rw-r--. 1 gacanepa gacanepa 0 Oct 30 09:01 myfile
[gacanepa@dev1 ~]$ su tecmint
Password:
[tecmint@dev1 gacanepa]$ rm /tmp/myfile
rm: remove write-protected regular empty file '/tmp/myfile'? y
rm: cannot remove '/tmp/myfile': Operation not permitted
```

This t indicates that the sticky bit is set for /tmp
drwxrwxrwt. 7 root root 108 Oct 30 08:59 /tmp
root logs out and user gacanepa creates an empty file within /tmp.
gacanepa logs out and user tecmint attempts to delete the file.
Since the sticky bit is set for the parent directory, the delete operation fails.

Спеціальні атрибути файлів Linux

Існують інші атрибути, які дозволяють додатково обмежувати операції, дозволені з файлами. Наприклад, запобігти перейменуванню, переміщенню, видаленню чи навіть зміні файлу. Вони встановлюються за допомогою команди chattr і можуть переглядатися за допомогою інструменту lsattr, як показано нижче.

```
# chattr +i file1  
# chattr +a file2
```

Спеціальні атрибути файлів Linux

Після виконання цих двох команд файл1 буде незмінним (це означає, що його не можна переміщувати, перейменовувати, змінювати чи видаляти), тоді як файл2 перейде в режим лише додавання (можна відкрити лише в режимі додавання для запису).

```
[root@dev1 ~]# touch file1
[root@dev1 ~]# chattr +i file1
[root@dev1 ~]# lsattr file1
-----i----- file1
[root@dev1 ~]# rm file1
rm: remove regular empty file 'file1'? y
rm: cannot remove 'file1': Operation not permitted
[root@dev1 ~]# chattr -i file1
[root@dev1 ~]# lsattr file1
----- file1
[root@dev1 ~]# rm file1
rm: remove regular empty file 'file1'? y
[root@dev1 ~]# echo "Hi there" > file2
[root@dev1 ~]# chattr +a file2
[root@dev1 ~]# cat /dev/null > file2
-bash: file2: Operation not permitted
[root@dev1 ~]# echo "This is another line" >> file2
[root@dev1 ~]# cat file2
Hi there
This is another line
[root@dev1 ~]# lsattr file2
-----a----- file2
[root@dev1 ~]# chattr -a file2
[root@dev1 ~]# cat /dev/null > file2
```

When the immutable attribute is set for a file, not even root can delete it!

If we need to modify a file that has the immutable attribute set, we will have to remove the attribute first.

You cannot delete the contents of a file that has the append-only attribute set. However, you can append content to it.

You need to remove the append-only attribute if you need to delete some of the contents of the file.

Доступ до кореневого облікового запису та використання sudo

Одним із способів отримати доступ до кореневого облікового запису є введення.

```
$ su
```

а потім введіть пароль root.

Якщо автентифікація пройшла успішно, ви ввійдете в систему як root із поточним робочим каталогом, як і раніше. Якщо ви хочете, щоб вас було розміщено в домашньому каталозі root,

```
$ su -
```

а потім введіть пароль root.

Доступ до кореневого облікового запису та використання sudo

```
[gacanepa@dev1 ~]$ pwd  
/home/gacanepa  
[gacanepa@dev1 ~]$ su  
Password:  
[root@dev1 gacanepa]# pwd  
/home/gacanepa  
[root@dev1 gacanepa]# exit  
exit  
[gacanepa@dev1 ~]$ su -  
Password:  
Last login: [REDACTED] on pts/0  
[root@dev1 ~]# pwd  
/root  
[root@dev1 ~]# █
```

Доступ до кореневого облікового запису та використання sudo

Наведена вище процедура вимагає, щоб звичайний користувач знов пароль адміністратора, що становить серйозну загрозу безпеці. З цієї причини системний адміністратор може налаштовувати команду sudo, щоб дозволити звичайному користувачеві виконувати команди як інший користувач (зазвичай суперкористувач) у дуже контролюваній та обмежений спосіб. Таким чином, обмеження можуть бути встановлені для користувача, щоб дозволити йому виконувати одну або кілька конкретних привілейованих команд і ніяких інших.

Для автентифікації за допомогою sudo користувач використовує власний пароль. Після введення команди нам буде запропоновано ввести наш пароль (а не суперкористувача), і якщо автентифікація пройшла успішно (і якщо користувачеві було надано привілеї на виконання команди), зазначена команда буде виконана.

Щоб надати доступ до sudo, системний адміністратор повинен відредагувати файл /etc/sudoers. Рекомендується редагувати цей файл за допомогою команди visudo, а не відкривати його безпосередньо за допомогою текстового редактора.

```
# visudo
```

Доступ до кореневого облікового запису та використання sudo

Це відкриває файл /etc/sudoers за допомогою vim

Це найактуальніші рядки.

```
Defaults    secure_path="/usr/sbin:/usr/bin:/sbin"  
root       ALL=(ALL) ALL  
tecmint    ALL=/bin/yum update  
gacanepa   ALL=NOPASSWD:/bin/updatedb  
%admin     ALL=(ALL) ALL
```

Давайте розглянемо їх близче.

```
Defaults    secure_path="/usr/sbin:/usr/bin:/sbin:/usr/local/bin"
```

Цей рядок дозволяє вказати каталоги, які використовуватимуться для sudo, і використовується для запобігання використанню каталогів користувача, які можуть завдати шкоди системі.

Доступ до кореневого облікового запису та використання sudo

Наступні рядки використовуються для визначення дозволів.

```
root      ALL=(ALL)  ALL
```

- Перше ключове слово ALL вказує, що це правило застосовується до всіх хостів.
- Друге ALL вказує на те, що користувач у першому стовпці може виконувати команди з правами будь-якого користувача.
- Третє ALL означає, що будь-яка команда може бути виконана.

```
tecmint  ALL=/bin/yum update
```

Доступ до кореневого облікового запису та використання sudo

Якщо після знака = не вказано жодного користувача, sudo припускає користувача root. У цьому випадку користувач tecmint зможе запустити оновлення утм як root.

```
gасанера      ALL=NOPASSWD:/bin/updatedb
```

Директива **NOPASSWD** дозволяє користувачеві gасанера запускати */bin/updatedb* без необхідності вводити свій пароль.

```
%admin      ALL=(ALL)  ALL
```

Доступ до кореневого облікового запису та використання sudo

Знак % вказує на те, що цей рядок стосується групи під назвою «admin». Значення решти рядка таке ж, як і для звичайного користувача. Це означає, що члени групи «admin» можуть виконувати всі команди як будь-який користувач на всіх хостах.

Щоб побачити, які привілеї надає вам sudo, скористайтеся опцією «-l», щоб перелічити їх.

The screenshot shows two terminal sessions side-by-side, labeled 'Before' and 'After', illustrating the effect of adding a user to the sudoers file.

Before:

```
[gacanepa@dev1 root]$ sudo -l
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for gacanepa:
Sorry, user gacanepa may not run sudo on dev1.
[gacanepa@dev1 root]$
```

A blue arrow points downwards from the 'Before' terminal to the 'After' terminal, with the text "Before and after adding user gacanepa to the sudoers file" positioned below it.

After:

```
User gacanepa may run the following commands on this host:
(root) NOPASSWD: /bin/updatedb
```

Питання та відповіді