

## Admins - Anomalie #1115

### controller.vm.april-int openvpn est tombé

16/12/2012 18:02 - Loïc Dachary

<b>Statut:</b>	Fermé	<b>Début:</b>	16/12/2012
<b>Priorité:</b>	Immédiate	<b>Echéance:</b>	
<b>Assigné à:</b>	Loïc Dachary	<b>% réalisé:</b>	100%
<b>Catégorie:</b>	Task	<b>Temps estimé:</b>	0.00 heure
<b>Version cible:</b>	Décembre 2012 (2/2)	<b>Temps passé:</b>	2.00 heures
<b>Difficulté:</b>	3 Moyen		

#### Description

openvpn ne fonctionne plus sur controller.vm.april-int. Il est relancé. Un effet de bord est que toutes les instances openstack ne ping plus 192.168.0.0/16. Sur nagios.vm.april-int par exemple:

```
root@nagios:~# ip r
default via 10.145.4.4 dev eth0
10.145.4.0/24 dev eth0 proto kernel scope link src 10.145.4.9
192.168.0.0/16 via 192.168.4.1 dev eth0 src 192.168.4.5
192.168.4.0/24 dev eth0 proto kernel scope link src 192.168.4.5
root@nagios:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:1a:bb:7b brd ff:ff:ff:ff:ff:ff
    inet 10.145.4.9/24 brd 10.145.4.255 scope global eth0
    inet 192.168.4.5/24 scope global eth0
    inet6 fe80::f816:3eff:fe1a:bb7b/64 scope link tentative dadfailed
        valid_lft forever preferred_lft forever
```

malgré tout c'est **10.145.4.4** qui est utilisé pour router **192.168.2.12** au lieu de **192.168.4.1**

```
root@nagios:~# ip r get 192.168.2.12
192.168.2.12 via 10.145.4.4 dev eth0 src 192.168.4.5
    cache <redirected> ipid 0x8c6f
```

ce qui est **probablement** un effet de bord du fait que la route vers **192.168.2.12** a échoué pendant la panne du VPN et que la route par défaut a été utilisée a la place. Pour rétablir la situation il suffit de flusher le cache:

```
root@nagios:~# ip r flush cache
root@nagios:~# ip r get 192.168.2.12 from 192.168.4.5
192.168.2.12 from 192.168.4.5 via 192.168.4.1 dev eth0
    cache ipid 0x8c6f
```

#### Historique

##### #1 - 17/12/2012 10:35 - Loïc Dachary

Pour reproduire le problème:

```
ssh root@controller.vm.april-int
root@controller:~# ip r
default via 10.145.4.4 dev eth0
10.145.4.0/24 dev eth0 proto kernel scope link src 10.145.4.5
192.168.0.0/24 via 192.168.0.21 dev tun0 src 192.168.4.1
192.168.0.21 dev tun0 proto kernel scope link src 192.168.0.22
192.168.1.0/24 via 192.168.0.21 dev tun0
```

```

192.168.2.0/24 via 192.168.0.21 dev tun0
192.168.3.0/24 via 192.168.0.21 dev tun0
192.168.4.0/24 dev eth0 proto kernel scope link src 192.168.4.1
192.168.5.0/24 via 192.168.0.21 dev tun0
root@controller:~# ip r show cache 192.168.42.42
root@controller:~#
root@controller:~# ping -c1 192.168.42.42
PING 192.168.42.42 (192.168.42.42) 56(84) bytes of data.
From 212.27.40.57 icmp_seq=1 Packet filtered
--- 192.168.42.42 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
root@controller:~# ip r show cache 192.168.42.42
192.168.42.42 via 10.145.4.4 dev eth0 src 10.145.4.5
    cache
192.168.42.42 from 10.145.4.5 via 10.145.4.4 dev eth0
    cache

```

## #2 - 17/12/2012 10:59 - Loïc Dachary

- Statut changé de *En cours de traitement* à *Résolu*

```

commit 54aa1c40732654736401962f0775e94b10456169
Author: Loic Dachary <loic@dachary.org>
Date: Mon Dec 17 09:55:23 2012 +0000

```

```

flush all routes when the VPN goes up to discard incorrect cached routes https://agir.april.org/issues/111
5

```

```

diff --git a/.etckeeper b/.etckeeper
index ba2ed97..c69f180 100755
--- a/.etckeeper
+++ b/.etckeeper
@@ -441,6 +441,8 @@ maybe chmod 0644 './openvpn/keys/ca.crt'
    maybe chmod 0644 './openvpn/keys/yopo.crt'
    maybe chmod 0644 './openvpn/keys/yopo.csr'
    maybe chmod 0600 './openvpn/keys/yopo.key'
+maybe chgrp staff './openvpn/route-flush'
+maybe chmod 0755 './openvpn/route-flush'
    maybe chmod 0755 './openvpn/update-resolv-conf'
    maybe chmod 0755 './opt'
    maybe chmod 0644 './os-release'
diff --git a/openvpn/client.conf b/openvpn/client.conf
index 743a6fa..168f74a 100644
--- a/openvpn/client.conf
+++ b/openvpn/client.conf
@@ -133,4 +133,6 @@ mute 20
    log /var/log/openvpn/openvpn.log
    log-append /var/log/openvpn/openvpn.log

```

```

-
+script-security 2
+# for more information https://agir.april.org/issues/1115
+up /etc/openvpn/route-flush
diff --git a/openvpn/route-flush b/openvpn/route-flush
new file mode 100755
index 0000000..384dc57
--- /dev/null
+++ b/openvpn/route-flush
@@ -0,0 +1,2 @@
+#!/bin/bash
+/sbin/ip route flush cache

```

## #3 - 17/12/2012 10:59 - Loïc Dachary

- % réalisé changé de 0 à 100

## #4 - 17/12/2012 12:41 - Loïc Dachary

Si le controller envoie des ICMP redirect c'est pas bon. On tente de le desactiver mais il envoie encore des redirect.

```

root@controller:~# tcpdump -i eth0 host jenkins.vm.april-int
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:38:05.968852 IP 192.168.4.3 > 192.168.20.238: ICMP echo request, id 22377, seq 1, length 64

```

```
11:38:05.968899 IP 192.168.4.1 > 192.168.4.3: ICMP redirect 192.168.20.238 to host 10.145.4.4, length 92
11:38:05.968926 IP 192.168.4.3 > 192.168.20.238: ICMP echo request, id 22377, seq 1, length 64
11:38:10.977876 ARP, Request who-has 192.168.4.3 tell 192.168.4.1, length 28
11:38:10.978251 ARP, Reply 192.168.4.3 is-at fa:16:3e:54:fc:2f (oui Unknown), length 28
^C
5 packets captured
9 packets received by filter
0 packets dropped by kernel
root@controller:~# sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0
```

**#5 - 17/12/2012 13:55 - Loïc Dachary**

<http://dachary.org/?p=1704> flushing OpenVPN routes to prevent temporary incorrect routing

**#6 - 29/05/2019 12:19 - Quentin Gibeaux**

- Statut changé de Résolu à Fermé