sudo

context

dit document beschrijft de werking van sudo. Hiermee laat je gebruikers toe om bepaalde acties uit te voeren met andere privileges (vaak: root) zonder het wachtwoord uit handen te geven.

werking

- laat je commando voorafgaan door **su** om cmd met root-rechten uit te voeren

```
sudo useradd -c "New kid" -m kid01
```

- als een wachtwoord wordt gevraagd, geef dan je gebruikerswachtwoord in
het commando wordt uitgevoerd als een andere gebruiker.
- om je verleende rechten na te kijken:

```
sudo -l
```

- als je een commando probeert uit te voeren waarvoor je geen rechten hebt, wordt opnieuw een wachtwoord prompt gegeven:

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

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for jveys:
```

Dit geldt ook voor commando's die niet correct werden gedefinieerd in de configuratie.

configuratie

- bij voorkeur via `visudo` omdat er dan een syntax controle wordt uitgevoerd.

- toegangrechten kan je instellen op volgende niveaus:
  - gebruiker/groep
  - host waarop je commando mag uitvoeren
  - gebruiker waaronder je het commando mag uitvoeren
  - commando dat je mag uitvoeren
- voorbeeld:

```
%ApacheAdmin  node02=(www-data) /usr/bin/systemctl restart apache2
```

  leden van de groep ApacheAdmin mogen op node02 een herstart van Apache doen als gebruiker www-data

- hosts, gebruikers, commando's kan je bundelen in **aliassen**
- voorbeeld:

```
Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted,
/sbin/partprobe, /bin/mount, /bin/umount
```

- let erop steeds het volledige (en correcte!) **pad naar het uitvoerbaar bestand** te vermelden. Anders faalt je commando.
- met de optie `NOPASSWD:` moet de gebruiker niet bijkomend aanmelden.
  voorbeeld:

```
user.name ALL=(ALL:ALL) NOPASSWD:ALL
```

- om wat onderverdeling in verschillende configs te maken, kan je best je configuratie bewaren onder /etc/sudoers.d/.
  Je kan die dan bewerken ahv `visudo -f /etc/sudoers.d/<naamVanBestand>`.
  Als je een programma verdeelt via een pacakge manager kan je je sudo configuratie op die manier meesturen.

voorbeeld

- standaard CentOS configuratie vind je hier in github.

logging

- acties worden standaard geloged naar /var/log/secure

```
Jan 24 14:33:21 node01 sudo:   jveys : TTY=pts/2 ; PWD=/home/jveys ; USER=root ; COMMAND=/bin/systemctl start tb-g
w-default
Jan 24 14:33:21 node01 sudo: pam_unix(sudo:session): session opened for user root by jveys(uid=0)
Jan 24 14:33:21 node01 polkitd[1042]: Registered Authentication Agent for unix-process:15068:8502098 (system bus n
ame :1.146 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationA
gent, locale en_US.UTF-8)
Jan 24 14:33:21 node01 sudo: pam_unix(sudo:session): session closed for user root
Jan 24 14:33:21 node01 polkitd[1042]: Unregistered Authentication Agent for unix-process:15068:8502098 (system bus
 name :1.146, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from
bus)
Jan 24 14:33:24 node01 sudo:   jveys : TTY=pts/2 ; PWD=/home/jveys ; USER=root ; COMMAND=/bin/systemctl status tb-
gw-default
Jan 24 14:33:24 node01 sudo: pam_unix(sudo:session): session opened for user root by jveys(uid=0)
Jan 24 14:33:24 node01 sudo: pam_unix(sudo:session): session closed for user root
```

- bemerk hoe er tijdelijk een sessie als een andere gebruiker wordt gestart: `session opened for user root by …`

problemen, problemen

- de meeste problemen zijn gevolg van 2 fouten:
  - commando wordt uitgevoerd waarvoor de gebruiker geen rechten heeft
  - het commando staat niet correct gedefinieerd in de configuratie.
- wachtwoord prompt wordt getoond ook al staat `NOPASSWD:` in de configuratie.
  - controleer dat pad naar het commando correct gedefinieerd staat in de configuratie.

meer info

voeg hier linken toe naar verdere uitleg

Linux