



MISE EN PLACE D'UN SERVICE WEB #1

R5 – Administration des services

[Résumé](#)

Julien VINCENT
Gaston Berger Lille

Table des matières

1. Contexte.....	2
2. Mise en pratique.....	2
3. Réalisation du TP.....	3
A. Installation d'un serveur red hat.....	3
B. Installation d'un service WEB (nginx).....	3
4. Installation moteur BDD.....	7
5. Déploiement du site FR.....	7
6. Déploiement du site UK.....	11
7. Restriction accès IP.....	12
8. Analyse des logs.....	13

1. Contexte

Vous avez la charge de l'administration des serveurs WEB de la société Ordi Global Corporation, cette société ayant une volonté d'internationalisation de ces produits, vous devez mettre en place le site du groupe dans les deux régions (France et Grande Bretagne).

Par soucis de normalisation :

La France aura le raccourci FR.

La Grande Bretagne aura le raccourci UK.

Votre hébergeur proposant des services de VPS avec un système de paiement, il est indispensable de sécuriser l'ensemble des éléments.

Pour le moment, un seul serveur est nécessaire mais en cas d'augmentation du trafic et de la criticité, il sera peut-être étudié la mise en place d'un cluster pour la haute disponibilité.


Pour vous accompagner, vous venez de recevoir le package du site, il reste à vous de l'adapter selon la langue du pays.

2. Mise en pratique

- ❓ Dans le cadre du TP Mise en place d'un serveur web #1 , nous allons mettre en place, les éléments suivants :
 - o Installation d'un serveur
 - o Installation d'un service WEB (nginx)
 - o Déploiement des sites WEB
 - o Sécurisation d'un service WEB (nginx)

3. Réalisation du TP

A. Installation d'un serveur rocky	
B. Installation d'un service WEB (nginx)	
Nous aurons besoins sur la machine des packages suivants : <ul style="list-style-type: none">❑ Nginx❑ Php-fpm❑ Mariadb-server❑ Php❑ Php-mysqlnd	
	<p>Le fichier de configuration se trouve dans : /etc/nginx/</p> <p>On retrouvera les logs dans le répertoire : /var/log/nginx/error.log</p>
	<p>Par défaut, les fichiers pour le site web sont dans le répertoire : /usr/share/nginx/html</p>

		<p>On peut voir la page http par défaut (index.html)</p> <p>Tips : Si cela ne marche, regarde si le service http est autorisé : <code>firewall-cmd --list-service</code></p>
<p>Si on teste sur le port 80 :</p>		<p>Modifions le port d'écoute de nginx (par défaut 80 pour le protocole html)</p> <p>Il faut se rendre dans le fichier de configuration nginx et modifier le paramètre :</p> <pre>listen 8080 default_server;</pre> <p>On relance le service et testons une connexion avec le port :</p>

[Tapez ici][Tapez ici][Tapez ici]



Ce site est inaccessible

192.168.1.38 n'autorise pas la connexion.

Voici quelques conseils :

- Vérifier la connexion
- [Vérifier le proxy et le pare-feu](#)

ERR_CONNECTION_REFUSED

Actualiser

Si on teste sur le port 8080 :

[Tapez ici][Tapez ici][Tapez ici]



Ce site est inaccessible

192.168.1.38 n'autorise pas la connexion.

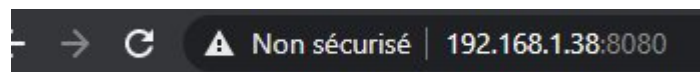
Voici quelques conseils :

- Vérifier la connexion
- [Vérifier le proxy et le pare-feu](#)

ERR_CONNECTION_REFUSED

Actualiser

Même résultat ? Pourquoi ?



Après la correction, la page apparaît, que devons-nous faire ?

[Tapez ici][Tapez ici][Tapez ici]

	Remettons le port http par défaut, c'est-à-dire 80 et on redémarre le service. service nginx restart
<h2>4. Installation moteur BDD</h2>	
<p>Pour rappel :</p> <pre>systemctl enable --now mariadb.service // pour le lancer et mettre au démarrage mysql_secure_installation // Faire la configuration de base mysql -u root -p // se connecter create database XX // créer une bdd CREATE USER 'USER'@'localhost' IDENTIFIED BY 'MDP'; // créer un utilisateur GRANT ALL PRIVILEGES ON BDD.* TO 'USER'@'localhost'; // Attribution des droits FLUSH PRIVILEGES; // Forcer la prise en compte Show databases ; // permet de voir les BDDs. Show tables ; // voir les tables.</pre>	<p>Comme nous avons installés mariadb, il est nécessaire de le configurer.</p> <p>TIPS : Il faudra conserver ces logins tout au long du TP (astuce un keepass permet cela facilement)</p>
<h2>5. Déploiement du site FR</h2>	
<pre>mkdir -p /var/www/ecommerce.fr/</pre>	Nous allons déployer el site FR. Nous allons créer le répertoire ecommerce.fr/ dans l'arborescence /var/www/
Astuce : Winscp permet de le faire très facilement en utilisant le protocole ssh.	Puis avec le package fournis, vous déposerez l'ensemble des fichiers dans le répertoire ecommerce.fr
<pre>; 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</pre>	Maintenant, nous allons démarrer modifier les paramètres de php-fpm RDV dans : /etc/php-

<p>Vous noterez la valeur listen, par défaut : listen = /run/php-fpm/www.sock</p>	<p>fpm.d/www.conf</p> <p>Puis modifier le fichier avec les informations ci-contre :</p>
	<p>Ensuite, vous pouvez activer le démarrage automatique et démarrer dès maintenant le service.</p>
<pre>server { listen 80; listen [::]:80; root /var/www/site_commerce.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; } }</pre>	<p>Nous allons pouvoir maintenant créer le fichier de configuration nginx.</p> <p>Il faut le créer dans le répertoire de configuration /etc/nginx /conf.d/</p> <p>Son nom sera site_commerce.fr.conf</p>
	<p>Courage, la mise en place du site est pour bientôt, il faut maintenant, configurer le fichier de configuration php pour établir la connexion avec</p>

[Tapez ici][Tapez ici][Tapez ici]

	le moteur de bdd.
<pre> <?php \$SETTINGS["mysql_user"]='exploit_fr'; \$SETTINGS["mysql_pass"]='exploit'; \$SETTINGS["hostname"]='localhost'; \$SETTINGS["mysql_database"]='fr'; \$SETTINGS["data_table"]='registrations'; \$SETTINGS["paypal_address"]='email@domain.com'; ?> </pre>	<p>Il faut modifier le fichier conf.php se (que vous venez de déposer dans /var/www/site_commerce.fr)</p> <p>Vous devez renseigner les informations avec les informations lors de la création de la base et de l'utilisateur.</p>
<p>Exemple :</p> <pre> [root@web01 site_commerce.fr]# mysql -u exploit_fr -p Enter password: Welcome to the MariaDB monitor. Commands end with ; or \g. Your MariaDB connection id is 39 Server version: 10.3.28-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 fr 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 [fr]> source /var/www/site_ecommerce_fr/database.sql </pre>	<p>Nous allons maintenant exécuter le script SQL fournit (satabase.sql).</p> <p>Pour cela, il faut se connecter sur le moteur BDD et sélectionner la base.</p> <p>Nous pouvons exécuter le script en faisant source emplacement_du_script</p>
	On doit faire une relance du nginx afin de faire nos tests.



Subscription Sign up Form

Basic	Standard	Premium
\$5	\$10	\$20
per month	per month	per month
Full access Documentation Customers Support Free Updates Unlimited Domains	Full access Documentation Customers Support Free Updates Unlimited Domains	Full access Documentation Customers Support Free Updates Unlimited Domains
Sign Up	Sign Up	Sign Up


Design by W3layouts

Si tout fonctionne, lorsque vous tapez ecommerce.fr, vous devrez avoir l'affichage ci-contre.

[Tapez ici][Tapez ici][Tapez ici]

<div> <div>PHP Version 7.2.24</div>  </div> <table> <tr><td>System</td><td>Linux web01 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Mar 25 14:36:04 EDT 2021 x86_64</td></tr> <tr><td>Build Date</td><td>Oct 22 2019 08:28:36</td></tr> <tr><td>Server API</td><td>FPM/FastCGI</td></tr> <tr><td>Virtual Directory Support</td><td>disabled</td></tr> <tr><td>Configuration File (php.ini) Path</td><td>/etc</td></tr> <tr><td>Loaded Configuration File</td><td>/etc/php.ini</td></tr> <tr><td>Scan this dir for additional .ini files</td><td>/etc/php.d</td></tr> <tr><td>Additional .ini files parsed</td><td>/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqld.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini</td></tr> <tr><td>PHP API</td><td>20170718</td></tr> <tr><td>PHP Extension</td><td>20170718</td></tr> <tr><td>Zend Extension</td><td>320170718</td></tr> <tr><td>Zend Extension Build</td><td>API320170718,NTS</td></tr> <tr><td>PHP Extension Build</td><td>API20170718,NTS</td></tr> <tr><td>Debug Build</td><td>no</td></tr> <tr><td>Thread Safety</td><td>disabled</td></tr> <tr><td>Zend Signal Handling</td><td>enabled</td></tr> <tr><td>Zend Memory Manager</td><td>enabled</td></tr> <tr><td>Zend Multibyte Support</td><td>disabled</td></tr> <tr><td>IPv6 Support</td><td>enabled</td></tr> <tr><td>DTrace Support</td><td>available, disabled</td></tr> <tr><td>Registered PHP Streams</td><td>https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar</td></tr> <tr><td>Registered Stream Socket Transports</td><td>tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2</td></tr> <tr><td>Registered Stream Filters</td><td>zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*</td></tr> </table> <div> <div> This program makes use of the Zend Scripting Language Engine: Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies </div>  </div>	System	Linux web01 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Mar 25 14:36:04 EDT 2021 x86_64	Build Date	Oct 22 2019 08:28:36	Server API	FPM/FastCGI	Virtual Directory Support	disabled	Configuration File (php.ini) Path	/etc	Loaded Configuration File	/etc/php.ini	Scan this dir for additional .ini files	/etc/php.d	Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqld.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini	PHP API	20170718	PHP Extension	20170718	Zend Extension	320170718	Zend Extension Build	API320170718,NTS	PHP Extension Build	API20170718,NTS	Debug Build	no	Thread Safety	disabled	Zend Signal Handling	enabled	Zend Memory Manager	enabled	Zend Multibyte Support	disabled	IPv6 Support	enabled	DTrace Support	available, disabled	Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar	Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2	Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*	<p>Un test supplémentaire permet de vérifier si php est correctement opérationnel :</p> <p><code>echo '<?php phpinfo(); ?>' > /usr/share/nginx/html/info.php</code></p> <p>Vous aurez cette affichage en allant sur la page info.php depuis votre navigateur web.</p>
System	Linux web01 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Mar 25 14:36:04 EDT 2021 x86_64																																														
Build Date	Oct 22 2019 08:28:36																																														
Server API	FPM/FastCGI																																														
Virtual Directory Support	disabled																																														
Configuration File (php.ini) Path	/etc																																														
Loaded Configuration File	/etc/php.ini																																														
Scan this dir for additional .ini files	/etc/php.d																																														
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mysqld.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini																																														
PHP API	20170718																																														
PHP Extension	20170718																																														
Zend Extension	320170718																																														
Zend Extension Build	API320170718,NTS																																														
PHP Extension Build	API20170718,NTS																																														
Debug Build	no																																														
Thread Safety	disabled																																														
Zend Signal Handling	enabled																																														
Zend Memory Manager	enabled																																														
Zend Multibyte Support	disabled																																														
IPv6 Support	enabled																																														
DTrace Support	available, disabled																																														
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar																																														
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2																																														
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*																																														
	<p>Maintenant à vous de jouer pour personnaliser la page en FR (le fichier de configuration est le suivant : sign-up.php</p>																																														
<h2>6. Déploiement du site UK</h2>																																															
	<p>Nous allons maintenant déployer le 2eme site UK.</p> <p>A vous de jouer</p>																																														

[Tapez ici][Tapez ici][Tapez ici]

<pre>[root@WEB01 nginx]# ls -lrt total 24 -rw-r--r--. 1 root root 0 19 sept. 07:12 ecommerce.uk.error.log -rw-r--r--. 1 root root 0 19 sept. 07:12 ecommerce.fr.error.log -rw-r--r--. 1 root root 1770 19 sept. 07:12 error.log -rw-r--r--. 1 root root 4778 19 sept. 07:17 access.log -rw-r--r--. 1 root root 623 19 sept. 07:55 ecommerce.fr.access.log -rw-r--r--. 1 root root 4629 19 sept. 07:55 ecommerce.uk.access.log [root@WEB01 nginx]# pwd /var/log/nginx</pre>	<p>On peut voir pour chaque site, les logs d'accès.</p>
<p>Avant de continuer, vous devez :</p> <ul style="list-style-type: none"> - Avoir les 2 sites opérationnels (FR & UK) - Avoir un snapshot 	
<h2>7. Restriction accès IP</h2>	
	<p>Certains pirates s'amuse à tester les vulnérabilités de notre site internet. La bonne nouvelle, nous avons les adresses IP des pirates. Nous allons ajouter une restriction d'ip sur le site ecommerce.fr :</p> <p>On va créer dans le répertoire /etc/nginx , un fichier se nommant blockip.conf</p> <p>Il va contenir l'ip de notre pirate (par exemple l'ip de votre poste pour vérifier) : deny IP;</p>

	<p>On va ajouter dans le fichier de configuration du site ecommerce.fr.conf de prendre en compte ce fichier :</p> <p>include blockip.conf;</p> <p>On recharge nginx</p> <p>L'accès au site ecommerce est impossible depuis notre IP</p> <p>Mais le site ecommerce.uk est cependant toujours accessible.</p>
8. Analyse des logs	
<pre>[root@localhost nginx]# ls access.log error.log [root@localhost nginx]#</pre>	<p>Les accès et les erreurs des sites sont présents dans le répertoire : /var/log/nginx.</p> <p>Les erreurs sont dans error.log</p> <p>Les accès dans le fichier access.log</p>
<pre>2022/11/15 10:32:50 [error] 10432#10432: *2 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such f //192.168.75.128/" [root@localhost nginx]# cat access.log ::1 - - [15/Nov/2022:10:27:48 +0100] "GET / HTTP/1.1" 200 7620 "-" "curl/7.76.1" "-" 192.168.75.1 - - [15/Nov/2022:10:32:50 +0100] "GET / HTTP/1.1" 200 7620 "-" "Mozilla/5.0 (Windows NT 10.0; 192.168.75.1 - - [15/Nov/2022:10:32:50 +0100] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://192.168 192.168.75.1 - - [15/Nov/2022:10:32:50 +0100] "GET /poweredby.png HTTP/1.1" 200 368 "http://192.168.75.128/ 192.168.75.1 - - [15/Nov/2022:10:32:50 +0100] "GET /favicon.ico HTTP/1.1" 404 3332 "http://192.168.75.128/" [root@localhost nginx]#</pre>	<p>Cependant la lecture des logs peut être complexe au début :</p>
	<p>Pour nous simplifier la lecture, nous utiliserons Goaccesss ,</p>

	<p>permettant de transformer ces logs dans une interface plus exploitable. Pour cela, il est nécessaire d'activer le repository epel-release.</p> <p>Puis d'installer le package goaccess.</p>
<p>goaccess -f chemindufichieraccess</p> <p>Exemple :</p> <p>goaccess -f /var/log/acesss.log</p>	<p>Pour utiliser le goaccess, il faut exécuter la commande ci-contre :</p>

```

+-----+
| 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 |
+-----+

```

Vous aurez une interface, il faut sélectionner le premier format et faire entrer.


```
Dashboard - Overall Analyzed Requests (15/Nov/2022 - 15/Nov/2022)

Total Requests 10 Unique Visitors 2 Requested Files 1 Referrers 0
Valid Requests 5 Log Parsing Time 1s Static Files 2 Log Size 843.0 B
Failed Requests 0 Excl. IP Hits 0 Not Found 1 Tx. Amount 33.58 KiB
Log Source /var/log/nginx/access.log

> 1 - Unique visitors per day - Including spiders

Hits      h% Vis.      v% Tx. Amount Data
-----
  5 100.00%    2 100.00%  33.58 KiB 15/Nov/2022 |

2 - Requested Files (URLs)

Hits      h% Vis.      v% Tx. Amount Mtd Proto  Data
-----
  2 40.00%    2 100.00%  14.88 KiB GET HTTP/1.1 /

3 - Static Requests

Hits      h% Vis.      v% Tx. Amount Mtd Proto  Data
-----
  1 20.00%    1 50.00%   15.08 KiB GET HTTP/1.1 /icons/poweredby.png
  1 20.00%    1 50.00%   368.0 B GET HTTP/1.1 /poweredby.png

4 - Not Found URLs (404s)

Hits      h% Vis.      v% Tx. Amount Mtd Proto  Data
-----
  1 20.00%    0 0.00%    3.25 KiB GET HTTP/1.1 /favicon.ico

5 - Visitor Hostnames and IPs

Hits      h% Vis.      v% Tx. Amount Data
-----
  4 80.00%    1 50.00%   26.14 KiB 192.168.75.1 |
  1 20.00%    1 50.00%    7.44 KiB ::1 |

[?] Help [Enter] Exp. Panel
```

Vous aurez accès à une interface complète permettant d'avoir les statistiques d'accès de votre site WEB (IP / navigateur / erreurs / nombre de visiteur..)

[Tapez ici][Tapez ici][Tapez ici]

[Tapez ici][Tapez ici][Tapez ici]