http://daffyduke.lautre.net/spip/?Documentation-sudo

Documentation sudo

- 1- Blog-Notes - Au boulot -

Date de mise en ligne : lundi 7 novembre 2011

Préambule

Le recours aux caractères génériques dans les règles du sudon'est pas conseillés. Mais il n'est pas toujours possible de s'en passer. C'est pourquoi il convient de les utiliser scrupuleusement afin de limiter l'apparition de failles de sécurité. Nous listons ici la façon de les limiter pour les commandes présentes dans une configuration sudoclassique.

Les commandes impactée

La commande rm

Soit la règle :

```
 /usr/bin/rm /etc/omv*
```

Elle est contournable de 2 façons :

```
 /usr/bin/rm /etc/omv/../passwd
/usr/bin/rm /etc/omv/tot /etc/passwd
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
 !/usr/bin/rm  *..*
!/usr/bin/rm  *[    ]*    (
espace et
tabulation dans le crochet)
```

attention : Dans ce cas de figure, il ne faut pas permettre l'usage des options (rm -r , rm -f)

L'éditeur vi

Soit la règle :

```
 /usr/bin/vi  /produits/patro*/KM_COMMUN/ORACLE/*
```

Elle est contournable de 3 façons :

```
 /usr/bin/vi
/produits/patrol/KM_COMMUN/ORACLE/../../../../etc/passwd
/usr/bin/vi  /produits/patrol/KM_COMMUN/ORACLE/toto
/etc/passwd
Execution de
:!cmd  pendant l'edition d'un fichier
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
 !/usr/bin/rm  *..*
!/usr/bin/rm  *[      ]*    (
espace et
tabulation dans le crochet)
NOEXEC: /usr/bin/vi  /produits/patro*/KM_COMMUN/ORACLE/*
```

Les commandes : chmod, chown et chgrp

Soit la régle :

```
 /usr/bin/chmod * /var/adm/atria/rgy/*
```

Elle est contournable de 2 façons :

```
 /usr/bin/chmod 666 /var/adm/atria/rgy/../../../etc/shadow
/usr/bin/chmod 666 /var/adm/atria/rgy/toto  /etc/shadow
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
 !/usr/bin/chmod  *..*
!/usr/bin/chmod  *[      ]*[      ]*      (
espace et
tabulation dans le crochet)
```

La commande cat

Soit la régle :

```
 /usr/bin/cat /etc/VRTSvcs/conf/config/main.cf*
```

Elle est contournable de 2 façons :

```
 /usr/bin/cat
/etc/VRTSvcs/conf/config/main.cfdir/../../../../etc/shadow
/usr/bin/cat  /etc/VRTSvcs/conf/config/main.cf  /etc/shadow
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
 !/usr/bin/cat  *..*
!/usr/bin/cat  *[      ]*    (
espace et
tabulation dans le crochet)
```

La commande grep

Soit la régle :

```
 /usr/bin/grep * /var/log/cron
```

est contournable de la façon suivante :

```
 /usr/bin/grep root /etc/shadow /var/log/cron
```

Pour limiter ces failles, il faut rajouter la règles suivante.

```
 !/usr/bin/grep  *[    ]*[    ]*  (espace et tabulation dans le
crochet)
```

attention : Dans ce cas de figure, il ne faut pas permettre l'usage des options (grep -i , grep -v)

Les commandes : cp et mv

Soit la régle :

```
 /usr/bin/cp /produits/admindb/*
/produits/patro*/KM_COMMUN/ORACLE/*
```

Elle est contournable de 2 façons :

```
 /usr/bin/cp /produits/admindb/../../etc/shadow
/produits/patrol/KM_COMMUN/ORACLE
/usr/bin/cp /produits/admindb/toto /etc/shadow
/produits/patro*/KM_COMMUN/ORACLE/
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
 !/usr/bin/cp *[  ]*[    ]* (espace et tabulation dans le crochet)
!/usr/bin/cp *..*
```

la commande tar

Soitr la règle :

```
/usr/bin/tar xvf /bases/clearcase/vues/*
```

Elle est contournable de la façon suivante :

```
/usr/bin/tar xvf /bases/clearcase/vues/../../../etc/system.tar
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
!/usr/bin/tar *..*
```

la commande mkdir

Soit la commande :

```
/usr/bin/mkdir  /applis/*/mqm/*
```

Elle est contournable de la façon suivante :

```
/usr/bin/mkdir  /applis/abc/mqm/../../../etc/rep
/usr/bin/mkdir  /applis/abc/mqm/ /etc/rep
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
!/usr/bin/mkdir *..*
!/usr/bin/mkdir *[      ]*  (espace et tabulation dans le
crochet)
```

Chemin absolu avec generiques

Soit la commande :

/local/secours/applis/*/*

Elle est contournable de la façon suivante :

/local/secours/applis/../fic

Pour limiter ces failles, il faut rajouter les règles suivantes.

!/local/secours/applis/../*

la commande ls

Soit la commande :

```
/usr/bin/ls /applis/sto/app/ftp_root/*
```

Elle est contournable de la façon suivante :

```
/usr/bin/ls /applis/sto/app/ftp_root/../../../var/sadm/install
/usr/bin/ls /applis/sto/app/ftp_root/toto  /var/sadm/install
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
!/usr/bin/ls *..*
!/usr/bin/ls *[    ]*
```

Pour limiter ces failles, il faut rajouter les règles suivantes.

```
!/local/secours/applis/../*
```