
ONE IDENTITY
by Quest

Sudo logs for Blue Teamers

Peter Czanik
Open Source Evangelist
One Identity
@PCzanik

ONE IDENTITY by Quest

About me

- Working at One Identity
- syslog-ng & sudo upstream
- Help in RPM and FreeBSD packaging
- Blogger and speaker at open source events

Overview

- What is sudo? What is syslog-ng?
- Versions to use
- JSON-formatted logging
- Chroot, working directory
- Logging sub-commands

What is sudo?

- Sudo allows a system administrator to delegate authority by giving certain users the ability to run some commands as root or another user while providing an audit trail of the commands and their arguments. (https://www.sudo.ws/)

- A lot more than just a prefix

A basic /etc/sudoers

%wheel ALL=(ALL) ALL

- Who
- Where
- As which user
- Which command

Sudo for Blue Teams

- Control and log access
- Record and play back terminal input and output
- Modular: extend with your own code, now even in Python

- Sudo logs are parsed automatically by syslog-ng: alerting, NoSQL

IO logs API

- Accessing input and output from user sessions

- Python examples:
  - Breaking session if a given text appears on screen
  - Breaking session if “rm -fr” is typed in the command line

IO logs API example: code

```
import sudo

class MyIOPlugin(sudo.Plugin):
    def log_ttyout(self, buf):
        if "MySecret" in buf:
            sudo.log_info("Don't look at my secret!")
            return sudo.RC_REJECT
```

Syslog-ng

- Enhanced logging daemon with a focus on portability and high-performance central log collection. Originally developed in C.

- Logging: Recording events, such as:

Jan 14 11:38:48 linux-0jbu sshd[7716]: Accepted publickey for root from 127.0.0.1 port 48806 ssh2

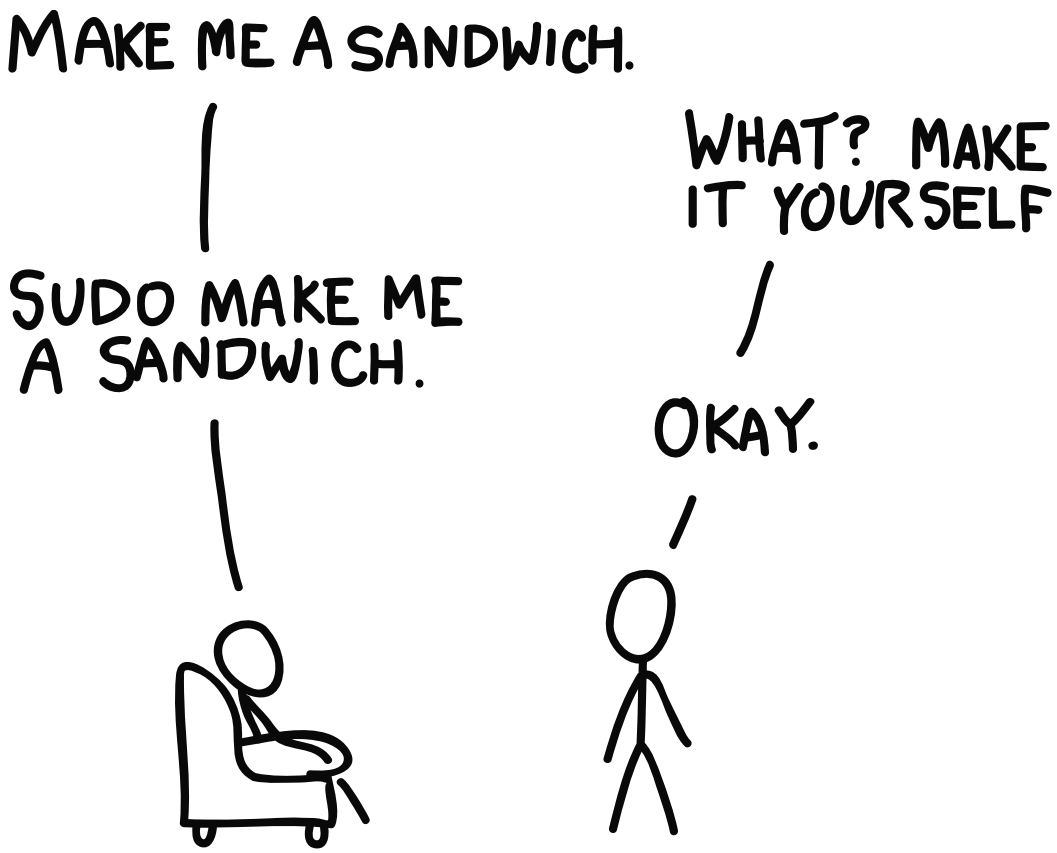
Syslog-ng

- Collecting data
- Processing
- Filtering
- Storing (forwarding) logs

Versions to use

- Version 1.9.8+ of sudo (earlier versions have no sub-command logging)
  - https://www.sudo.ws/getting/packages/
- Version 3.31+ of syslog-ng (earlier versions do not parse sudo JSON logs automagically)
  - https://www.syslog-ng.com/products/open-source-log-management/3rd-party-binaries.aspx

It can get you a sandwich… (by XKCD)



New options for logging

- JSON-formatted logs
- Forward logs to sudo_logsrvd
- Introduced in sudo 1.9.4

Basis syslog-ng configuration

```
filter f_sudo {
  program(sudo);
};
destination d_sudo {
  file("/var/log/sudo");
};
log {
  source(s_sys);
  filter(f_sudo);
  destination(d_sudo);
};
```

JSON-formatted logs

- Traditionally plain-text logs with minimal information
- Due to syslog constraints

- Nov 18 12:31:33 centos7sudo sudo[30666]: czanik : 3 incorrect password attempts ; TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/bash
- Nov 18 12:31:43 centos7sudo sudo[30670]: czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/bash
- Nov 18 12:31:49 centos7sudo sudo[30670]: czanik : command rejected by I/O plugin ; TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/bash

JSON-formatted logs

- JSON-formatted logs have more information in a structured format

Defaults log_format=json

Nov 18 12:40:30 centos7sudo sudo[30891]:
@cee:{"reject":{"reason":"command rejected by I/O
plugin","server_time":{"seconds":1605699630,"nanoseconds":9332939
11,"iso8601":"20201118114030Z","localtime":"Nov 18
11:40:30"},"submit_time":{"seconds":1605699620,"nanoseconds":130
500349,"iso8601":"20201118114020Z","localtime":"Nov 18
11:40:20"},"submituser":"czanik","command":"/bin/bash","runuser":"ro
ot","runcwd":"/home/czanik","ttyname":"/dev/pts/0","submithost":"cent
os7sudo.localdomain","submitcwd":"/home/czanik","runuid":0,"columns"
:118,"lines":60,"runargv":["/bin/bash"]}}

JSON-formatted logs

- Use jq, etc. to make more human readable on the terminal:


```
{
 "sudo": {
  "accept": {
   "uuid": "616bc9efcf-b239-469d-60ee-deb5af8ce6",
    "server_time": {
     "seconds": 1643374700,
     "nanoseconds": 222446715,
     "iso8601": "20220128125820Z",
     "localtime": "Jan 28 13:58:20"
    },
    "submituser": "czanik",
[...]
```

Configuring syslog-ng

```
filter f_sudo {
  program(sudo);
};
destination d_sudo {
  file("/var/log/sudo" template("$(format-json --scope rfc5424 --scope dot-nv-pairs
       --rekey .* --shift 1 --scope nv-pairs --exclude MESSAGE --exclude .journal*)\n\n"));
};
log {
  source(s_sys);
  filter(f_sudo);
  destination(d_sudo);
};
```

Configuring syslog-ng

{"cee":{"sudo":{"accept":{"uuid":"e6da96eb4d-e494-4fa2-2270-f13d79969d","ttyname":"/dev/pts/0",
"submituser":"czanik","submithost":"localhost.localdomain","submitcwd":"/home/czanik",
"submit_time":{"seconds":"1643380947","nanoseconds":"462682022","localtime":"Jan 28 15:42:27","iso8601":"20220128144227Z"},
"server_time":{"seconds":"1643380947","nanoseconds":"477977979","localtime":"Jan 28 15:42:27","iso8601":"20220128144227Z"},
"runuser":"root","runuid":"0","runenv[9]":"SUDO_COMMAND=/bin/bash","runenv[8]":"HOME=/root",
"runenv[7]":"USER=root","runenv[6]":"LOGNAME=root","runenv[5]":"MAIL=/var/mail/root",
"runenv[4]":"PATH=/home/czanik/.local/bin:/home/czanik/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin",
"runenv[3]":"TERM=xterm-256color","runenv[2]":"SHELL=/bin/bash","runenv[1]":"HOSTNAME=localhost.localdomain",
"runenv[12]":"SUDO_GID=1000","runenv[11]":"SUDO_UID=1000","runenv[10]":"SUDO_USER=czanik",
"runenv[0]":"LANG=en_US.UTF-8","runcwd":"/home/czanik","runargv[0]":"/bin/bash","lines":"60",
"command":"/bin/bash","columns":"118"}}},"app":{"name":"cee"},"SOURCE":"s_sys","PROGRAM":"sudo",
"PRIORITY":"notice","PID":"13575","HOST_FROM":"localhost","HOST":"localhost.localdomain",
"FACILITY":"authpriv","DATE":"Jan 28 15:42:27"}

Using chroot and cwd

- Previously full root shell access was needed to start an application from a user inaccessible directory
- Full root access easily gained using chroot
- Starting with sudo 1.9.3 both can be configured from /etc/sudoers

Using chroot

- The chroot command needs root privileges
- Using with sudo it is still possible to “sudo chroot /”
- Chroot support must be explicitly enabled in sudoers

Using chroot

- If directory is not restricted in sudoers:

Defaults:%wheel runchroot=*

- “sudo --chroot / -s” can do the same ☺
- But at least it is nicely logged:

Sep 24 15:58:55 centos7sudo sudo[8149]: czanik : TTY=pts/0 ; CHROOT=/ ; PWD=/home/czanik ; USER=root ; TSID=00001G ; COMMAND=/bin/bash

Using chroot

- Directory can be restricted in sudoers:

Defaults:%wheel runchroot=/var/lib/mock/epel7-x86_64/root

- If chroot or a given directory is not allowed, it is logged:

Sep 25 08:43:32 centos7sudo sudo[2640]: czanik : user not allowed to change root directory to /an/interesting/directory ; TTY=pts/0 ; CHROOT=/an/interesting/directory ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/bash

Reporting on chroot violations in syslog-ng

```
filter f_sudo {
  program(sudo);
};
destination d_sudo {
  file("/var/log/sudo" template("$(format-json --scope rfc5424 --scope dot-nv-pairs
       --rekey .* --shift 1 --scope nv-pairs --exclude MESSAGE --exclude .journal*)\n\n"));
};
log {
  source(s_sys);
  filter(f_sudo);
  if (match("/" value(".cee.sudo.accept.runchroot"))) {
    destination { file("/var/log/sudo_danger" template("$(format-welf --key DATE
                --key .cee.sudo.accept.submituser)\n")); };
    # ToDo: change to a slack or smtp destination
  };
  destination(d_sudo);
};
```

Logging and intercepting sub-commands

- Before sudo 1.9.8 only session recording helped in case of shell or editor access
- Watching recordings is boring and time consuming
- 1.9.8 introduced:
  - Logging
  - Intercepting
- Works in most cases (does not work for built-in commands, etc.)

Logging sub-commands

- Enable with:

Defaults log_subcmds

- Turn on JSON formatting:

Defaults log_format=json

Logging sub-commands: editor screenshot

```
I    Unnamed (Modified)                                  Row 14    Col 1
czplaptop:/home/czanik # id
uid=0(root) gid=0(root) groups=0(root)
czplaptop:/home/czanik # ls /usr/share/syslog-ng/include/scl/
apache                  ewmm          logmatic  snmptrap
cee                     fortigate     mbox      solaris
checkpoint              graphite      netskope  sudo
cim                     graylog2      nodejs    sumologic
cisco                   iptables      osquery   syslogconf
collectd                junos         pacct     system
default-network-drivers  linux-audit  paloalto  telegram
discord                 loadbalancer  rewrite   websense
elasticsearch           loggly        slack     windowseventlog
czplaptop:/home/czanik # exit
```

Logging sub-commands

- Log without logging subcommands:

Aug 30 13:03:00 czplaptop sudo[10150]: Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/joe

Logging sub-commands

- Logs when logging subcommands:

```
Aug 30 13:13:14 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/joe
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/bin/sh –c /bin/bash
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/bin/bash
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/readlink /proc/10889/exe
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/dircolors –b /etc/DIR_COLORS
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/tput hs
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/tput –T dumb+sl hs
Aug 30 13:13:37 czplaptop sudo[10874]:   Czanik : TTY=pts/1 ; PWD=/home/Czanik ; USER=root ; COMMAND=/usr/bin/tput bold
Aug 30 13:13:37 czplaptop sudo[10874Aug 30 13:13:14 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/joe
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/sh -c /bin/bash
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/bash
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/readlink /proc/10889/exe
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/dircolors -b /etc/DIR_COLORS
[…]
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/sed -r s@/*:|([^\\]):@\1\n@g;H;x;s@/\n@\n@
Aug 30 13:13:37 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/tty
Aug 30 13:13:42 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/id
Aug 30 13:13:56 czplaptop sudo[10874]:   czanik : TTY=pts/1 ; PWD=/home/czanik ; USER=root ; COMMAND=/usr/bin/ls -A -N --color=none -T 0 /usr/share/syslog-ng/include/scl/
```

Logging sub-commands

- Log with JSON formatting:

Aug 30 13:29:28 czplaptop sudo[11740]:
@cee:{"sudo":{"accept":{"uuid":"18f25b2438-0c44-ddaf-a264-
c70998d319","server_time":{"seconds":1630322968,"nanoseconds":12453428
3,"iso8601":"20210830112928Z","localtime":"Aug 30
11:29:28"},"submit_time":{"seconds":1630322965,"nanoseconds":357407987,
"iso8601":"20210830112925Z","localtime":"Aug 30
11:29:25"},"submituser":"czanik","command":"/usr/bin/joe","runuser":"root","r
uncwd":"/home/czanik","ttyname":"/dev/pts/1","submithost":"czplaptop","subm
itcwd":"/home/czanik","runuid":0,"columns":80,"lines":24,"runargv":["joe","/et
c/issue"],"runenv":["LANG=en_US.UTF-
8","COLORTERM=truecolor","TERM=xterm-
256color","MAIL=/var/mail/root","PATH=/usr/sbin:/usr/bin:/sbin:/bin:/usr/local
/bin:/usr/local/sbin","LOGNAME=root","USER=root","HOME=/root","SHELL=/bin
/bash","SUDO_COMMAND=/usr/bin/joe
/etc/issue","SUDO_USER=czanik","SUDO_UID=1000","SUDO_GID=100"]}}}

Intercepting sub-commands

- Can prevent applications from running
- Enabling is a two-step process in sudoers

Defaults intercept

- And the actual rule:

czanik ALL = (ALL) ALL, !/usr/bin/who

Intercepting sub-commands

- Even if running a shell with full root access:

```
czanik@czplaptop:~> sudo -s
czplaptop:/home/czanik # who
Sorry, user czanik is not allowed to execute
'/usr/bin/who' as root on czplaptop.
bash: /usr/bin/who: Permission denied
```

Intercepting sub-commands

- Shells can easily be disabled
- It has “side effects”

Defaults intercept
Cmnd_Alias SHELLS=/usr/bin/bash, /usr/bin/sh
czanik ALL = (ALL) ALL, !SHELLS

Intercepting sub-commands

- Starting a shell does not work anymore

```
czanik@czplaptop:~> sudo -s
Sorry, user czanik is not allowed to execute '/bin/bash'
as root on czplaptop.
```

Intercepting sub-commands

- Also prevents running external applications

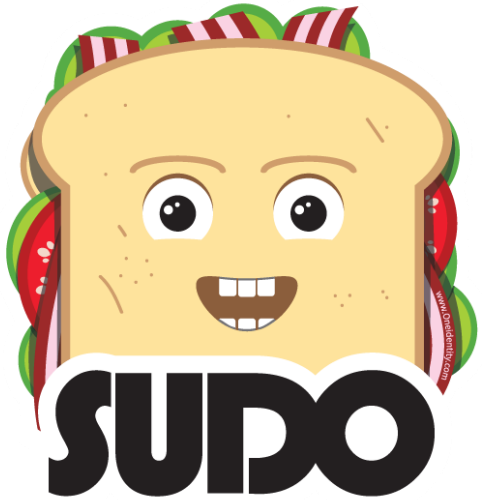
```
czanik@czplaptop:~> sudo vi /etc/issue
Sorry, user czanik is not allowed to execute '/bin/bash -c
/bin/ls' as root on czplaptop.
Cannot execute shell /bin/bash
Press ENTER or type command to continue
czanik@czplaptop:~>
```

Summary

- Recent versions of sudo let you see and control a lot more activities:
  - More detailed, easier to use log messages collected to a central location
  - Less need for root shells
  - Track and intercept sub-commands
- Using syslog-ng you have built-in support for sudo logs:
  - You can easily alert on the new JSON-formatted logs
  - Send parsed fields to NoSQL to easily search and report on events

Questions?

- Sudo website: https://www.sudo.ws/
- My email: peter.czanik@oneidentity.com
- Twitter: @Pczanik



ONE IDENTITY by Quest


ONE IDENTITY
by Quest