

## Menggunakan SUDO (superuser do)

Ada dua cara umum untuk menguasai tugas root ke user biasa. Anda dapat mengubah izin file untuk program yang biasanya hanya di jalankan oleh root. Tipikalnya kita menggunakan set-UID untuk melakukan hal tersebut sehingga user tertentu dapat berlaku sebagai root. Namun hal ini tidaklah aman dan pengaturan yang tidak praktis. Pilihan lainnya yaitu menggunakan sudo, yang merupakan kependekan dari *superuser do*.

Program sudo memungkinkan user untuk menjalankan perintah-perintah yang di seleksi sebagai root. Ketika user biasa menggunakan sudo untuk mengeksekusi perintah dengan hak istimewa (root), sudo akan mencatat perintah tersebut berikut argumennya sehingga audit dapat dengan mudah dilakukan.

Jika program sudo belum terinstall anda dapat mendownload sourcena di <http://www.courtesan.com/sudo> atau versi RPM di <http://rpmfind.net> . Namun kali ini kita akan menginstall dengan menggunakan paket source RPM yaitu *sudo-1.6.3-4.src.rpm*. Setelah mendownload paket source RPM, ikuti tahap berikut untuk menginstall sudo.

1. Ubah user menjadi root

```
su
```

2. Jalankan perintah

```
rpm -ivh sudo-1.6.3-4.src.rpm
```

untuk mengekstrak sudo ke direktori */usr/src/redhat/SOURCES*, lalu ubah direktori ke */usr/src/redhat/SOURCES*, ketikkan *ls -l sudo\** anda akan melihat file berikut:

```
-rw- r-- r-- 1 root root 285126 Apr 10 2000 sudo-1.6.3.tar.gz
```

3. Ekstrak sudo-1.6.3.tar.gz

```
tar zxvf sudo-1.6.3.tar.gz
```

Lalu masuk ke direktori sudo-1.6.3

```
cd sudo-1.6.3
```

4. Jalankan script

```
./configure --with-pam
```

untuk meng'compile sudo dengan dukungan PAM.

5. Jalankan perintah *make* untuk kompilasi, jika tidak terjadi kesalahan anda

dapat menginstall sudo ke sistem dengan perintah `make install`.

6. Copy'kan file `sample.pam` ke `/etc/pam.d/sudo`

```
cp sample.pam /etc/pam.d/sudo
```

```
cp sample.pam /etc/pam.d
```

Lalu modifikasi file `/etc/pam.d/sudo` sebagai berikut :

```
##PAM-1.0
auth required /lib/security/pam_stack.so          service=system-auth
account required /lib/security/pam_stack.so      service=system-auth
password required /lib/security/pam_stack.so    service=system-auth
session required /lib/security/pam_stack.so     service=system-auth
```

7. Jalankan perintah `make clean` untuk menghapus file objek yang tidak penting lagi.

## Konfigurasi dan Menjalankan sudo

Konfigurasi sudo terletak di file `/etc/sudoers`. Gunakan program `visudo` untuk mengedit file ini. Perintah `visudo` :

- mengunci file `/etc/sudoers` untuk mencegah pengubahan secara simultan oleh sesi root ganda.
- Memeriksa syntax konfigurasi.

Defaultnya program `visudo` menggunakan editor `vi`. Jika anda tidak cocok dengan `vi` dan biasa menggunakan editor seperti `emacs` atau `pico`, anda dapat meng'set variabel `EDITOR` environment ke editor favorit anda. Contohnya jika anda ingin menggunakan editor `pico`, jalankan `export EDITOR=/usr/bin/pico` untuk di shell `bash` , atau jalankan `setenv EDITOR /usr/bin/pico` untuk shell `csh`, `tcsh`. Kemudian jalankan program `visudo` untuk mengedit isi `/etc/sudoers` dengan editor favorit anda.

File `/etc/sudoers` defaultnya hanya berisi entri berikut :

```
root    ALL=(ALL) ALL
```

Arti dari entri diatas yaitu user `root` dapat menjalankan perintah apa saja di host tersebut sebagai user manapun. Konfigurasi `/etc/sudoers` cukup luas dan kadang membingungkan. Seksi berikut akan membahas pendekatan yang sederhana untuk mengkonfigurasi sudo untuk penggunaan yang praktis.

Dua tipe konfigurasi yang mungkin untuk sudo ialah :

- ◆ Alias. Alias merupakan nama lain dari sesuatu dengan fungsi yang sama. Ada empat tipe alias yang didukung oleh konfigurasi sudo.
  - *Host\_Alias* = daftar dari satu atau lebih hostname. Sebagai contoh, *WEBSERVERS = k2.nitec.com, everest.nitec.com*, mendefinisikan alias host **WEBSERVERS**.
  - *User\_Alias* = daftar dari satu atau lebih pemakai (user). Contohnya, *JRADMINS = dilbert, catbert* mendefinisikan pemakai **JRADMIN**, dimana terdaftar dua user.
  - *Cmnd\_Alias* = daftar dari satu atau lebih perintah. Contohnya *COMMANDS = /bin/kill, /usr/bin/killall* mendefinisikan alias perintah **COMMANDS**, dimana terdaftar dua perintah.
- ◆ Spesifikasi user. Spesifikasi user mendefinisikan siapa yang dapat menjalankan perintah apa sebagai user yang mana.

Sebagai contoh :

```
JRADMINS          WEBSERVER = (root)          COMMANDS
```

Spesifikasi user ini menjelaskan bahwa sudo membolehkan user **JRADMINS** untuk menjalankan program dalam **COMMANDS** pada sistem **WEBSERVER** sebagai root. Dengan kata lain, menspesifikasikan bahwa user *dilbert* dan *catbert* dapat menjalankan perintah */bin/kill* atau */usr/bin/killall* pada *k2.nitec.com*, *everest.nitec.com* sebagai root. Daftar contoh konfigurasi.

Contoh konfigurasi /etc/sudoers

```
Host_Alias WEBSERVER = www.nitec.com
User_Alias WEBMASTERS = sheila, kabir
Cmnd_Alias KILL = /bin/kill, /usr/bin/killall
WEBMASTERS WEBSERVER=(root) KILL
```

Pada konfigurasi awal menguasai user sheila dan kabir untuk menjalankan (melalui sudo) perintah kill (*/bin/kill* dan */usr/bin/killall*) sebagai root pada host [www.nitec.com](http://www.nitec.com). Dengan kata lain, dua user tersebut dapat mematikan proses apapun pada [www.nitec.com](http://www.nitec.com). Lalu bagaimana hal ini bisa berguna ? Katakanlah user sheila menemukan bahwa program *oops.pl* yang dijalankan oleh administrator sistem sebelum makan siang telah membuat performansi webserver menjadi lambat dan tersendat. Sheila dapat mematikan proses tersebut tanpa harus menunggu sysadmin kembali. User sheila dapat menjalankan perintah *ps auxww | grep oops.pl* untuk melihat apakah program tersebut masih berjalan.

```
root 11681 80.0 0.4 2568 1104 pts/0 S 11:01 0:20 perl /tmp/oops.pl
```

Sheila lalu mencoba untuk mematikan proses tersebut dengan perintah `kill -9 11681`, namun sistem menjawab *11681: Operation not permitted error message*. Dia menyadari bahwa proses tersebut dimiliki oleh root ( seperti terlihat pada output ps) dan menjalankan perintah `sudo kill -9 11681` untuk mematikan proses tadi. Karena sheila baru pertama kali menjalankan perintah sudo, ia menerima pesan berikut dari perintah sudo.

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these two things:
```

```
#1) Respect the privacy of others.
```

```
#2) Think before you type.
```

```
Password:
```

Pada point tersebut diminta passwordnya sendiri (bukan passwordnya root) dan jika passwordnya benar maka sudo melakukan perintah yang diminta tadi. Seperti yang terlihat sudo dapat melakukan tugas dengan aman untuk tingkat junior administrator atau coworkers. Daftar dibawah memperlihatkan konfigurasi sudo yang digunakan untuk menguasai tugas administrasi Web server kepada junior administrator.

```
# sudoers file.
# This file MUST be edited with the 'visudo'
# command as root.
# See the sudoers man page for the details on how
# to write a sudoers file.
# Host alias specification
Host_Alias WEBSERVER = www.intevo.com
# User alias specification
User_Alias WEBMASTERS = wsajr1, wsajr2
# Cmnd alias specification
Cmnd_Alias APACHE = /usr/local/apache/bin/apachectl
Cmnd_Alias KILL = /bin/kill, /usr/bin/killall
Cmnd_Alias REBOOT = /usr/sbin/shutdown
Cmnd_Alias HALT = /usr/sbin/halt
# User privilege specification
WEBMASTERS WEBSERVER=(root) APACHE, KILL, REBOOT, HALT
```

Konfigurasi ini membolehkan dua junior Web administrator (*wsajr1* dan *wsajr2*) untuk *start*, *restart*, *stop* Apache Web Server menggunakan perintah `/usr/local/apache/bin/apachectl`. Mereka juga dapat mematikan proses pada server dan reboot atau halt server jika diperlukan. Semua ini dapat dilakukan tanpa harus memiliki full akses root.

*Perintah-perintah yang mengizinkan akses shell (seperti editor vi atau program seperti less) tidak seharusnya dijalankan melalui fasilitas sudo, karena seorang user dapat menjalankan perintah apapun melalui shell dan mendapatkan full akses root secara sengaja maupun tidak disengaja.*

*Jangan memberikan akses sudo ke user yang tidak anda percaya. Juga lihat kebiasaan dari user sudo secara berkala dengan menggunakan log sudo.*

### **Auditing User sudo**

Secara default sudo mencatat seluruh percobaan untuk menjalankan perintah (yang berhasil atau tidak) melalui syslog. Anda dapat menjalankan `sudo -V` untuk menemukan fasilitas syslog mana yang digunakan untuk informasi log. Atau anda juga dapat menolak konfigurasi default syslog di `/etc/sudoers`. Contohnya, tambahkan baris berikut di `/etc/sudoers` untuk memaksa sudo menggunakan fasilitas auth syslog.

*Defaults*                    `syslog=auth`

Untuk memisahkan sudo log dari file-file log yang diutus syslog, anda tambahkan baris berikut pada file `/etc/sudoers`:

*Defaults*                    `log_year, logfile=/var/log/sudo.log`

Ini akan memaksa sudo untuk menulis entri log ke file `/var/log/sudo.log` setiap sudo dijalankan.

**Referensi : RedHat Press – RedHat Linux Security dan Optimization**

**-Mohammed J. Kabir**

Semoga Bermanfaat  
Faiz