TP HAProxy

2 serveurs web sont requis.

Installation HAProxy

```
duncan@duncan-VirtualBox:~$ sudo apt install haproxy
```

Configuration d'HAProxy

Ligne à ajouter à la fin du fichier **/etc/haproxy/haproxy.cfg**

```
listen cluster_web
    bind *:80
    mode http
    balance roundrobin

    option httpclose
    option forwardfor

    server web1 10.1.43.2:80 check
    server web2 10.1.43.3:80 check

    stats enable
    stats hide-version
    stats refresh 30s
    stats show-node
    stats auth admin:admin
    stats uri /stats
```

Les IP sont à changer en fonction des votre :

- La première est l'adresse de votre serveur HAProxy
- Les 2 autres sont les IP de vos serveur web

Vérification du service HAProxy

```
duncan@duncan-VirtualBox:~$ sudo service haproxy status
● haproxy.service - HAProxy Load Balancer
     Loaded: loaded (/lib/systemd/system/haproxy.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-11-15 09:51:08 CET; 4s ago
       Docs: man:haproxy(1)
             file:/usr/share/doc/haproxy/configuration.txt.gz
    Process: 4250 ExecStartPre=/usr/sbin/haproxy -Ws -f $CONFIG -c -q $EXTRAOPTS (code=exited, status=0/SUCCESS)
   Main PID: 4252 (haproxy)
      Tasks: 3 (limit: 2270)
     Memory: 69.7M
        CPU: 198ms
     CGroup: /system.slice/haproxy.service
             ├─4252 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid -S /run/haproxy-master.sock
             └─4254 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid -S /run/haproxy-master.sock
```

Configuration Serveur Web

Serveur web 1

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:55:b1:fb brd ff:ff:ff:ff:ff:ff
    inet 10.1.43.2/24 brd 10.1.43.255 scope global noprefixroute enp0s3
```

```
duncan@serverweb1:~$ ip route list
default via 10.1.43.1 dev enp0s3 proto static metric 20100
```

Serveur web 2

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:df:fb:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.1.43.3/24 brd 10.1.43.255 scope global noprefixroute enp0s3
```

```
duncan@serverweb2:~$ ip route list
default via 10.1.43.1 dev enp0s3 proto static metric 20100
```

Modification **/var/www/index.html**

Serveur web 1

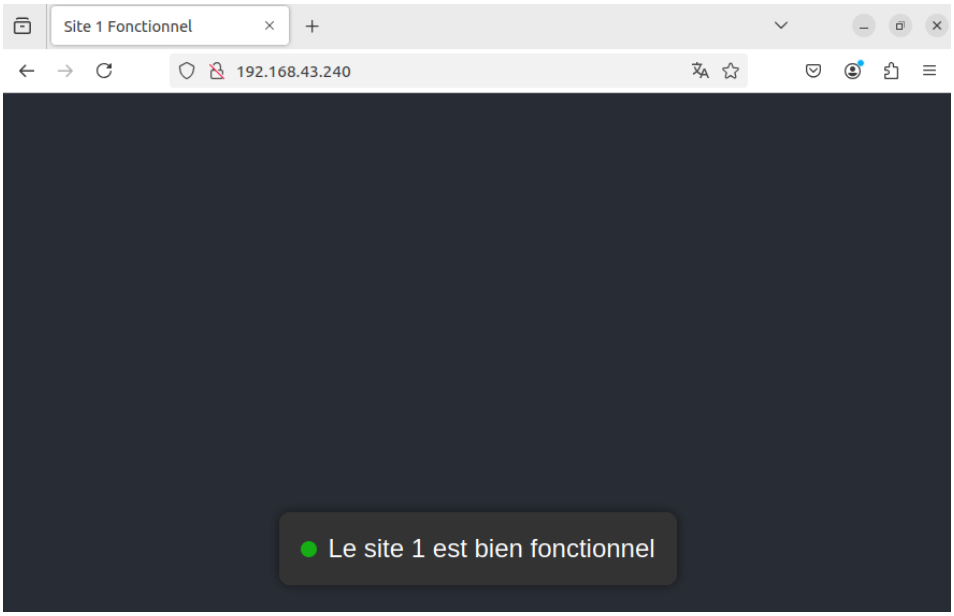
```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Site 1 Fonctionnel</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="status-message">
        <span class="status-dot"></span> Le site 1 est bien fonctionnel
    </div>
</body>
</html>
```

Serveur web 2

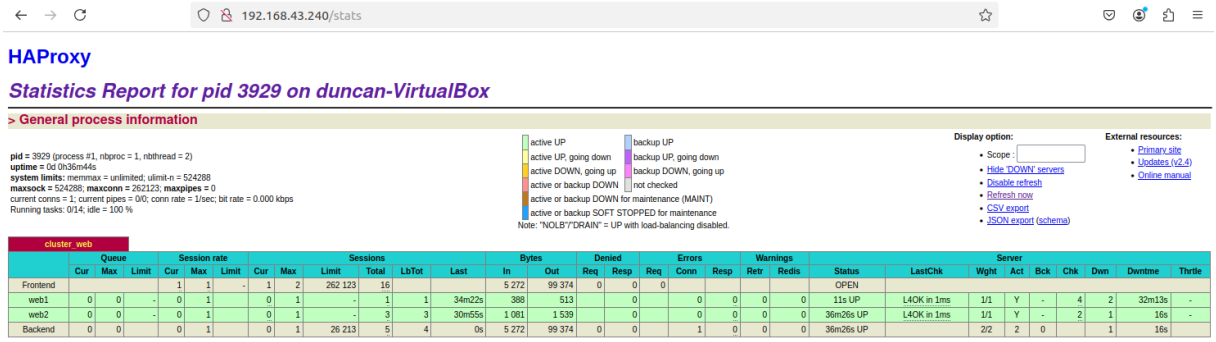
```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Site 2 Fonctionnel</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="status-message">
        <span class="status-dot"></span> Le site 2 est bien fonctionnel
    </div>
</body>
</html>
```

Test

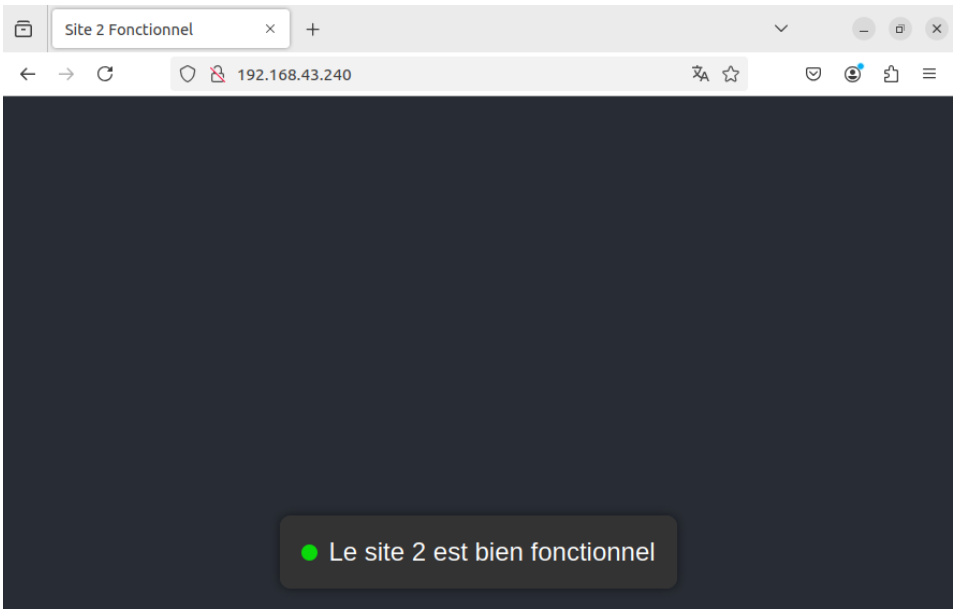
Connexion au serveur HAProxy sur la machine client



Vérification des machines

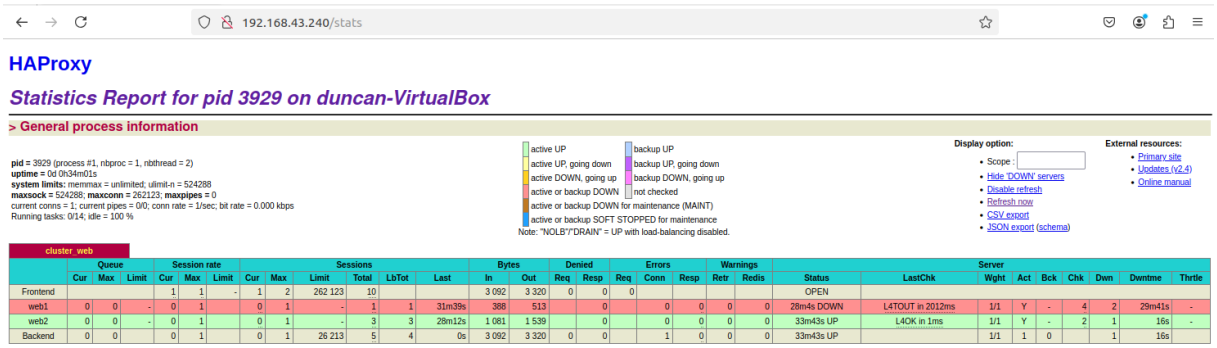


Désactivation du Serveur web 1



Le serveur HAProxy a bien basculé sur le Serveur web 2

On peut voir que le serveur web 1 est bien hors ligne et que le serveur web 2 a pris le relais.



Création du script pour le firewall

```
duncan@duncan-VirtualBox:~$ sudo cat /etc/init.d/firewall
#!/bin/bash

start() {
    echo -n "Application des règles iptables: "

    iptables -F
    iptables -X
    iptables -t nat -F

    sysctl -w net.ipv4.ip_forward=1

    iptables -P FORWARD DROP

    iptables -A FORWARD -d 10.1.43.2 -j ACCEPT
    iptables -A FORWARD -s 10.1.43.2 -j ACCEPT
    iptables -A FORWARD -d 10.1.43.3 -j ACCEPT
    iptables -A FORWARD -s 10.1.43.3 -j ACCEPT

    iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

    iptables -t nat -A PREROUTING -p tcp -d 192.168.43.240 --dport 2221 -j DNAT --to-destination 10.1.43.2:22
    iptables -t nat -A PREROUTING -p tcp -d 192.168.43.240 --dport 2222 -j DNAT --to-destination 10.1.43.2:22

    echo "Termine."
}

stop() {
    echo -n "Suppression des règles iptables: "

    iptables -F
    iptables -X
    iptables -t nat -F

    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT

    echo "Termine."
}
```

```
case $1 in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        stop
        start
        ;;
    status)
        /sbin/iptables -L
        /sbin/iptables -t nat -L
        ;;
    *)
        echo "Usage: $0 {start|stop|restart|status}"
        exit 1
        ;;
esac
exit 0
```

Changement des droit pour que le fichier puisse être éxecuté

```
duncan@duncan-VirtualBox:~$ sudo chmod +x /etc/init.d/firewall
```

Redémarrage du daemon

```
duncan@duncan-VirtualBox:~$ sudo systemctl daemon-reload
```

Démarrage du service firewall

```
duncan@duncan-VirtualBox:~$ sudo service firewall start
```

Vérification des règles avec iptable

```
duncan@duncan-VirtualBox:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             10.1.43.2
ACCEPT     all  --  10.1.43.2            anywhere
ACCEPT     all  --  anywhere             10.1.43.3
ACCEPT     all  --  10.1.43.3            anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
duncan@duncan-VirtualBox:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             duncan-VirtualBox    tcp dpt:2221 to:10.1.43.2:22
DNAT       tcp  --  anywhere             duncan-VirtualBox    tcp dpt:2222 to:10.1.43.2:22

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
```

Test

Connexion ssh depuis le client ubuntu aux serveurs web

```
duncan@clientubuntu:~$ sudo ssh duncan@10.1.43.2
[sudo] password for duncan:
duncan@10.1.43.2's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Fri Nov 15 16:13:41 2024 from 10.1.43.1
duncan@serverweb1:~$
```

```
duncan@clientubuntu:~$ sudo ssh duncan@10.1.43.3
The authenticity of host '10.1.43.3 (10.1.43.3)' can't be established.
ED25519 key fingerprint is SHA256:LUPAo9mGKG6+yxt+krp0ClaGO+yzvV/SxNB7YmWl3Oc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.43.3' (ED25519) to the list of known hosts.
duncan@10.1.43.3's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Fri Sep  6 14:53:31 2024 from 192.168.150.51
duncan@serverweb2:~$
```

Désactivation du service firewall

```
duncan@duncan-VirtualBox:~$ sudo service firewall stop
```

Nouveau test

L’accès est refusé grâce aux règles du firewall