Distribution EOLE - Proposition Scénario #20325

Les journaux iptables doivent être filtrés correctement

27/04/2017 09:50 - Olivier FEBWIN

Statut:	Classée sans suite	**% réalisé:**	0%
Priorité:	Normal	**Temps estimé:**	0.00 heure
Assigné à:		**Temps passé:**	1.00 heure
Catégorie:			
Version cible:			

Description

Problème

Les journaux iptables ne semblent pas être filtrés correctement par nos règles rsyslog.

Le message doit contenir la chaîne de caractère **iptables** mais il est possible de se retrouver avec des messages ne venant pas du noyau.

Il faut ajouter un filtre sur la provenance des messages (**kernel**) en plus de filtrer sur le contenu du message.

Demande initiale

Après avoir testé les différents niveaux de log pour les iptables, je me suis aperçu que seul /var/log/rsyslog/local/iptables/iptables.warning.log était abondé par la règle *iptables -A ext-bas -i eth0 -m limit --limit 2/sec -j LOG --log-prefix "iptables connection attempt: "*.
Les autres logs sont envoyés dans /var/log/syslog pour les niveaux 0, 1, 2, et 3 et /var/log/rsyslog/local/kernel/kernel.*.log

```
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--DEFAUT "
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--7-debug " --l
og-level 7
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--6-info " --lo
g-level 6
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--5-notice " --
log-level 5
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--4-warning " -
-log-level 4
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--3-error " --l
og-level 3
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--2-crit " --lo
g-level 2
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--1-alert " --l
og-level 1
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "TEST-LOG--0-emerg " --l
og-level 0

root@amon25-dsden02:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=677 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.195/4.195/4.195/0.000 ms

root@amon25-dsden02:~# grep TEST-LOG-- /var/log/* -R
/var/log/rsyslog/local/kernel/kernel.emerg.log:2017-04-27T09:38:08.913948+02:00 amon25-dsden02.dsd
en02.in.ac-amiens.fr kernel: [40746.365791] TEST-LOG--0-emerg IN= OUT=eth0 SRC=10.67.128.240 DST=8
.8.8.8 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/rsyslog/local/kernel/kernel.warning.log:2017-04-27T09:38:08.914001+02:00 amon25-dsden02.d
sden02.in.ac-amiens.fr kernel: [40746.366455] TEST-LOG--4-warning IN= OUT=eth0 SRC=10.67.128.240 D
ST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/rsyslog/local/kernel/kernel.warning.log:2017-04-27T09:38:08.914020+02:00 amon25-dsden02.d
sden02.in.ac-amiens.fr kernel: [40746.366480] TEST-LOG--DEFAUT IN= OUT=eth0 SRC=10.67.128.240 DST=
```

```
8.8.8.8 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/rsyslog/local/kernel/kernel.alert.log:2017-04-27T09:38:08.913971+02:00 amon25-dsden02.dsd
en02.in.ac-amiens.fr kernel: [40746.366434] TEST-LOG--1-alert IN= OUT=eth0 SRC=10.67.128.240 DST=8
.8.8.8 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/syslog:2017-04-27T09:38:08.913948+02:00 amon25-dsden02.dsden02.in.ac-amiens.fr kernel: [4
0746.365791] TEST-LOG--0-emerg IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x0
0 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/syslog:2017-04-27T09:38:08.913971+02:00 amon25-dsden02.dsden02.in.ac-amiens.fr kernel: [4
0746.366434] TEST-LOG--1-alert IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x0
0 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/syslog:2017-04-27T09:38:08.913980+02:00 amon25-dsden02.dsden02.in.ac-amiens.fr kernel: [4
0746.366442] TEST-LOG--2-crit IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x00
 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/syslog:2017-04-27T09:38:08.913985+02:00 amon25-dsden02.dsden02.in.ac-amiens.fr kernel: [4
0746.366449] TEST-LOG--3-error IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x0
0 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
root@amon25-dsden02:~#
```

Comment faire pour envoyer des logs iptables dans /var/log/rsyslog/local/iptables/iptables.*.log ?

Historique

#1 - 27/04/2017 09:57 - Olivier FEBWIN

et /var/log/rsyslog/local/kernel/kernel.*.log pour les niveaux 0, 1, 4 (qui est aussi le niveau par défaut)

#2 - 27/04/2017 10:04 - Olivier FEBWIN

bizarre, je viens de recommencer les tests et j'ai ces logs en plus

```
/var/log/rsyslog/local/kernel/kernel.notice.log:2017-04-27T09:38:08.914007+02:00 amon25-dsden02.dsden02.in.ac-
amiens.fr kernel: [40746.366461] TEST-LOG--5-notice IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00
 PREC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/rsyslog/local/kernel/kernel.info.log:2017-04-27T09:38:08.914012+02:00 amon25-dsden02.dsden02.in.ac-am
iens.fr kernel: [40746.366468] TEST-LOG--6-info IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 PRE
C=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
/var/log/rsyslog/local/kernel/kernel.debug.log:2017-04-27T09:38:08.914016+02:00 amon25-dsden02.dsden02.in.ac-a
miens.fr kernel: [40746.366474] TEST-LOG--7-debug IN= OUT=eth0 SRC=10.67.128.240 DST=8.8.8.8 LEN=84 TOS=0x00 P
REC=0x00 TTL=64 ID=51566 DF PROTO=ICMP TYPE=8 CODE=0 ID=31811 SEQ=1
```

#3 - 27/04/2017 10:05 - Olivier FEBWIN

donc dans /var/log/rsyslog/local/kernel/kernel.*.log pour les niveaux 0, 1, 4 (qui est aussi le niveau par défaut), 5, 6 et 7

#4 - 12/05/2017 16:58 - Daniel Dehennin

- Sujet changé de Envoyer tous les logs iptables dans /var/log/rsyslog/local/iptables/iptables. à Les journaux iptables doivent être filtrés correctement*

- Description mis à jour

- Assigné à mis à Daniel Dehennin

#5 - 29/05/2017 10:49 - Daniel Dehennin

- Tracker changé de Demande à Proposition Scénario

- Description mis à jour

- Assigné à Daniel Dehennin supprimé

La journalisation fonctionne si vous avez le mot clef **iptables** dans le message :

```
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--DEFAUT "
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--7-debug " --log
-level 7
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--6-info " --log-
level 6
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--5-notice " --lo
g-level 5
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--4-warning " --l
og-level 4
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--3-error " --log
-level 3
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--2-crit " --log-
level 2
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--1-alert " --log
-level 1
root@amon25-dsden02:~# iptables  -I OUTPUT -d 8.8.8.8 -j LOG --log-prefix "iptables: TEST-LOG--0-emerg " --log
-level 0
```

#6 - 29/05/2017 11:27 - Olivier FEBWIN

OK c'est noté. Merci !

#7 - 17/01/2018 15:34 - Gilles Grandgérard

- Statut changé de Nouveau à Classée sans suite