

# What you most likely did not know about sudo...

Peter Czanik / One Identity (Balabit)



# Overview

- What is sudo
- From aliases to plugins
- What is new in 1.9?

# What is sudo?

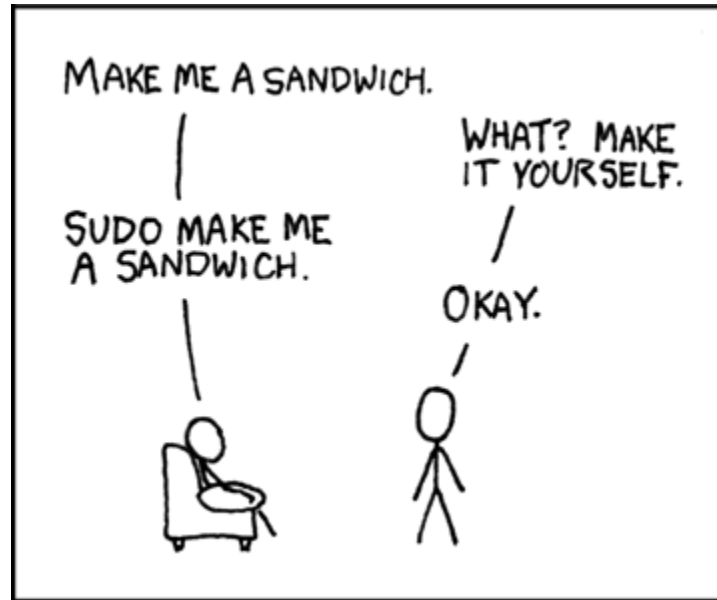
- Answers, depending on experience and size of environment:
  - A tool to complicate life
  - A prefix for administrative commands
  - A way to see who did what

# 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

# What is sudo?

- It can make you a sandwich :)



By xkcd.com

# Basic /etc/sudoers

```
%wheel ALL=(ALL) ALL
```

- Who
- Where
- As which user
- Which command

# Aliases

- Aliases:
  - Simplify configuration
  - Less error-prone

**Host\_Alias WEBSERVERS = www1, www2, www3**

**User\_Alias ADMINS = smith, johnson, williams**

**Cmnd\_Alias REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff**

**ADMINS WEBSERVERS = REBOOT**

# Defaults

- Changes the default behavior:

Defaults secure\_path="/usr/sbin:/usr/bin:/sbin:/bin"

Defaults env\_keep = "LANG LC\_ADDRESS LC\_CTYPE"

Defaults !insults

- Can be user/host/etc specific

Defaults:%wheel insults



# Insults

- Fun, but not always PC :)

```
czanik@linux-mewy:~> sudo ls
```

```
[sudo] password for root:
```

```
Hold it up to the light --- not a brain in sight!
```

```
[sudo] password for root:
```

```
My pet ferret can type better than you!
```

```
[sudo] password for root:
```

```
sudo: 3 incorrect password attempts
```

```
czanik@linux-mewy:~>
```

# Digest verification

```
peter ALL =  
sha244:11925141bb22866afdf257ce7790bd6275feda80b3b241c108b  
79c88 /usr/bin/passwd
```

- Modified binaries do not run
- Difficult to maintain
- Additional layer of protection

# Session recording

- Recording the terminal
- Play it back
- Difficult to modify (not cleartext)
- Easy to delete (saved locally) with unlimited access
  - Stay tuned :)

# Plugin-based architecture

- Starting with version 1.8
- Replace or extend functionality
- Both open source and commercial

# Plugin-based architecture

- sudo\_pair
- Making sure that no user can enter commands on their own
- Terminate session on suspicious activity
- Developed in Rust
- [https://github.com/square/sudo\\_pair/](https://github.com/square/sudo_pair/)

# Plugin-based architecture

- Demo of sudo\_pair

# Configuration hints

- Use visudo for syntax check
- Use EDITOR to use another text editor :-)
- A syntactically correct config still does not mean that you can execute anything :-)
- root password (even for Ubuntu!)

# Configuration

- Read from top to bottom
- Start with generic
- Add exceptions at the end



# Sample configuration

```
Defaults !visiblepw
Defaults always_set_home
Defaults match_group_by_gid
Defaults always_query_group_plugin
Defaults env_reset
Defaults env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin
root ALL=(ALL) ALL
%wheel ALL=(ALL) ALL
Defaults:%wheel insults
Defaults !insults
Defaults log_output
```

# Where is the problem?

- There was a common mistake

# Central management

- Puppet, Ansible, etc.
  - Not real-time
  - Users can modify locally
  - Error-prone
- LDAP
  - Propagates real-time
  - Can't be modified locally
  - Many limitations

# Logging and alerting

- E-mail alerts
- All events to syslog
  - Make sure logs are centralized
  - Using syslog-ng sudo logs are automatically parsed and you can also do alerting to Slack, Splunk, Elasticsearch, etc.
- Debug logs
  - Debug rules
  - Report problems

# syslog-ng

- 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

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

# Configuring syslog-ng

- “Don't Panic”
- Simple and logical, even if it looks difficult at first
- Pipeline model:
  - Many different building blocks (sources, destinations, filters, parsers, etc.)
  - Connected into a pipeline using “log” statements

# syslog-ng.conf: getting started

```
@version:3.23
```

```
@include "scl.conf"
```

```
# this is a comment :)
```

```
options {flush_lines (0); keep_hostname (yes);};
```

```
source s_sys { system(); internal();};
```

```
destination d_mesg { file("/var/log/messages"); };
```

```
filter f_default { level(info..emerg) and not (facility(mail)); };
```

```
log { source(s_sys); filter(f_default); destination(d_mesg); };
```

# syslog-ng.conf: sudo building blocks

```
filter f_sudo {program(sudo)};
```

```
destination d_test {  
  file("/var/log/sudo.json"  
  template("${format-json --scope nv_pairs --scope dot_nv_pairs --scope rfc5424}\n\n"));  
};
```

```
destination d_slack {  
  slack(hook-url("https://hooks.slack.com/services/TF8LZ3CSF/BF8CJKVT3/  
C2qdnMXCwDD3ATOFVMyxMyHB"  
  ));  
};
```

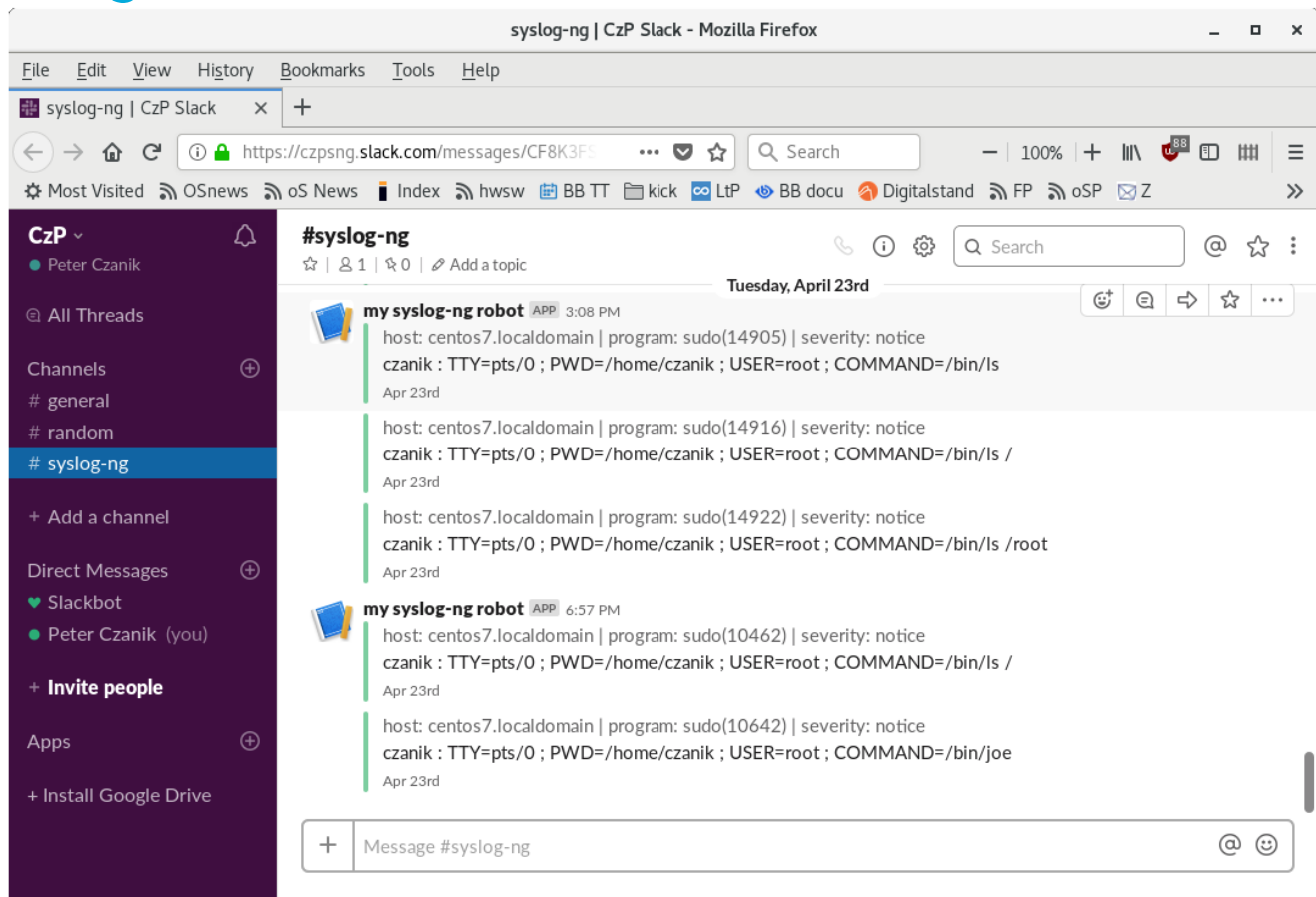


# syslog-ng.conf: sudo log statement

# name-value pairs come from the sudo parser

```
log {  
    source(s_sys);  
    filter(f_sudo);  
    if (match("czanik" value(".sudo.SUBJECT"))) {  
        destination { file("/var/log/sudo_filtered"); };  
        destination(d_slack);  
    };  
    destination(d_test);  
};
```

# sudo logs in Slack



The screenshot shows a Slack interface in a Mozilla Firefox browser window. The browser title is "syslog-ng | CzP Slack - Mozilla Firefox". The address bar shows the URL "https://czpsng.slack.com/messages/CF8K3FS". The Slack interface displays a channel named "#syslog-ng" with 1 member and 0 topics. The channel is currently active, and the left sidebar shows a list of channels including "# syslog-ng".

The channel history shows several messages from a bot named "my syslog-ng robot". The messages are timestamped "Tuesday, April 23rd" and contain sudo log entries:

- 3:08 PM: host: centos7.localdomain | program: sudo(14905) | severity: notice  
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls  
Apr 23rd
- Apr 23rd: host: centos7.localdomain | program: sudo(14916) | severity: notice  
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /  
Apr 23rd
- Apr 23rd: host: centos7.localdomain | program: sudo(14922) | severity: notice  
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /root  
Apr 23rd
- 6:57 PM: host: centos7.localdomain | program: sudo(10462) | severity: notice  
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /  
Apr 23rd
- Apr 23rd: host: centos7.localdomain | program: sudo(10642) | severity: notice  
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/joe  
Apr 23rd

The bottom of the screen shows a message input field with a plus sign on the left and a search icon on the right. The text "Message #syslog-ng" is visible in the input field.

# Coming to sudo 1.9

- Recording Service: collect sudo IOlogs centrally
- Audit Plugin (ToDo)
- Approval Plugin framework (ToDo)
- Python support for plugins

# Recording Service

- Collect sudo IOlogs centrally
- Streamed in real-time, securely
- Convenient, available, secure

# Python support

- Extend sudo using Python
- Using the same API-s as C plugins
- API: [https://www.sudo.ws/man/sudo\\_plugin.man.html](https://www.sudo.ws/man/sudo_plugin.man.html)
- No development environment or compilation is needed

# IO logs API

- Demo

# Not just a prefix, but...

## 1.8

- Fine tuned permissions
- Aliases / Defaults / Digest verification
- Session recording / Logging and alerting
- LDAP
- Plugins

## 1.9

- Python plugin
- Logging API, Approval API
- Central session recording collection



# Questions?



sudo website: <https://www.sudo.ws/>

My e-mail: [peter.czanik@oneidentity.com](mailto:peter.czanik@oneidentity.com)

Twitter: <https://twitter.com/PCzanik>

