datto

sudo command: Tips and tricks

Fred Mora - System Engineering, Datto

Agenda

- What is the sudo command
- Normal, boring use
- Under the hood
- More interesting case
- The sudoers file

What is the sudo command

- “super-user do” - Perform a task as super-user (root)
- Goal: Delegate a limited authority to non-root users
  - sudo appeared on BSD Unix in the 1980s
  - This is a concern as old as Unix
- Very useful, and it can do more for you than the normal, boring use.

Sudo : The bog-standard usage

- When you install a modern distro, it asks you for a user account, and gives that account sudo access

- To run administrative command, you then do:

```
$ sudo risky_command
[sudo] password for fmora:
```

- Several commands to run?
  $ **sudo bash**

- So that’s the boring use case.

A peek under the hood

- The fmora user is part of a special group (sudo on ubuntu):

```
$ id fmora
uid=1000(fmora) gid=1000(fmora)
groups=1000(fmora),4(adm),24(cdrom),27(sudo)
, ...
```

- This group is given special privileges in the /etc/ssudoers file:

```
# Allow members of group sudo to execute any
command
%sudo    ALL=(ALL:ALL) ALL
```

- More on that file later.

More interesting scenarios

- User timmy should be able to run a limited list of commands (e.g., shutdown -h) without a password prompt.
- The sudoers file then contains:

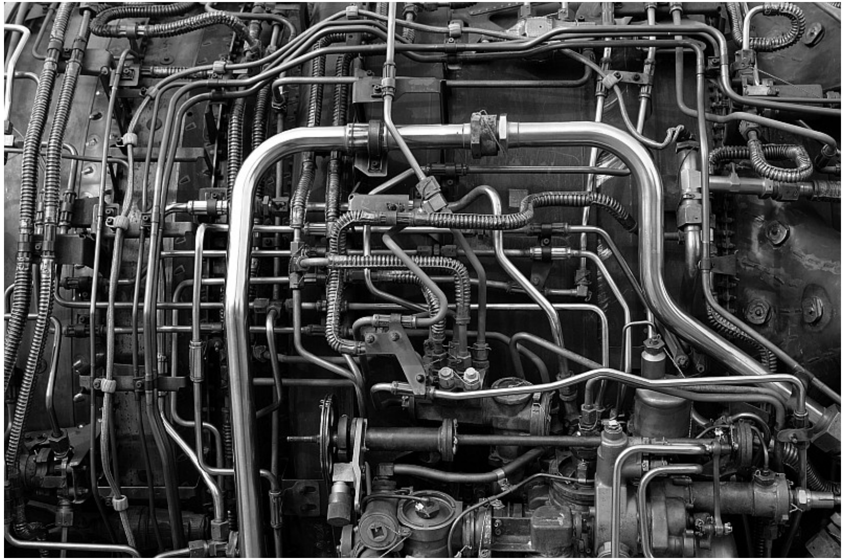
  ```
  CMDLIST = /sbin/shutdown -h *, \
      /usr/sbin/service kodi restart
  timmy  ALL=(ALL) NOPASSWD: CMDLIST
  ```

- CMDLIST is an alias for a list of commands
- The * in shutdown lets the user pass arguments (e.g., ‘now’)
- NOPASSWD skips the sudo password prompt

- The ALL keyword means “match all”
- The generic sudo line is:
  who where = (as_whom) what
  - who = user list
  - where = list of hostnames
  - as_whom: Under what ID the command runs
  - what: Commands

The sudoers file

- sudoers contains the config of the sudo command
- Should not be edited manually. Use `sudo visudo` instead:
  - visudo checks the syntax before leaving the editor
  - Avoids leaving you with a screwed up sudoers, unable to fix it!
- Put only trivial things in /etc/sudoers
- Complex config should be in /etc/sudoers.d/



Production example: techsupport user

```
File /etc/sudoers.d/techsupport:

# Minutes between sudo password prompts
Defaults:techsupport timestamp_timeout=30

# Clean env to start
Defaults:techsupport env_reset
Defaults:techsupport secure_path="/usr/local/sbin:/usr/local/bin:\
/usr/sbin:/usr/bin:/sbin:/bin"
Defaults:techsupport env_keep="SSH_CONNECTION SSH_AUTH_SOCK SSH_TTY"

Cmnd_Alias      DANGEROUS = /usr/sbin/usermod, /bin/mount, /bin/rm, /bin/kill
Cmnd_Alias      DATTO = /datto/scripts/
Cmnd_Alias      VIEWFILES =  /usr/bin/less, /usr/bin/tail, /bin/grep, /bin/cat
# NOEXEC prevents commands from issuing a sub-shell
techsupport          ALL = NOPASSWD: NOEXEC: VIEWFILES
techsupport          ALL = NOPASSWD: DANGEROUS, DATTO
```

Make sure that /etc/sudoers contains:

```
includedir /etc/sudoers.d
```

Questions?