ulimit

La comanda **ulimit** permet consultar i configurar certes limitacions als usuaris del sistema. Per defecte la comanda ulimit sense arguments ens mosra el límit de lmida de fitxer

```
ulimit
unlimited
```

Amb la opció -a podem veure la coniguració actual de l'usuari

```
ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) 1000
pending signals                 (-i) 3906
max locked memory       (kbytes, -l) 64
...
```

/etc/security/limits.conf

El fitxer de configuració limits.conf permet establir diferents límits pels usuaris o grups d'usuaris del sistema. La seva estructura és la següent:

```
<domain>      <type>      <item>      <value>
```

On:

- domain pot ser:
  - Un nom d'usuari
  - Un nom de grup
  - Un asterisc (*) per definir una entrada per defecte (s'aplica a tots els usuaris que no tenen una entra pròpia)
  - El comodí % es pot fer servir amnb grups per definir un maxlogin
- type pot ser:
  - hard: límits que els usuaris no poden modificar (els implementa el kernel)
  - soft: els usuaris poden modificar el valor de límit (sempre per sota d'un valor hard fixat pel root)
  - -: fixa els 2 límits (hard i soft) al mateix temps
- item pot ser:
  - core: limita la mida màxima dels fitxers core en KB.
  - data: mida màxima de les dades en KB.
  - fsize: mida màxima de fitxer en KB
  - memlock: espai màxim d'adreces de memòria bloquejades (KB)
  - nofile: Nombre màxim de fitxers oberts
  - rss: mida màxima de la memòria RSS (resident set size) en KB (ignorat a versions de Linux 2.4.30 o superiors.)
  - stack: mida màxima de la pila en KB
  - cpu: màxim temps de CPU en minuts

- nproc: nombre màxim de processos.
- as: límit d'espai d'adreces (KB)
- maxlogins: nombre màxim de logins per un usuari
- maxsyslogins: nombre màxim de logins al sistema.
- priority: prioritat per executar processos en el sistema
- locks: nombre màxim de fitxer blocats que un usuari pot suportar
- sigpending: nombre màxim de senyals pendents
- msgqueue: memòria màxima utilitzada per POSIX per les cues de missatges
- nice: màxima prioritat permesa a utilitzar
- rtprio: prioritat màxima del paràmetre realtime
- chroot: canvia a un directori arrel

sudo

La comanda **sudo** (switch user and do) ens permet poder executar operacions en nom d'un altre usuari. Algunes de les seves opcions interessants són:

- -u: indica l'usuari en el nom del qual volem executar la comanda
- -h: indica el host on volem que s'executi la comanda

/etc/sudoers

El fitxer de configuració que defineix de quina manera podem utilitzar la comanda sudo és /etc/sudoers. Aquest fitxer, per modificar-ho, disposa d'una comanda especial per fer-ho, visudo. A través d'ella podem editar la configuració de la comanda sudo, que es pot dividir en 3 grans seccions:

- Opcions
- Alias
- Regles d'accés

Opcions

Les opcions (defaults) permeten definir determinades característiques de comportament per als alias definits. Aquestes opcions es poden configurar en 4 nivells diferents:

- Globals
- Per usuari
- Per usuari amb privilegis
- Per equip

La manera de configurar cada un d'aquests nivells d'opcions sería la següent:

Opcions globals

```
Defaults <option1>, <option2>, ...
```

Opcions d'usuari

```
Defaults:<user> <option1>, <option2>, ...
```

Opcions d'usuari amb privilegis

```
Defaults><user> <option1>, <option2>, ...
```

Opcions d'equip

```
Defaults@<host> <option1>, <option2>, ...
```

Les posibles opcions a configurar són moltes, i s'agrupen en 4 categories diferets:

- flags (o booleans)
- enters
- strings
- llistes

Flags

S'acostumen a utilitzar de manera global. Per activar la opció només cal indicar-la, si la volem desactivar posem "!" davant d'ella (consultar opcions per defecte)

- mail_always: s'enviarà un correu cada vegada que s'utilitzi la comanda sudo (necessita la opció mailto_user)
- autehenticate: indica que els usuaris han d'autenticar-se per poder fer servir la comanda sudo (activat per defecte)
- log_host: es guarda en els logs el nom de màquina des del que s'ha esecutat la comanda sudo
- rootpw: els usuaris que intentin fer ús de la comanda sudo han d'autenticar-se amb la contrasenya de root.

Enters

Són opcions que es defineixen amb un valor determinat

- passwd_tries:intents permesos per validar la contrasenya a l'utilitzar sudo
- passwd_timeout: temps d'espera màxim per introduïr la contrasenya
- umask: valor que es farà servir per la creació de fitxers amb la comanda sudo

Strings

Són opcions on els valors a assignar són missatges, rutes, ... Si el valor conté espais s'ha de tancar tot el valor entre ""

- badpass_message: missatge a mostrar quan s'introdueix malament la contrasenya

LListes

Permeten configurar les variables d'entorn pròpies de sudo. Només hi ha 3 possibilitats.

- env_check
- env_delete
- env_reset

Aquestes llistes es poden gestionar amb:

- = Reemplaçar
- += Afegir
- -= Eliminar
- ! Deshabilitar

Alguns exemples d'utilització serien: Eliminar una variable de les disponibles:

```
Defaults env_delete -= HOSTNAME
```

Elimina la variable d'entorn $HOSTNAME d'entre les disponibles per l'execució de sudo Afegir una variable de les disponibles:

```
Defaults env_delete += DISPLAY
```

Afegeix la variable d'entorn $DISPLAY a les disponibles per l'execució de sudo

Alias

Els alias són elements que permeten englobar sobre un mateix nom un conjunt d'objectes d'una mateixa naturalesa. La seva sintaxi és:

```
<Alias_type> <Alias_Name> = <value1>, <value2>, ... <valueN>
```

El fitxer de sudoers permet 4 tipus diferents de alias:

- Cmnd_Alias: defineix un alias per a una (o vàries) comandes
- User_Alias: defineix un alias per a un (o varis) usuaris
- Runas_Alias: defineix un alias d'un usuari administrador o amb privilegis
- Host_Alias: defineix un alias per a un equip

El <Alias_Name> pot contenir lletres, números o guions baixos, però sempre ha de començar per una lletra majúscula (s'acostumen a escriure tot en majúscules)

Cmnd_Alias

Els alias de comandes permeten poder englobar dins d'un únic objecte un conjunt d'ordres. Existeixen

vàries formes de definir aquests alias. Veiem alguns exemples: Agrupar un conjunt de comandes:

```
  Cmnd_Alias WEB = /usr/sbin/apachectl, /usr/sbin/a2ensite,
/usr/sbin/a2dissite
```

Amb aquest alias WEB estem definint totes aquestes comandes relacionades amb el servidor Apache com un objecte únic que després podem utiitzar en les regles d'accés del fitxer sudoers. Definir una comanda amb opcions:

```
  Cmnd_Alias APAGAR = /usr/bin/shutdown -h 17\:00
```

A l'usuari que es permeti aquest alias podrà executar aquesta comanda només amb les opcions definides en el alias. Definir alias “anidats”:

```
  Cmnd_Alias NET_ADMIN = /sbin/ip, /sbin/ifconfig, WEB
```

A traves d'aquesta configuració podem dfinir un alias com el conjunt de vàries comandes i altres alias ja definits. Definir tot un directori:

```
  Cmnd_Alias EXECUTABLES = /sbin, !/sbin/poweroff
```

Aquest aias permetrà utilitzar tots els arxius executables que es trobin dins de /sbin, a excepció de la comanda poweroff. Aquesta configuració és arriscada perquè no té en compte les possibles restriccions a futures comandes que es puguin ubicar en aquest directori.

User_Alias

Els alias d'usuaris permeten definir un o més usuaris com a objecte únic, o grups d'usuaris utilitzant el símbol “%”. Veiem alguns exemples: Definir un conjunt d'usuaris:

```
  User_Alias STUDENTS = ana, david, maria, daniel
```

Aquest alias farà que les polítiques aplicades a ell actuin sobre aquests 4 usuaris del sistema. Definir conjunt de grups i usuaris:

```
  User_Aias OPERATORS = carme, joan, %professorat
```

Amb aquest alias els usuaris carme i joan i tots els membres del grup professorat estan definits com un objecte al que aplciar regles d'accés. Definir eclusions d'usuaris:

```
  User_Alias TOTHOM = ALL, !pilar, !miquel
```

El paràmetre ALL permet fer referència a tot el conjunt de possibles valors a utlittzar, i en aquest cas fa referència a tots els ususaris del sistema.

Runas_Alias

Funciona igual que els User_Alias, amb la diferència que permet indicar als usuaris a través del seu UID (precedit del síbol #)

```
Runas_Alias SECRETARIA = sergi, #1003
```

Host_alias

Els Host_Alias permeten definir un o més equips. Es poden referenciar per la seva IP, el seu nom (si es troba a /etc/hosts) o nom de domini si existeix un servei DNS capaç de resoldre'l.

```
Host_Alias LAN = 192.168.7./24, 172.18.0.0/255.255.0.0
Host_Alias SERVERS = 192.168.7.70, aries, geminis.domain.lan
```

Regles d'accés

Les regles d'accés defineixen quins usuaris poden executar determinades comandes en nom de certs usuaris i des de quins equips. La sintaxi de les regles d'accés és:

```
<user> <host> = <command1>, command2>, ....
```

Veiem alguns exemples er intentar entendre millor aquest funcionament: L'usuari <user> pot executar la comanda IP en qualsevol euip:

```
<user> ALL = /sbin/ip
```

Els usuaris definits en el User_Alias ADMIN poden executar en qualsevol equip qualsevol comanda amb sudo

```
ADMIN ALL = ALL
```

Els usuaris del grup d'operadors poden executar en la màquina server la comanda test-smtp.sh com si fossin l'ususari postmaster

```
%operadors server = (postmaster) /usr/local/bin/test-smtp.sh
```

Un usuari té permisos per executar en qualsevol equip amb qualsevol usuari qualsevol comanda

```
<user> ALL = (ALL) ALL
```

El conjunt d'usuaris definits en el User_Alias OPERATORS pot canviar la contrasenya de tots els usuaris (menys al root)

```
OPERATORS ALL = /usr/bin/passwd *, !/usr/bin/passwd root
```

Un usuari pot fer ús de la comanda ifconfig sense arguments

```
<user> ALL = "/sbin/ifconfig"
```

Tags

Quan es defineixen regles, en la llista de comandes es poden utilitzar diferents tags. Existeixen un total de 6 diferents:

- NOPASSWD|PASSWD determina si es sol·licita o no contrasenya per executar una comanda determinada
- NOEXEC|EXEC determina si es poden executar escapades de shell (shell escape) des d'una comanda permesa amb visudo
- SETENV|NSETENV determina si modifica l'entorn de variables en l'execució d'una comand