

Squid Proxy log timestamp human readable / Convert and beautify Proxy unixtime logs in human-readable form howto

Author : admin

```
root@pcfreak:/home/hipo# tail -f /var/log/squid/access.log|ccze -CA
Feb 19 21:01:50 153 127.0.0.1 TCP_MISS_ABORTED/301 660 GET http://google.com/ - HIER_DIRECT/216.58.212.46 text/html
Feb 19 21:01:50 163 127.0.0.1 TCP_MISS/200 6253 GET http://www.google.com/ - HIER_DIRECT/216.58.206.196 text/html
Feb 19 21:02:11 401 127.0.0.1 TCP_MISS/200 10906 GET http://www.google.com/search? - HIER_DIRECT/216.58.206.196 text/html
Feb 19 21:02:32 0 127.0.0.1 TCP_MEM_HIT/301 667 GET http://google.com/ - HIER_NONE/- text/html
Feb 19 21:02:32 91 127.0.0.1 TCP_MISS/200 5917 GET http://www.google.com/ - HIER_DIRECT/216.58.206.196 text/html
Feb 19 21:02:43 691 127.0.0.1 TCP_MISS_ABORTED/302 434 GET http://lwn.net/ - HIER_DIRECT/45.33.94.129 text/plain
Feb 19 21:02:52 1052 127.0.0.1 TCP_MISS/200 16439 GET http://stallman.org/ - HIER_DIRECT/216.116.72.174 text/html
Feb 19 21:03:08 498 127.0.0.1 TCP_MISS/301 600 GET http://gnu.org/ - HIER_DIRECT/209.51.188.148 text/html
Feb 19 21:03:09 719 127.0.0.1 TCP_MISS/200 9586 GET http://www.gnu.org/ - HIER_DIRECT/209.51.188.148 text/html
Feb 19 21:03:15 573 127.0.0.1 TCP_MISS/200 8204 GET http://pravoslavieto.com/ - HIER_DIRECT/5.249.226.45 text/html
```

If you have installed Squid Cache Proxy recently and you need to watch who is accessing the proxy and what Internet (website is viewed) under `/var/log/squid/access.log /var/log/store.log /var/log/access.log` etc., you will be unpleasantly surprised the log's records are logged in a weird human unreadable format called UTC as **Squid Proxy server does not store the date / year / hour time information in a human readable format.**

Squid uses the format:

. and you have to be a robot of a kind or a math genius to read it :)

To display Squid Proxy log in a human readable, luckily you can use below one-liner regular expression.

```
cat access.log | perl -p -e 's/^\s*([0-9]*)/'["localtime($1)."]'/e'
```

If you have to review squid logs multiple times and on a regular basis you can either set some kind of cmd alias in `$HOME/.bashrc` such as:

```
alias readproxylog='cat access.log | perl -p -e 's/^\s*([0-9]*)/'["localtime($1)."]'/e'
```

Or for those who prefer beauty install and use a log beautifier / colorizer such as **ccze**

```
root@pcfreak:/home/hipo# apt-cache show ccze|grep -i desc -A 3
```

Description-en: robust, modular log coloriser

CCZE is a robust and modular log coloriser, with plugins for apm, exim, fetchmail, httpd, postfix, procmail, squid, syslog, ulogd, vsftpd, xferlog and more.

Description-md5: 55cd93dbcf614712a4d89cb3489414f6

Homepage: <https://github.com/madhouse/ccze>

Tag: devel::prettyprint, implemented-in::c, interface::commandline,
role::program, scope::utility, use::checking, use::filtering,

```
root@pcfreak:/home/hipo# apt-get install --yes ccze
```

```
tail -f /var/log/squid/access.log | ccze -CA
```

ccze is really nice to view `/var/log/syslog` errors and **make your daily sysadmin life a bit more colorful**

```
tail -f -n 200 /var/log/messages | ccze
```

```
1. hipo@pcfreak: ~ (ssh)
X hipo@pcfreak: ~ (ssh) %1 X bash %2
Feb 18 14:14:19 pcfreak mtp-probe: bus: 1, device: 5 was not an MTP device
Feb 18 14:14:24 pcfreak kernel: [4222213.697250] usb1p0: removed
Feb 18 14:14:24 pcfreak kernel: [4222213.700548] usb1p 1-1.1:1.0: usb1p0: USB Bidirectional printer d
ev 5 if 0 alt 0 proto 2 vid 0x04F9 pid 0x035B
Feb 18 14:14:24 pcfreak udev-configure-printer: Re-enabled printer ipp://localhost/printers/DCP1610W
Feb 18 14:14:36 pcfreak kernel: [4222225.412660] usb 1-1.1: USB disconnect, device number 5
Feb 18 14:14:36 pcfreak kernel: [4222225.414385] usb1p0: removed
Feb 18 14:14:36 pcfreak udev-configure-printer: Disabled printer ipp://localhost/printers/DCP1610W as
the corresponding device was unplugged or turned off
Feb 18 14:27:02 pcfreak kernel: [4222971.650646] usb 1-1.1: new high-speed USB device number 6 using
ehci-pci
Feb 18 14:27:02 pcfreak kernel: [4222971.759989] usb 1-1.1: New USB device found, idVendor=04f9, idPr
oduct=035b
Feb 18 14:27:02 pcfreak kernel: [4222971.761460] usb 1-1.1: New USB device strings: Mfr=0, Product=0,
SerialNumber=3
Feb 18 14:27:02 pcfreak kernel: [4222971.762890] usb 1-1.1: SerialNumber: E74370K4N282553
Feb 18 14:27:02 pcfreak kernel: [4222971.765899] usb1p 1-1.1:1.0: usb1p0: USB Bidirectional printer d
ev 6 if 0 alt 0 proto 2 vid 0x04F9 pid 0x035B
Feb 18 14:27:02 pcfreak mtp-probe: checking bus 1, device 6: "/sys/devices/pci0000:00/0000:00:1a.0/us
b1/1-1/1-1.1"
Feb 18 14:27:02 pcfreak mtp-probe: bus: 1, device: 6 was not an MTP device
Feb 18 14:27:07 pcfreak kernel: [4222976.850306] usb1p0: removed
Feb 18 14:27:07 pcfreak kernel: [4222976.862853] usb1p 1-1.1:1.0: usb1p0: USB Bidirectional printer d
ev 6 if 0 alt 0 proto 2 vid 0x04F9 pid 0x035B
Feb 18 14:27:07 pcfreak udev-configure-printer: Re-enabled printer ipp://localhost/printers/DCP1610W
Feb 18 14:27:12 pcfreak kernel: [4222981.410333] usb 1-1.1: USB disconnect, device number 6
Feb 18 14:27:12 pcfreak kernel: [4222981.411863] usb1p0: removed
Feb 18 14:27:12 pcfreak udev-configure-printer: Disabled printer ipp://localhost/printers/DCP1610W as
the corresponding device was unplugged or turned off
Feb 18 18:55:05 pcfreak kernel: [4239054.916501] qmail-remote[23967] segfault at ed5b8dc0 ip 00000000
00407a02 sp 00007ffced5b8d88 error 4 in qmail-remote[400000+b000]
Feb 18 23:55:04 pcfreak kernel: [4257055.351749] qmail-remote[23896] segfault at 11ba8060 ip 00000000
```

For a frequent tail + ccze usage with ccze you can add to ~/.bashrc following shell small function

```
tailc () { tail $@ | ccze -A }
```

Below is a list of supported syntax highlighting colorizer:

\$ ccze -l

Available plugins:

Name	Type	Description
apm	Partial	Coloriser for APM sub-logs.
distcc	Full	Coloriser for distcc(1) logs.
dpkg	Full	Coloriser for dpkg logs.
exim	Full	Coloriser for exim logs.
fetchmail	Partial	Coloriser for fetchmail(1) sub-logs.
ftpstats	Full	Coloriser for ftpstats (pure-ftpd) logs.
httpd	Full	Coloriser for generic HTTPD access and error logs.
icecast	Full	Coloriser for Icecast(8) logs.
oops	Full	Coloriser for oops proxy logs.
php	Full	Coloriser for PHP logs.
postfix	Partial	Coloriser for postfix(1) sub-logs.
procmail	Full	Coloriser for procmail(1) logs.
proftpd	Full	Coloriser for proftpd access and auth logs.
squid	Full	Coloriser for squid access, store and cache logs.
sulog	Full	Coloriser for su(1) logs.
super	Full	Coloriser for super(1) logs.
syslog	Full	Generic syslog(8) log coloriser.
ulogd	Partial	Coloriser for ulogd sub-logs.
vsftpd	Full	Coloriser for vsftpd(8) logs.
xferlog	Full	Generic xferlog coloriser.

At many cases for sysadmins like me that prefer clarity over obscurity, even a better solution is to just change in **/etc/squid/squid.conf**

the logging to turn it in human-readable form, to do so add to config somewhere:

Logformat squid %tl.%03tu %6tr %>a %Ss/%03Hs %

You will get log output in format like:

18/Feb/2019:18:38:47 +0200.538 4787 y.y.y.y TCP_MISS/200 41841 GET http://google.com/
- DIRECT/x.x.x.x text/html

SQUID's format recognized parameters in above example are as follows:

- %** a literal % character
- >a** Client source IP address
- >A** Client FQDN
- >p** Client source port
- la** Local IP address (http_port)
- lp** Local port number (http_port)
- sn** Unique sequence number per log line entry
- ts** Seconds since epoch
- tu** subsecond time (milliseconds)
- tl** Local time. Optional strftime format argument
default %d/%b/%Y:%H:%M:%S %z
- tg** GMT time. Optional strftime format argument
default %d/%b/%Y:%H:%M:%S %z
- tr** Response time (milliseconds)
- dt** Total time spent making DNS lookups (milliseconds)