Mise en Place d'un Service Web

I. Installation d'un service WEB (nginx)

a. Installations Packages

```
[root@localhost ~]# dnf install nginx
Rocky Linux 9 - BaseOS                                          3.3 MB/s | 2.3 MB     00:00
Rocky Linux 9 - AppStream                                       8.1 MB/s | 8.3 MB     00:01
Rocky Linux 9 - Extras                                           50 kB/s |  16 kB     00:00
Dependencies resolved.
================================================================================================
 Package                 Architecture        Version                    Repository          Size
================================================================================================
Installing:
 nginx                   x86_64              2:1.20.1-20.el9.0.1        appstream           36 k
```

```
[root@localhost ~]# dnf install php-fpm
Last metadata expiration check: 0:00:50 ago on Sat Dec 14 15:29:31 2024.
Dependencies resolved.
================================================================================================
 Package                 Architecture        Version                    Repository          Size
================================================================================================
Installing:
 php-fpm                 x86_64              8.0.30-1.el9_2             appstream          1.6 M
Installing dependencies:
```

```
[root@localhost ~]# dnf install mariadb-server
Last metadata expiration check: 0:01:17 ago on Sat Dec 14 15:29:31 2024.
Dependencies resolved.
================================================================================================
 Package                 Architecture        Version                    Repository          Size
================================================================================================
Installing:
 mariadb-server          x86_64              3:10.5.22-1.el9_2          appstream          9.6 M
Upgrading:
 audit                   x86_64              3.1.5-1.el9                baseos             254 k
 audit-libs              x86_64              3.1.5-1.el9                baseos             120 k
```

```
[root@localhost ~]# dnf install php
Last metadata expiration check: 0:03:39 ago on Sat Dec 14 15:29:31 2024.
Dependencies resolved.
================================================================================================
 Package                 Architecture        Version                    Repository          Size
================================================================================================
Installing:
 php                     x86_64              8.0.30-1.el9_2             appstream          7.7 k
Installing dependencies:
```

```
[root@localhost ~]# dnf install php-mysqlnd
Last metadata expiration check: 0:04:10 ago on Sat Dec 14 15:29:31 2024.
Dependencies resolved.
================================================================================================
 Package                 Architecture        Version                    Repository          Size
================================================================================================
Installing:
 php-mysqlnd             x86_64              8.0.30-1.el9_2             appstream          148 k

Transaction Summary
================================================================================================
```

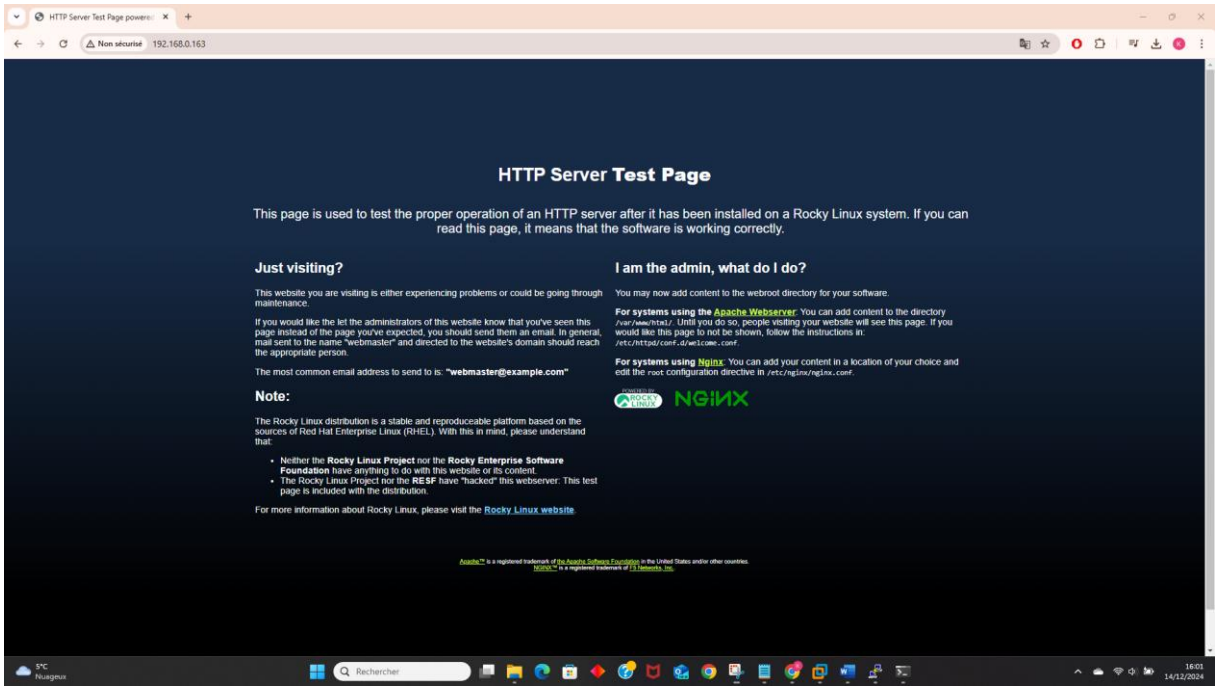
b. Création fichier de log

```
[root@localhost nginx]# cat > error.log
```

```
[root@localhost ~]# cd /var/log/nginx/
[root@localhost nginx]# ls
error.log
[root@localhost nginx]#
```

c. Firewall

```
[root@localhost ~]# firewall-cmd --list-service
cockpit dhcpv6-client ssh
[root@localhost ~]# firewall-cmd --permanent --add-service=http
success
[root@localhost ~]# forewall-cmd --reload
-bash: forewall-cmd: command not found
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```



d. Test port 8080

```
server {
    listen       8080;
    listen       [::]:8080;
    server_name  _;
    root         /usr/share/nginx/html;
```

II. Installation moteur BDD

a. Configuration Mariadb

```
[root@localhost nginx]# systemctl enable --now mariadb.service
Created symlink /etc/systemd/system/mysql.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/systemd/system/mariadb.service
.
[root@localhost nginx]#
```

```
[root@localhost nginx]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.
```

b. Création BDD

```
[root@localhost nginx]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.5.22-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE KHALEDBDD;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'Khaled'@'localhost' IDENTIFIED BY 'root';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON BDD.* TO 'Khaled'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW DATABASES
    -> .
    -> .
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server ve
rsion for the right syntax to use near '.
.' at line 2
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| KHALEDBDD          |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.001 sec)
```

```
MariaDB [(none)]> USE KHALEDBDD
Database changed
MariaDB [KHALEDBDD]> SHOW TABLES
    -> ;
Empty set (0.000 sec)

MariaDB [KHALEDBDD]>
```

III. Déploiement du site FR

```
[root@localhost ~]# mkdir -p /var/www/ecommerce.fr
[root@localhost ~]# cd /var/www
[root@localhost www]# ls
cgi-bin  ecommerce.fr  html
[root@localhost www]#
```

```
[root@localhost www]# cd /var/www/ecommerce.fr
[root@localhost ecommerce.fr]# ls
PricingSubscription
[root@localhost ecommerce.fr]# cd /var/www/ecommerce.fr/PricingSubscription/
[root@localhost PricingSubscription]# ls
config.php  css  database.sql  images  js  sign-up.php
[root@localhost PricingSubscription]#
```

root@localhost:/etc/php-fpm.d

```
  GNU nano 5.6.1                          www.conf                          Modified
; Start a new pool named 'www'.
; the variable $pool can be used in any directive and will be replaced by the
; pool name ('www' here)
[www]

; Per pool prefix
; It only applies on the following directives:
; - 'access.log'
; - 'slowlog'
; - 'listen' (unixsocket)
; - 'chroot'
; - 'chdir'
; - 'php_values'
; - 'php_admin_values'
; When not set, the global prefix (or @php_fpm_prefix@) applies instead.
; Note: This directive can also be relative to the global prefix.
; Default Value: none
;prefix = /path/to/pools/$pool

; Unix user/group of processes
; Note: The user is mandatory. If the group is not set, the default user's group
;       will be used.
; RPM: apache user chosen to provide access to the same directories as httpd
user = nginx
; RPM: Keep a group allowed to write in log dir.
group = nginx

; The address on which to accept FastCGI requests.
; Valid syntaxes are:
;   'ip.add.re.ss:port'    - to listen on a TCP socket to a specific IPv4 address on
;                            a specific port;
;   '[ip:6:addr:ess]:port' - to listen on a TCP socket to a specific IPv6 address on
;                            a specific port;
;   'port'                 - to listen on a TCP socket to all addresses
;                            (IPv6 and IPv4-mapped) on a specific port;
;   '/path/to/unix/socket' - to listen on a unix socket.
; Note: This value is mandatory.
listen = /run/php-fpm/www.sock
```

```
[root@localhost php-fpm.d]# systemctl start php-fpm
[root@localhost php-fpm.d]# systemctl reload nginx
```

```
[root@localhost ~]# cd /etc/nginx/conf.d
[root@localhost conf.d]# ls
php-fpm.conf
[root@localhost conf.d]# cat > site_commerce.fr.conf

^C
[root@localhost conf.d]# ls
php-fpm.conf  site_commerce.fr.conf
[root@localhost conf.d]#
```

root@localhost:/etc/nginx/conf.d

```
  GNU nano 5.6.1                                site_commerce.fr.conf
server {
listen 80;
listen [::]:80;
root /var/www/ecommerce.fr/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.fr ;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.fr.log;
error_log /var/log/nginx/error_ecommerce.fr.log;
location / {
try_files $uri $uri/ =404;
}
}
```

root@localhost:/var/www/ecommerce.fr/PricingSubscription

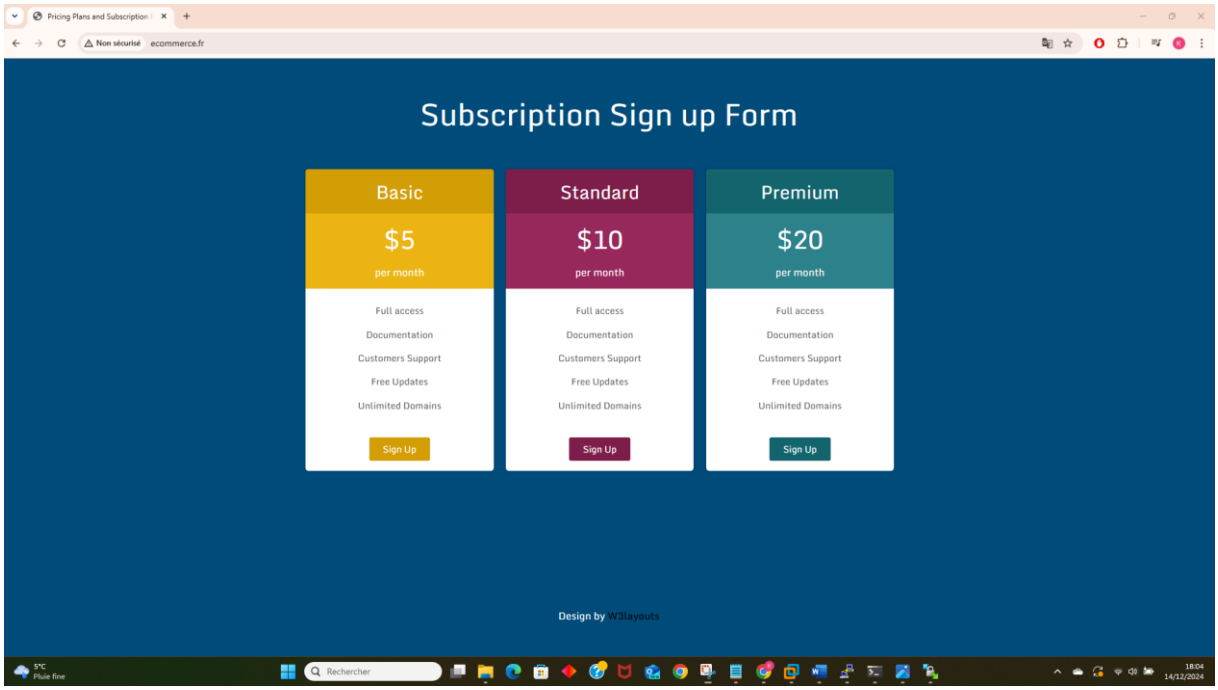
```
  GNU nano 5.6.1                          config.php                    Modified
<?php
$SETTINGS["mysql_user"]='Khaled';
$SETTINGS["mysql_pass"]='root';
$SETTINGS["hostname"]='localhost';
$SETTINGS["mysql_database"]='KHALEDBDD';
$SETTINGS["data_table"]='registrations';
$SETTINGS["paypal_address"]='email@domain.com';
?>
```

```
[root@localhost PricingSubscription]# mysql -u Khaled -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19
Server version: 10.5.22-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE KHALEDBDD
Database changed
MariaDB [KHALEDBDD]> SOURCE /var/www/ecommerce.fr/PrincingSubscription/database.sql
ERROR: Failed to open file '/var/www/ecommerce.fr/PrincingSubscription/database.sql', error: 2
MariaDB [KHALEDBDD]> source /var/www/ecommerce.fr/PrincingSubscription/database.sql
ERROR: Failed to open file '/var/www/ecommerce.fr/PrincingSubscription/database.sql', error: 2
MariaDB [KHALEDBDD]> source /var/www/ecommerce.fr/PricingSubscription/database.sql
Query OK, 0 rows affected (0.319 sec)

MariaDB [KHALEDBDD]>
```

Sans titre | infos_cles.txt | httpsw | MALKI | jdussa | ESXI | server | hosts

Fichier Modifier Affichage

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
      192.168.0.163     ecommerce.fr

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```



IV. Déploiement du site UK

```
[root@localhost html]# cd ~
[root@localhost ~]# mkdir -p /var/www/ecommerce.uk
[root@localhost ~]# cd /var/www
[root@localhost www]# ls
cgi-bin  ecommerce.fr  ecommerce.uk  html
[root@localhost www]# cd /var/www/ecommerce.uk
[root@localhost ecommerce.uk]# ls
PricingSubscription
[root@localhost ecommerce.uk]#
```

root@localhost:/etc/nginx/conf.d

```
 GNU nano 5.6.1                          site_commerce.uk.conf                          Modified
server {
listen 80;
listen [::]:80;
root /var/www/ecommerce.uk/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.uk ;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.uk.log;
error_log /var/log/nginx/error_ecommerce.uk.log;
location / {
try_files $uri $uri/ =404;
}
}
```

root@localhost:/var/www/ecommerce.uk/PricingSubscription

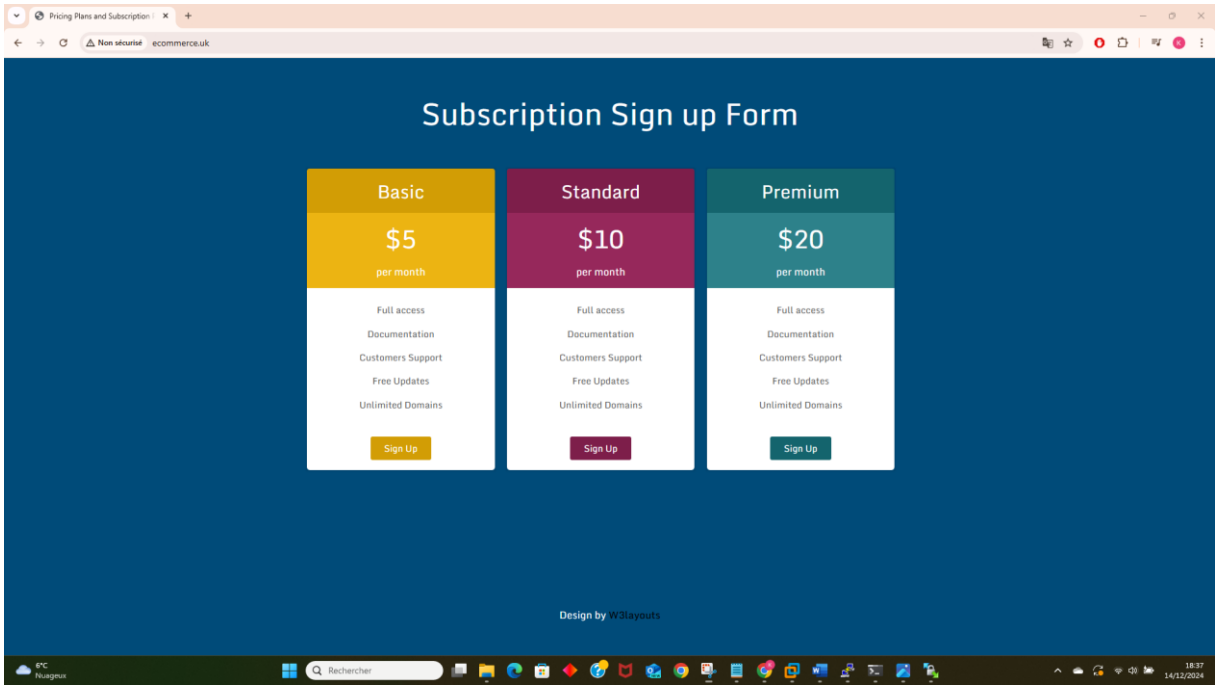
```
 GNU nano 5.6.1                              config.php                                 Modified
<?php
$SETTINGS["mysql_user"]='Khaled';
$SETTINGS["mysql_pass"]='root';
$SETTINGS["hostname"]='localhost';
$SETTINGS["mysql_database"]='KHALEDBDD';
$SETTINGS["data_table"]='registrations';
$SETTINGS["paypal_address"]='email@domain.com';
?>
```

```
[root@localhost PricingSubscription]# mysql -u Khaled -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 20
Server version: 10.5.22-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE KHALEDBDD
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [KHALEDBDD]> SOURCE /var/www/ecommerce.uk/PricingSubscription/database.sql
Query OK, 0 rows affected, 1 warning (0.000 sec)

MariaDB [KHALEDBDD]>
```

Sans titre | infos_cles.txt | httpsw | MALKI | jdussa | ESXI | server | hosts

Fichier Modifier Affichage

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
      192.168.0.163     ecommerce.fr
      192.168.0.163     ecommerce.uk

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```



V. Restriction accès IP

a. Création fichier blockip.conf

```
[root@localhost ~]# cd /etc/nginx
[root@localhost nginx]# cat > blockip.conf
^C
[root@localhost nginx]# ls
blockip.conf  fastcgi.conf.default    koi-win            nginx.conf.default   uwsgi_params.default
conf.d        fastcgi_params          mime.types         scgi_params          win-utf
default.d     fastcgi_params.default  mime.types.default  scgi_params.default
fastcgi.conf  koi-utf                 nginx.conf         uwsgi_params
[root@localhost nginx]#
```

root@localhost:/etc/nginx

```
 GNU nano 5.6.1                          blockip.conf                          Modified
deny 192.168.1.14;
```

b. Ajouter blockip.conf dans site_commerce.fr.conf

root@localhost:/etc/nginx/conf.d

```
 GNU nano 5.6.1                       site_commerce.fr.conf
server {
listen 80;
listen [::]:80;
root /var/www/ecommerce.fr/PricingSubscription/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.fr ;
include /etc/nginx/blockip.conf;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.fr.log;
error_log /var/log/nginx/error_ecommerce.fr.log;
location / {
try_files $uri $uri/ =404;
}
}
```

```
[root@localhost conf.d]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[root@localhost conf.d]# systemctl restart nginx
[root@localhost conf.d]#
```

VI. Logs (Goaccess)

```
[root@localhost conf.d]# dnf install epel-release -y
Last metadata expiration check: 2:34:03 ago on Sat Dec 14 16:35:31 2024.
Dependencies resolved.
================================================================================
 Package              Architecture        Version              Repository     Size
================================================================================
Installing:
 epel-release         noarch              9-7.el9              extras         19 k

Transaction Summary
================================================================================
```

```
[root@localhost conf.d]# dnf install goaccess
Extra Packages for Enterprise Linux 9 - x86_64                  9.3 MB/s |  23 MB     00:02
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64   3.4 kB/s | 2.5 kB     00:00
Dependencies resolved.
================================================================================
 Package                Architecture            Version                 Repository                  Size
================================================================================
Installing:
 goaccess               x86_64                  1.9.3-2.el9             epel                       456 k
Installing dependencies:
```

```
[root@localhost conf.d]# goaccess -f /var/log/access.log
```

root@localhost:/etc/nginx/conf.d

```
+-------------------------------------------------------------------------+
| Log Format Configuration                                                |
| [SPACE] to toggle - [ENTER] to proceed - [q] to quit                    |
|                                                                         |
| [x] NCSA Combined Log Format                                            |
| [ ] NCSA Combined Log Format with Virtual Host                          |
| [ ] Common Log Format (CLF)                                             |
| [ ] Common Log Format (CLF) with Virtual Host                           |
| [ ] W3C                                                                 |
| [ ] CloudFront (Download Distribution)                                  |
|                                                                         |
| Log Format - [c] to add/edit format                                     |
| %h %^[%d:%t %^] "%r" %s %b "%R" "%u"                                    |
|                                                                         |
| Date Format - [d] to add/edit format                                    |
| %d/%b/%Y                                                                |
|                                                                         |
| Time Format - [t] to add/edit format                                    |
| %H:%M:%S                                                                |
+-------------------------------------------------------------------------+
```

VII. Sécurisation d'un service WEB (nginx)

```
[root@localhost ~]# mkdir /etc/ssl/private
[root@localhost ~]# chmod 700 /etc/ssl/private
```

```
[root@localhost ~]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/priv
ate/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
.....+.+..++++++++++++++++++++++++++++++++++++++++++*.+..+...+.+.....+.+......+.....+.....
.+.......++++++++++++++++++++++++++++++++++++++++*.....+..+.........+..............+...+.++++
++
.+..++++++++++++++++++++++++++++++++++++*......+....+.....+................+..+......+.
...+...+.....+...+...++++++++++++++++++++++++++++++++++++++*....+...+......+.....+....+.....
+..........+...+..+.....+.+......+...+.....+.+......+........+....+...+...+...........+...+
..........+.....+...+...+.+......+.........+...+...........+.+.........+..+.......+..+...+...
+.........+......+...+....+......+.............+.......+...+......+..+....+......+..+.+.....
+......+.+..+......+....+..+.............+.............+.+...+..........+....+......+...
.....+...+...+....+...+........+.+......+.....+.......+...+..+......+....+......+.....
+..+...+................+.+...+...+..+.......+.....+....+......+.....+.........+...+..+...
.......+...+......+.....+......+.+.........+...+.....+.+..+....+................+..+....+..
..........+........+....+...........+......+.+........+.......+.....+................+....
....+...+....+...+...+..+.+...........+.+................+.......+...+..+.+........+......+.
...+......+.....+....+..+...+.......+..+.....................+.+........+.......+.....+...+..
........+......+.....+.......+..+.+......+..........+...+.+...+.....+.........+..+.+.......
.+......+.........+.......+.....+.........+....+.....+....+.....+.+..+....+..........++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
[root@localhost ~]# openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
Generating DH parameters, 2048 bit long safe prime
.....................................................................................................
.....................................................................................................
.....................................................................+...............
.....................................................................................................
```

root@localhost:/etc/nginx/conf.d

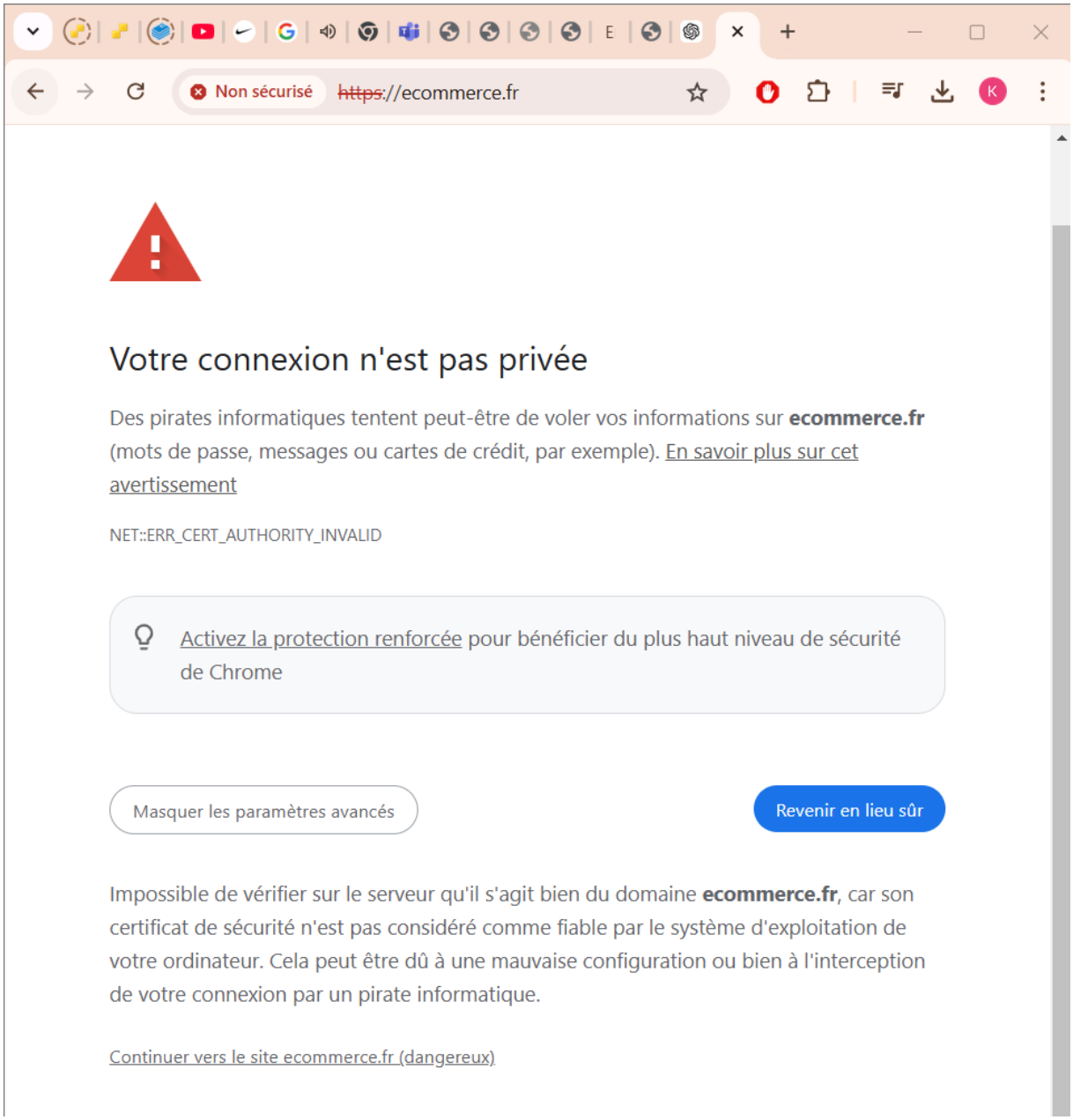
```
  GNU nano 5.6.1                          site_commerce.fr.conf
server {
listen 80;
listen [::]:80;
root /var/www/ecommerce.fr/PricingSubscription/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.fr ;
include /etc/nginx/blockip.conf;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.fr.log;
error_log /var/log/nginx/error_ecommerce.fr.log;
location / {
try_files $uri $uri/ =404;
}
}

server {
listen 443 http2 ssl;
listen [::]:443 http2 ssl;
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
ssl_dhparam /etc/ssl/certs/dhparam.pem;
root /var/www/ecommerce.fr/PricingSubscription/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.fr ;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.fr.log;
error_log /var/log/nginx/error_ecommerce.fr.log;
location / {
try_files $uri $uri/ =404;
}}
```

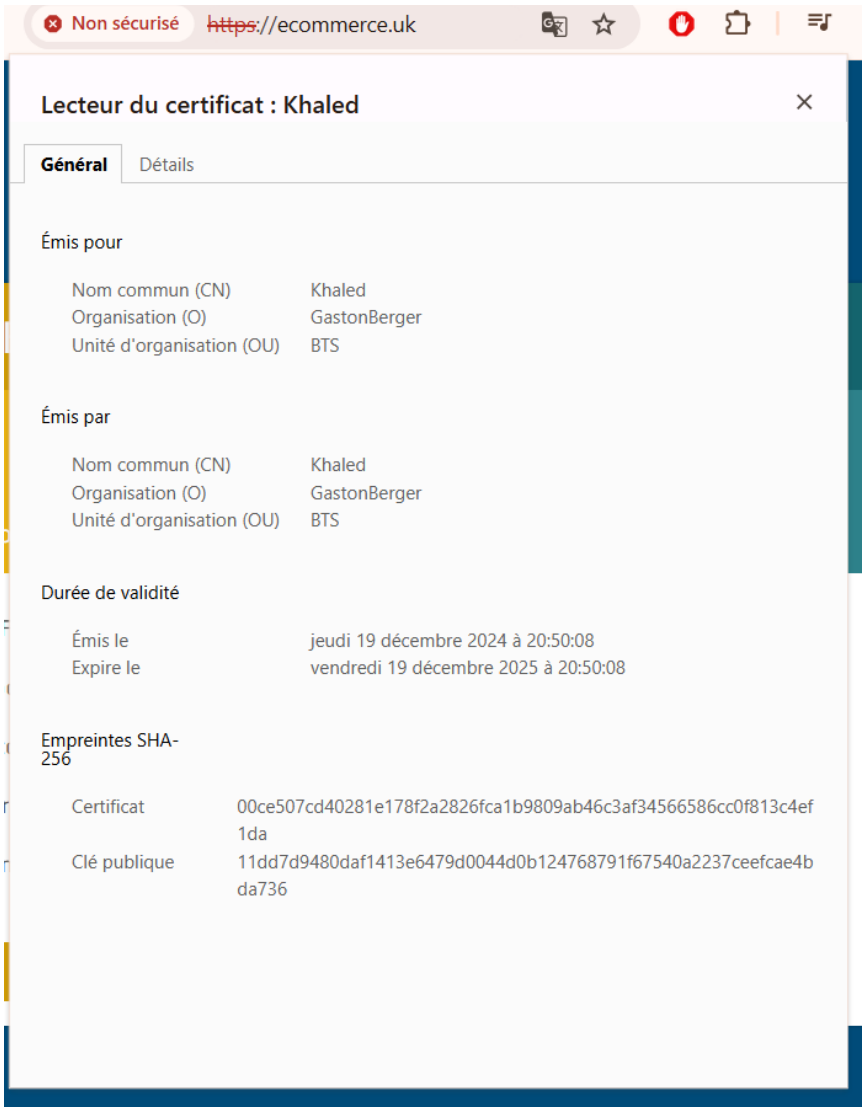
root@localhost:/etc/nginx/conf.d

```
  GNU nano 5.6.1                          site_commerce.uk.conf
server {
listen 80;
listen [::]:80;
root /var/www/ecommerce.uk/PricingSubscription;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.uk ;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.uk.log;
error_log /var/log/nginx/error_ecommerce.uk.log;
location / {
try_files $uri $uri/ =404;
}
}
server {
listen 443 http2 ssl;
listen [::]:443 http2 ssl;
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
ssl_dhparam /etc/ssl/certs/dhparam.pem;
root /var/www/ecommerce.uk/PricingSubscription/;
index index.html index.htm index.nginx-debian.html sign-up.php;
server_name ecommerce.uk ;
location ~* \.php$ {
fastcgi_pass unix:/run/php-fpm/www.sock;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
}
access_log /var/log/nginx/access_ecommerce.uk.log;
error_log /var/log/nginx/error_ecommerce.uk.log;
location / {
try_files $uri $uri/ =404;
}}
```

```
[root@localhost conf.d]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[root@localhost conf.d]# systemctl restart nginx
[root@localhost conf.d]#
```

```
[root@localhost conf.d]# firewall-cmd --add-port=443/tcp --permanent
success
[root@localhost conf.d]# firewall-cmd --reload
success
[root@localhost conf.d]#
```

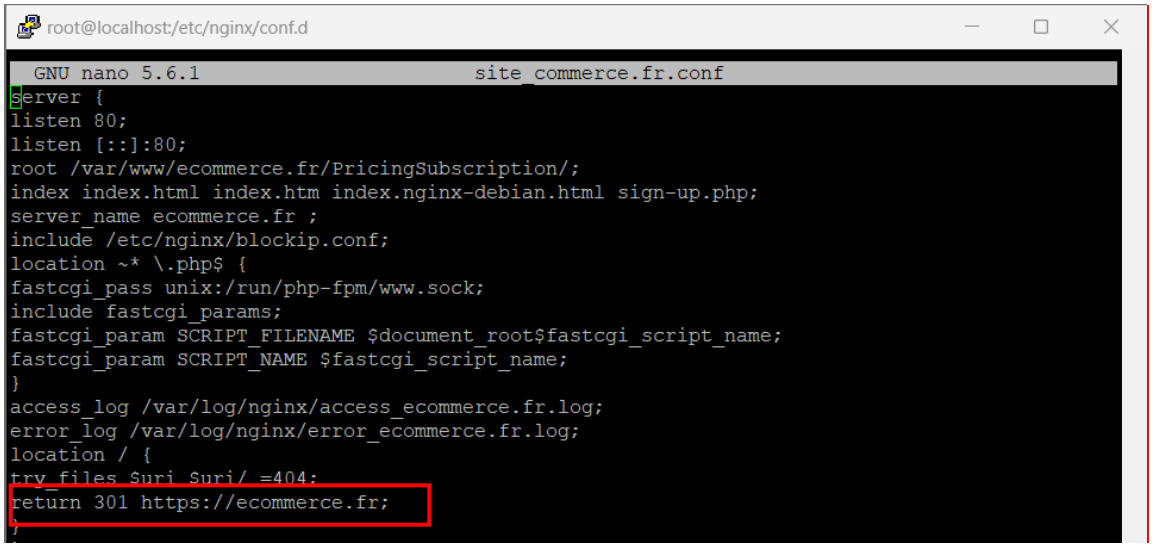




VIII. Redirection http https

```
[root@localhost conf.d]# firewall-cmd --remove-service=http --permanent
success
[root@localhost conf.d]# firewall-cmd --reload
success
[root@localhost conf.d]# firewall-cmd --list-service
cockpit dhcpv6-client https ssh
[root@localhost conf.d]#
```

On modifie les fichiers de conf en y ajoutant la ligne suivante :



IX. Installation de deux serveurs red hat

Il nous faut un deuxième serveur (WEB02) qui sera identique à celui configuré précédemment, mais sans BDD. On clone donc notre VM et on supprime mariadb et tous les fichiers en rapport.

```
[root@localhost ~]# systemctl stop mariadb
[root@localhost ~]# systemctl disable mariadb
Removed "/etc/systemd/system/multi-user.target.wants/mariadb.service".
Removed "/etc/systemd/system/mysql.service".
Removed "/etc/systemd/system/mysqld.service".
[root@localhost ~]# dnf remove mariadb-server mariadb mariadb-libs mariadb-client
No match for argument: mariadb-libs
No match for argument: mariadb-client
Dependencies resolved.
================================================================================
 Package                 Arch       Version                  Repository      Size
================================================================================
Removing:
 mariadb                 x86_64     3:10.5.22-1.el9_2        @appstream      18 M
 mariadb-server          x86_64     3:10.5.22-1.el9_2        @appstream      63 M
Removing unused dependencies:
 checkpolicy             x86_64     3.6-1.el9                @appstream     1.5 M
 mariadb-backup          x86_64     3:10.5.22-1.el9_2        @appstream      24 M
 mariadb-common          x86_64     3:10.5.22-1.el9_2        @appstream     179 k
 mariadb-connector-c     x86_64     3.2.6-1.el9_0            @appstream     540 k
```

X. Configuration BDD sur WEB01

```
[root@localhost ~]# firewall-cmd --zone=public --add-port=3306/tcp --permanent
success
[root@localhost ~]# firewall-cmd reload
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: reload
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

Dans le fichier de conf /etc/my.cnf.d/mariadbserver.cnf, on décommande la commande suivante :

```
#innodb_autoinc_lock_mode=2
#
# Allow server to accept connections on all interfaces.
#
bind-address=0.0.0.0
#
# Optional setting
#wsrep_slave_threads=1
```

```
MariaDB [(none)]> GRANT ALL on KHALEDBDD.* to Khaled@192.168.0.167 IDENTIFIED BY 'root';
Query OK, 0 rows affected (0.450 sec)
```

```
[root@localhost ~]# mysql -u Khaled -h 192.168.0.163 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.5.5-10.5.22-MariaDB MariaDB Server

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| KHALEDBDD          |
| information_schema |
+--------------------+
2 rows in set (0.03 sec)

mysql>
```

XI. Mise en place d'un serveur HA

a. Configuration HAPROXY

```
[root@localhost ~]# yum install haproxy
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
Dependencies resolved.
================================================================================
 Package                 Architecture            Version                 Repo
================================================================================
Installing:
 haproxy                 x86_64                  2.4.22-3.el9_3          apps

Transaction Summary
================================================================================
Install  1 Package

Total download size: 2.2 M
Installed size: 6.6 M
Is this ok [y/N]: y
Downloading Packages:
haproxy-2.4.22-3.el9_3.x86_64.rpm
--------------------------------------------------------------------------------
```

```
[root@localhost haproxy]# cp haproxy.cfg haproxy_copy.cfg
[root@localhost haproxy]#
```

Dans le fichier haproxy.cfg :

root@localhost:/etc/haproxy

```
  GNU nano 5.6.1                    haproxy.cfg                         Modified
    daemon

    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats

    # utilize system-wide crypto-policies
    ssl-default-bind-ciphers PROFILE=SYSTEM
    ssl-default-server-ciphers PROFILE=SYSTEM

#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    tcp
    listen                  stats
    bind *:8080
    mode                    http
    stats                   enable
    stats                   hide-version
    stats uri /stats
    stats admin if LOCALHOST
    stats auth haproxy:haproxy
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 3000

#---------------------------------------------------------------------
```

```
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend main
    bind *:80
    acl url_static       path_beg       -i /static /images /javascript /stylesheets
    acl url_static       path_end       -i .jpg .gif .png .css .js

    use_backend static          if url_static
    default_backend             app

#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
#---------------------------------------------------------------------
backend static
    balance     roundrobin
    server      static 127.0.0.1:4331 check

#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    balance     roundrobin
    server  web01 192.168.0.163:443 ssl verify none check
    server  web02 192.168.0.167:443 ssl verify none check
```

b. RSYSLOG

Dans le fichier /etc/rsyslog.conf on décommente les lignes suivante :

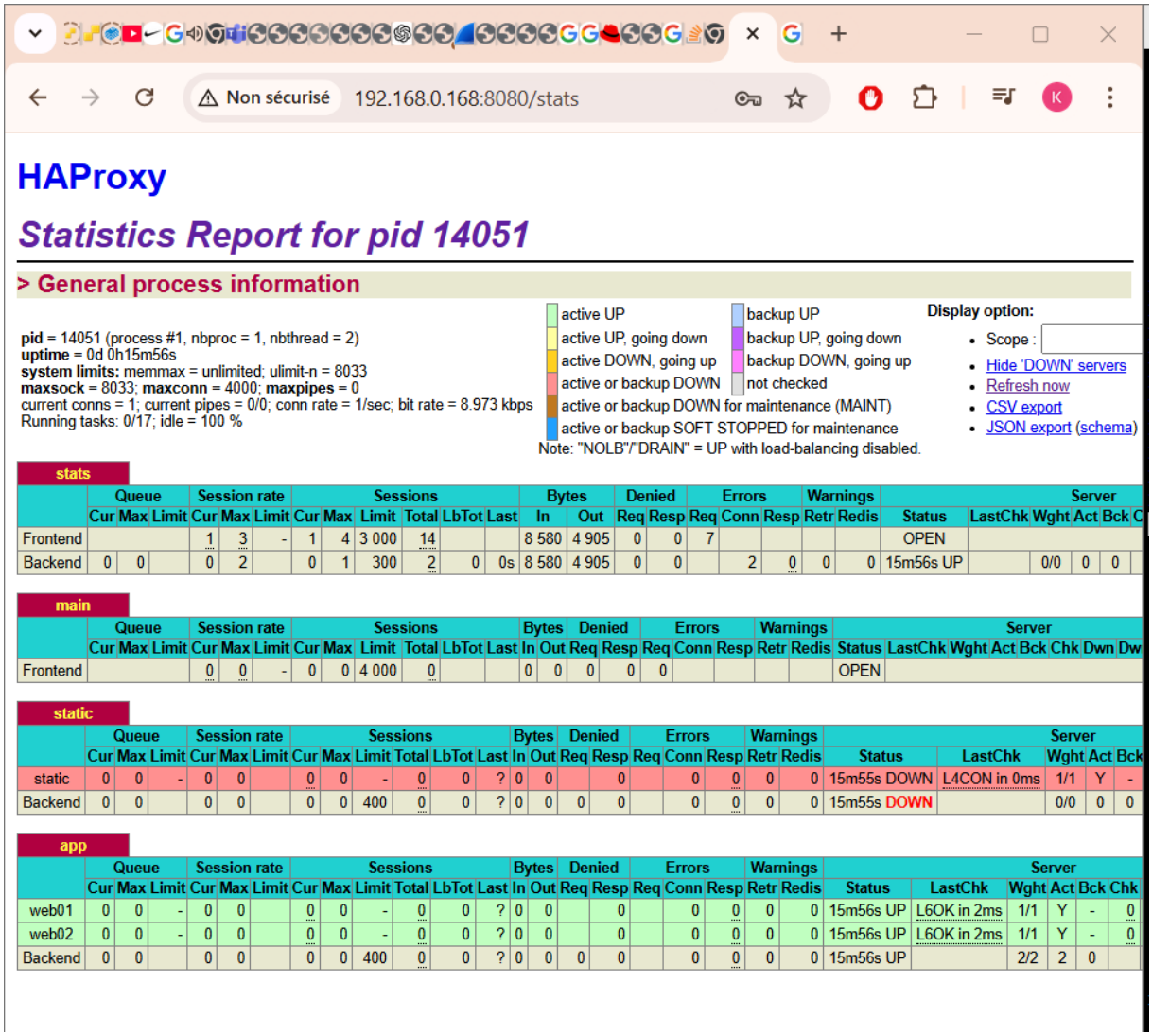
```
                        # local messages are retrieved through imjournal now.
module(load="imjournal"             # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
```

```
[root@localhost etc]# setsebool -P haproxy_connect_any 1
```

```
[root@localhost etc]# setsebool -P haproxy_connect_any 1
[root@localhost etc]# systemctl start haproxy
[root@localhost etc]# systemctl start rsyslog
```

On n’oubliera pas d’activer le port 8080 ainsi http sur le firewall.

XII. Depuis le serveur HAPROXY



XIII. Sécurisation HAPROXY

```
[root@localhost certs]# openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/pki/tls/certs/
haproxy.pem -out /etc/pki/tls/certs/haproxy.pem -days 365
.....+.....+.+.....+...+.+..............+.+.....+......+.......+..+....+......+...+..++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+..........+..+.......+.....++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....................+...+.........
.....+...+.+...........+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+..............+.+...+.....+....+.....+......+.......+...+..+............+.......+.....+..
.+...+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+..+...+...+
.............+....+...+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
*....+.........+...+...+........+.......+..+.........+...........+.+...+......+......+...+.
.+.+.........+.........+..+.........+........+.+...+......+.....+......+...+.......+...+..+.
...+..+...+....+......+.....+.++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++
-----
You are about to be asked to enter information that will be incorporated
```

On ajoute dans le fichier /etc/haproxy/haproxy.cfg :

```
#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         127.0.0.1 local2

    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon

    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats

    # utilize system-wide crypto-policies
    ssl-default-bind-ciphers PROFILE=SYSTEM
    ssl-default-server-ciphers PROFILE=SYSTEM
    maxsslconn 256
    tune.ssl.default-dh-param 2048
#---------------------------------------------------------------------
```

```
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend main
    bind *:80
    acl url_static       path_beg       -i /static /images /javascript /stylesheets
    acl url_static       path_end       -i .jpg .gif .png .css .js

    use_backend static          if url_static
    default_backend             app

    bind *:443 ssl crt /etc/pki/tls/certs/haproxy.pem
```