Infra Chapril - Demande #4599

Demande # 3741 (Nouveau): Configurer le routage de la VM

Ouverture de ports pour ludo

07/14/2020 10:26 AM - François Poulain

Status:	Fermé	**Start date:**	07/14/2020
Priority:	Normale	**Due date:**	
Assignee:	François Poulain	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Sprint 2020 été		

Description

```
cpm_screen    PoluX: yop, hurdman travaille sur le Chapril
                PoluX: y-aurait des ports à rediriger vers la vm ludo
hurdman           o/
PoluX            plop
cpm_screen    PoluX: je te laisse voir avec lui et si tu pouvais le faire, comme je sais que tu ma
îtrises :D <333
PoluX            je suis de passage :)
                yep dites moi quels ports :)
hurdman           si possible 30000 à 30010 udp
cpm_screen    PoluX: merciiiiiiiiiiiiiii :D
hurdman           je n'utiliserai que 30 000 au départ, mais en prévision
```

Related issues:

Related to Infra Chapril - Anomalie #4601: Redémarrage difficile des vm coon	**Fermé**	**07/15/2020**

History

#1 - 07/14/2020 10:55 AM - François Poulain

Sur maine

Alors la VM ludo résoud ainsi :

```
=(^-^)=root@maine:~# host ludo
ludo.cluster.chapril.org has address 192.168.1.21
ludo.cluster.chapril.org has IPv6 address 2a01:4f8:10b:c41::21
```

Routage et DNAT

On ajoute sur maine la ligne suivante pour configurer le DNAT et le routage:

```
diff --git a/firehol/firehol.conf b/firehol/firehol.conf
index e6a8344..72b66be 100644
--- a/firehol/firehol.conf
+++ b/firehol/firehol.conf
@@ -25,6 +25,7 @@ declare -A dispatching=(
    ["xmpp1"]='(        "5222" "tcp"     "192.168.1.52" "2a01:4f8:10b:c41::52" "2a01:4f8:10b:c42::52")'
    ["xmpp2"]='(        "5223" "tcp"     "192.168.1.52" "2a01:4f8:10b:c41::52" "2a01:4f8:10b:c42::52")'
    ["xmpp3"]='(        "5269" "tcp"     "192.168.1.52" "2a01:4f8:10b:c41::52" "2a01:4f8:10b:c42::52")'
+["minetest"]='( "30000-30010" "    udp" "192.168.1.21" "2a01:4f8:10b:c41::21" "2a01:4f8:10b:c42::21")'
   ["mumble"]='(       "64738" "tcp udp" "192.168.1.64" "2a01:4f8:10b:c41::64" "2a01:4f8:10b:c42::64")'
     ["turn"]='(        "3478" "tcp udp" "192.168.1.64" "2a01:4f8:10b:c41::64" "2a01:4f8:10b:c42::64")'
    ["jitsi"]='(       "10000"     "udp" "192.168.1.64" "2a01:4f8:10b:c41::64" "2a01:4f8:10b:c42::64")'
```

- minetest : nom du protocole, voir plus bas
- 30000-30010: ports de destination
- udp: protocole
- 192.168.1.21: ipv4 pour le dnat

- 2a01:4f8:10b:c41::64 2a01:4f8:10b:c42::64: ipv6 pour le routage

Définition du protocole

« minetest » doit faire référence à quelque chose de connu par firehol. Soit c'est livré avec (cf https://firehol.org/services/) soit c'est à définir. Ici on défini dans le fichier /etc/firehol/services/minetest.conf :

```
#FHVER: 1:213
# La premiere ligne ci dessus est nécessaire !!
server_minetest_ports="udp/30000:30010"
client_minetest_ports="default"
```

Le nom du fichier importe peu mais la présence de « minetest » dans le contenu importe fortement.

Cf https://firehol.org/guides/adding-services/

Test et chargement des regles

```
firehol try
```

En cas de succès il va progressivement charger les regles, vous demander une interaction, vous demander la validation. Ça évite des situations de perte de contrôle.

```
=(^-^)=root@maine:/etc/firehol# firehol try
FireHOL: Saving active firewall to a temporary file...  OK
FireHOL: Processing file '/etc/firehol/firehol.conf'...  OK  (4792 iptables rules)

Your firewall is ready to be fast-activated...
If you don't continue, no changes will have been made to your firewall.
Activate the firewall? (just press enter to confirm or Control-C to stop) :

FireHOL: Fast activating new firewall...  OK
Keep the firewall? (type 'commit' to accept - 30 seconds timeout) : commit

Successfull activation of FireHOL firewall.
FireHOL: Saving activated firewall to '/var/spool/firehol'...  OK
```

En cas d'échec ça se passe differemment. Exemple :

```
=(^-^)=root@maine:/etc/firehol# firehol try
FireHOL: Saving active firewall to a temporary file...  OK
FireHOL: Processing file '/etc/firehol/firehol.conf'... /usr/sbin/firehol: line 9705: rules_minetest: command
not found

--------------------------------------------------------------------------------
 ERROR : # 1
WHEN   : Complex rules for rules_minetest() for server 'minetest'
WHY    :  There is no service 'minetest' defined.
COMMAND: server minetest accept
MODE   : ipv4
SOURCE : 183@/etc/firehol/firehol.conf: server:

/usr/sbin/firehol: line 9705: rules_minetest: command not found

--------------------------------------------------------------------------------
 ERROR : # 2
WHEN   : Complex rules for rules_minetest() for server 'minetest'
WHY    :  There is no service 'minetest' defined.
COMMAND: server minetest accept
MODE   : ipv6
SOURCE : 199@/etc/firehol/firehol.conf: server:

 FAILED
```

```
NOTICE: No changes made to your firewall.

FireHOL: Restoring old firewall...  OK

Message from syslogd@maine at Jul 14 10:37:18 ...
 FireHOL[7129]: FAILED to activate the firewall from /etc/firehol/firehol.conf. Last good firewall restoration
: OK.
```

Sur coon

On veillera à dupliquer la configuration précédente sur coon

Sur la VM (reste à faire)

Après avoir installé la VM et suivi https://admin.chapril.org/doku.php?id=admin:procedures:configuration-firewall-guest vous allez avoir un firewall local quasiment tout fermé.

Pour l'ouvrir il va falloir :

- reprendre le fichier de définition de service
- déclarer le service ouvert, par exemple avec la conf suivante dans /etc/firehol/firehol-ext2me.conf

```
# Services acceptés
server minetest accept
```

#2 - 07/14/2020 11:02 AM - Christian P. Momon

- Status changed from Nouveau to En cours de traitement

- Assignee set to François Poulain

- Parent task set to #3741

#3 - 07/14/2020 11:15 AM - François Poulain

- Assignee changed from François Poulain to Yves-Gaël Chény

- % Done changed from 0 to 100

#4 - 07/14/2020 11:56 AM - Christian P. Momon

- Assignee changed from Yves-Gaël Chény to François Poulain

- % Done changed from 100 to 0

Hurdman ne gère pas encore les tickets d'infra. Et il y a déjà un ticket pour le routage de la vm : #3741.

Donc si ticket ok alors le passer à résolu :D

Question subsidiaire :
["minetest"]='("30000" " udp" "192.168.1.21" "2a01:4f8:10b:c41::21" "2a01:4f8:10b:c42::21")'

Confirmes-tu qu'il faut rajouter une ligne pour chaque port de 30001 à 30010 ?

#5 - 07/14/2020 07:20 PM - François Poulain

> Confirmes-tu qu'il faut rajouter une ligne pour chaque port de 30001 à 30010 ?

Bonne question. :) J'avais pensé que non, mais en regardant le code iptable engendré je dubite. Peut être il faut 30000:30010 à la place de 30000. Il faudrait mettre en place une façon de tester (pour tcp je sais faire, pour udp je ne sais pas).

#6 - 07/14/2020 07:30 PM - François Poulain

Bon ça s'apprend.

Sur ludo :

```
# netcat -lup 30000
```

Sur ma machine:

```
netcat -u fip.chapril.org 30000
```

Ensuite ce que je tape apparait coté ludo. \o/

Par contre ça pas marche en 30001. Je corrige le fw.

#7 - 07/14/2020 07:51 PM - François Poulain

Ça marche coté ludo.

```
=(^-^)=root@ludo:~# netcat -lup 30001
plouf
sdmlfk
^C
=(^-^)=root@ludo:~# netcat -lup 30010
dsqmfkj
^C
```

#8 - 07/14/2020 07:54 PM - François Poulain

J'ai amendé plus haut pour backporter dans un howto sur le wiki.

#9 - 07/15/2020 02:38 AM - Christian P. Momon

Excellent le coup du netcat !

Alors, oui ça fonctionne en ipv4 mais :

- ça ne fonctionne pas en ipv6 ;
- ça fait planter le reboot du SI Chapril.

On y est presque :D

#10 - 07/15/2020 09:04 AM - François Poulain

> ça ne fonctionne pas en ipv6

Je ne vois pas le rapport. :)

> ça fait planter le reboot du SI Chapril.

Non plus. :)

#11 - 07/15/2020 10:49 AM - Christian P. Momon

Voici quelques traces :

```
=(^-^)=root@coon:/etc/libvirt/qemu# for host in $(ls *xml | sed -e 's/.xml//g'| grep -v modele) ; do virsh sta
rt $host ; done
error: Failed to start domain admin
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain allo
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain bastion
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain bla
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain dns
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain drop
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain lamp
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain libreoffice
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain ludo
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain mail
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain pad
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain pouet
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain sympa
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain valise
error: Requested operation is not valid: network 'default' is not active

error: Failed to start domain xmpp
error: Requested operation is not valid: network 'default' is not active

================================================================================================

En regardant Virtmanager > coon > réseaux virtuels > default > État, il est indiqué « inactif ».
Si activation alors :
Erreur lors du démarrage du réseau « default »: internal error: Network is already in use by interface virbr0
Traceback (most recent call last):
  File "/usr/share/virt-manager/virtManager/asyncjob.py", line 75, in cb_wrapper
    callback(asyncjob, *args, **kwargs)
  File "/usr/share/virt-manager/virtManager/asyncjob.py", line 111, in tmpcb
    callback(*args, **kwargs)
  File "/usr/share/virt-manager/virtManager/libvirtobject.py", line 66, in newfn
    ret = fn(self, *args, **kwargs)
  File "/usr/share/virt-manager/virtManager/network.py", line 76, in start
    self._backend.create()
  File "/usr/lib/python3/dist-packages/libvirt.py", line 2996, in create
    if ret == -1: raise libvirtError ('virNetworkCreate() failed', net=self)
libvirt.libvirtError: internal error: Network is already in use by interface virbr0

================================================================================================

juil. 15 00:57:44 coon.chapril.org icinga2[1305]: [2020-07-15 00:57:44 +0200] information/ApiListener: Finishe
d reconnecting to endpoint 'admin.cluster.chapril.org' via host 'admin.cluster.chapril.org' and port '5665'
juil. 15 00:57:44 coon.chapril.org systemd[1]: Reloading Postfix Mail Transport Agent.
```

```
juil. 15 00:57:44 coon.chapril.org systemd[1]: Reloaded Postfix Mail Transport Agent.
juil. 15 00:57:44 coon.chapril.org kernel: e1000e: enp1s0 NIC Link is Down
juil. 15 00:57:44 coon.chapril.org kernel: virbr0: port 2(enp1s0) entered disabled state
juil. 15 00:57:44 coon.chapril.org libvirtd[2697]: libvirt version: 5.0.0, package: 4+deb10u1 (Guido Günther <
agx@sigxcpu.org> Thu, 05 Dec 2019 00:22:14 +0100)
juil. 15 00:57:44 coon.chapril.org libvirtd[2697]: hostname: coon.chapril.org
juil. 15 00:57:44 coon.chapril.org libvirtd[2697]: Network name='default' uuid=0f6e21a4-a6e3-45fe-af5b-3af5361
ec327 is tainted: hook-script
juil. 15 00:57:44 coon.chapril.org libvirtd[2697]: internal error: Network is already in use by interface virb
r0
juil. 15 00:57:45 coon.chapril.org kernel: drop UNMATCHED IN-external_trIN=enp0s31f6 OUT= MAC=90:1b:0e:cb:cd:1
2:40:71:83:a5:f1:d0:08:00 SRC=185.39.11.32 DST=94.130.8.3 LEN=40 TOS=0x00 PREC=0x00 TTL=250 ID=60789 PROTO=TCP
 SPT=41728 DPT=622 WINDOW=1024 RES=0x00 SYN URGP=0
juil. 15 00:57:52 coon.chapril.org sshd[2762]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eui
d=0 tty=ssh ruser= rhost=222.186.173.226  user=root
juil. 15 00:57:52 coon.chapril.org systemd[1]: systemd-fsckd.service: Succeeded.
juil. 15 00:57:52 coon.chapril.org kernel: drbd coon: bind before connect failed, err = -99
juil. 15 00:57:52 coon.chapril.org kernel: drbd coon: conn( WFConnection -> Disconnecting )
juil. 15 00:57:53 coon.chapril.org kernel: drop UNMATCHED IN-external_trIN=enp0s31f6 OUT= MAC=90:1b:0e:cb:cd:1
2:40:71:83:a5:f1:d0:08:00 SRC=93.174.93.123 DST=94.130.8.3 LEN=40 TOS=0x00 PREC=0x00 TTL=250 ID=57905 PROTO=TC
P SPT=43411 DPT=11395 WINDOW=1024 RES=0x00 SYN URGP=0
juil. 15 00:57:54 coon.chapril.org sshd[2762]: Failed password for root from 222.186.173.226 port 62800 ssh2
juil. 15 00:57:54 coon.chapril.org icinga2[1305]: [2020-07-15 00:57:54 +0200] information/ApiListener: Reconne
cting to endpoint 'admin.cluster.chapril.org' via host 'admin.cluster.chapril.org' and port '5665'
juil. 15 00:57:54 coon.chapril.org FireHOL[2965]: FireHOL started from '/' with: /usr/sbin/firehol start
juil. 15 00:57:54 coon.chapril.org FireHOL[2967]: Saving active firewall to a temporary file started
juil. 15 00:57:54 coon.chapril.org delayed_fw_reload[2714]: FireHOL: Saving active firewall to a temporary fil
e...  OK
juil. 15 00:57:54 coon.chapril.org FireHOL[2979]: Saving active firewall to a temporary file succeeded
juil. 15 00:57:54 coon.chapril.org FireHOL[2980]: Processing file '/etc/firehol/firehol.conf' started
juil. 15 00:57:55 coon.chapril.org drbd[1324]: WARN: stdin/stdout is not a TTY; using /dev/console
juil. 15 00:57:55 coon.chapril.org drbd[1324]: .
juil. 15 00:57:55 coon.chapril.org systemd[1]: Started LSB: Control DRBD resources..
juil. 15 00:57:55 coon.chapril.org kernel: drbd maine: bind before connect failed, err = -99
juil. 15 00:57:55 coon.chapril.org kernel: drbd maine: conn( WFConnection -> Disconnecting )
```

#12 - 07/15/2020 03:29 PM - François Poulain

Après une longue investigation avec Christian, on a tiqué sur :

```
Jul 15 00:01:20 coon delayed_fw_reload[1616]: ERROR: FireHOL is already running. Exiting...
```

On soupçonne une race condition qui apparait du fait que les regles iptables deviennent nombreuses (4000).

En regardant la conf systemd de libvirtd sur coon on tombe sur :

```
  Drop-In: /etc/systemd/system/libvirtd.service.d
           └─override.conf
[...]
  Process: 1441 ExecStartPost=/usr/local/bin/delayed_fw_reload (code=exited, status=0/SUCCESS)
```

Ça ressemble à une cochonceté oubliée, datant des premiers jours du cluster. Depuis, les hooks network on rendu ça inutiles.

Par ailleurs le code impliqué est plus que naïf.

```
# cat /usr/local/bin/delayed_fw_reload
#!/bin/bash

sleep 10 && firehol start
```

Je dégage tout ça de coon. Maine en est exempt.

#13 - 07/15/2020 04:37 PM - Christian P. Momon

- Status changed from En cours de traitement to Résolu

Redémarrage fait nominalement avec les modifs minetest. Donc nous validons que ça venait de ça \o/

Et les tests d'ouverture de port du range pour minetest sont OK. Fermeture du ticket :D

#14 - 07/15/2020 04:46 PM - Christian P. Momon

- Related to Anomalie #4601: Redémarrage difficile des vm coon added

#15 - 07/15/2020 05:01 PM - Christian P. Momon

Pour des raisons de simplicité, le domaine minetest n'est configuré que pour ipv4.

#16 - 09/01/2020 11:41 PM - Christian P. Momon

- Status changed from Résolu to Fermé

#17 - 09/03/2020 03:41 AM - Christian P. Momon

- Target version changed from Backlog to Sprint 2020 été