Linux (allgemein): Linux: geöffnete Dateien finden

Problem:

Bei Systemdiagnosen oder Problemen im laufenden Betrieb ist es Sinnvoll gewisse Zugriffe zu kontrollieren. Sobald es auf geöffnete Dateien, Sockets oder Ports geht hilft `lsof`.

Beispiele:

Erst brauchen wir eine kurze Übersetzung der Abkürzungen einer `lsof`-Ausgabe:

- `COMMAND`: Programmname (gekürzt)
- `PID`: die Nummer zur Prozessidentifikation
- `USER`: Besitzer der Prozesses
- `FD`: der Filedeskriptor
- `TYPE`: der Node-Typ
- `DEVICE`: die Device-Nummer
- `SIZE`: die Größe der Datei oder des Datei-Offsets in Bytes
- `NODE`: zeigt zum Beispiel die Inode oder das Protokoll an
- `NAME`: listet zusätzliche Informationen wie zum Beispiel den Dateinamen, Mountpoint oder die IP-Adressen bei einem Socket

Was hat ein Programm geöffnet?

```
# lsof -c init
COMMAND PID USER   FD   TYPE DEVICE    SIZE   NODE NAME
init      1 root  cwd    DIR    8,3    4096      2 /
init      1 root  rtd    DIR    8,3    4096      2 /
init      1 root  txt    REG    8,3   31432 666575 /sbin/init
init      1 root  mem    REG    8,3   90248 603264 /lib/ld-2.3.2.so
init      1 root  mem    REG    8,3 1244752 603269 /lib/libc-2.3.2.so
init      1 root   10u  FIFO    8,3         553865 /dev/initctl
```

Welche Programme hängen am SMTP-Port?

```
# lsof -i :25
COMMAND   PID    USER   FD   TYPE DEVICE SIZE NODE NAME
```

```
master   1120    root   11u  IPv4   2296       TCP *:smtp (LISTEN)
smtpd   18046 postfix    6u  IPv4   2296       TCP *:smtp (LISTEN)
smtpd   20629 postfix    6u  IPv4   2296       TCP *:smtp (LISTEN)
```

Welche Programme haben Logfiles geöffnet?

```
# lsof +D /var/log
COMMAND     PID     USER   FD   TYPE DEVICE    SIZE    NODE NAME
syslogd     693     root    2w   REG    8,6  667871  277451 /var/log/auth.log
syslogd     693     root    3w   REG    8,6 1752065  277442 /var/log/syslog
syslogd     693     root    7w   REG    8,6 1622736  277443 /var/log/mail.log
syslogd     693     root   10w   REG    8,6 1622580  277457 /var/log/mail.info
syslogd     693     root   11w   REG    8,6 1094180  277461 /var/log/mail.warn
syslogd     693     root   16w   REG    8,6   10477  277475 /var/log/debug
syslogd     693     root   17w   REG    8,6   14324  277487 /var/log/messages
clamd       726   clamav    3w   REG    8,6   11667 2301133 /var/log/clamav/clamav.log
freshclam   818   clamav    3wW  REG    8,6   59871 2301140
/var/log/clamav/freshclam.log
mysqld     3756    mysql   70w   REG    8,6  390551 1664663
/var/log/mysql/mysql-slow.log
snort     15341    snort    5w   REG    8,6  105968 2350082 /var/log/snort/alert
apache2   16211 www-data    2w   REG    8,6   76595  554911 /var/log/apache2/error.log
apache2   16211 www-data   77w   REG    8,6  161708  554892 /var/log/apache2/access.log
```

Weitere kurze Beispiele:

Anzeige aller Prozesse, die gerade auf Dateien zugreifen:

```
lsof
```

Anzeige aller Prozesse, die gerade auf die Datei "/usr/bin/vim" zugreifen (vi arbeiten):

```
lsof /usr/bin/vim
```

Anzeige aller Prozesse, die gerade auf die CD-ROM-Gerätedatei "/dev/hdc" zugreifen:

```
lsof /dev/hdc
```

Beenden aller Prozesse, die noch auf ein ins CD-ROM-Laufwerk eingelegtes Medium zugreifen:

```
kill $(lsof -t /cdrom)
```

Anzeige aller offenen Dateien des Prozesses mit der PID 2326:

```
lsof -p 2326
```

Anzeige aller offenen Dateien im Verzeichnis "/tmp" und seinen Unterverzeichnissen, ohne dabei auf symbolische Links zu achten:

```
lsof +D /tmp
```

Anzeige aller vom Benutzer "max" geöffneten Dateien:

```
lsof -u max
```

Anzeige aller offenen Dateien, die nicht der Benutzer "root" geöffnet hat:

```
lsof -u ^root
```

Anzeige einer ähnlichen Prozessliste wie `ps aux` durch Auflisten der Einträge mit Dateideskriptoreintrag "txt" statt der sonst üblichen Nummer ("txt" steht für Programmcode und Daten, also eine ausgeführte Datei):

```
lsof -d txt
```

Anzeige aller gelöschten Dateien, die noch geöffnet sind und daher Plattenplatz verbrauchen, aber in keinem Verzeichnis erscheinen (Dateien mit weniger als einem Link):

```
lsof +L1
```

Anzeige aller netzwerkrelevanten Dateien:

```
lsof -i
```

Anzeige aller netzwerkrelevanten Dateien, ohne die Portnummern als Dienstbezeichnung auszuschreiben und ohne die Hostnamen aufzulösen (daher deutlich performanter):

```
lsof -i -P -n
```

Anzeige aller IPv6-bezogenen Dateien:

```
lsof -i6
```

Anzeige aller aktiven Verbindungen:

```
lsof -i | grep '\->'
```

Anzeige aller derzeit vom Benutzer "www-data" geöffneten Netzwerkdateien (UND-Verknüpfung durch "-a"):

```
lsof -a -i -u www-data
```

Eindeutige ID: #1245
huschi
2008-02-07 10:33