RÉALISATION PERSONNELLE

Mise en place d'un hébergement web sécurisé sur un VPS

Auteur : Winness RAKOTOZAFY

Version mars 2023

AVANT – PROPOS

Dans le cadre de cette documentation, nous allons mettre en place un hébergement web sur un VPS sous Linux de manière sécurisé.

Tout d'abord, il vous faudra comme prérequis d'acheter un **VPS** depuis les fournisseurs tel que Amazon (AWS), Microsoft Azure, OVH, Linode, etc et d'un **nom de domaine**. Notre choix, par préférence, se porte sur le fournisseur français, OVH, avec une distribution sous Debian Bullseye.

Ensuite, après que les accès au VPS vous seront fournis, nous allons nous connecter sur le serveur, pour y configurer les bonnes pratiques de sécurité d'un serveur Linux accessible sur Internet. Ces bonnes pratiques se tournent autour de la sécurisation du protocole SSH, mise en place d'un pare-feu,

Puis, au cours de cette documentation, nous allons mettre en place un service web sous Apache, avec l'intégration d'un certificat Let's Encrypt pour avoir un accès sécurisé en HTTPS pour notre site web.

Enfin, nous allons paramétrer l'enregistrement DNS de notre nom de domaine pour pointer vers l'adresse IP de notre VPS pour que notre site web soit accessible en ligne.

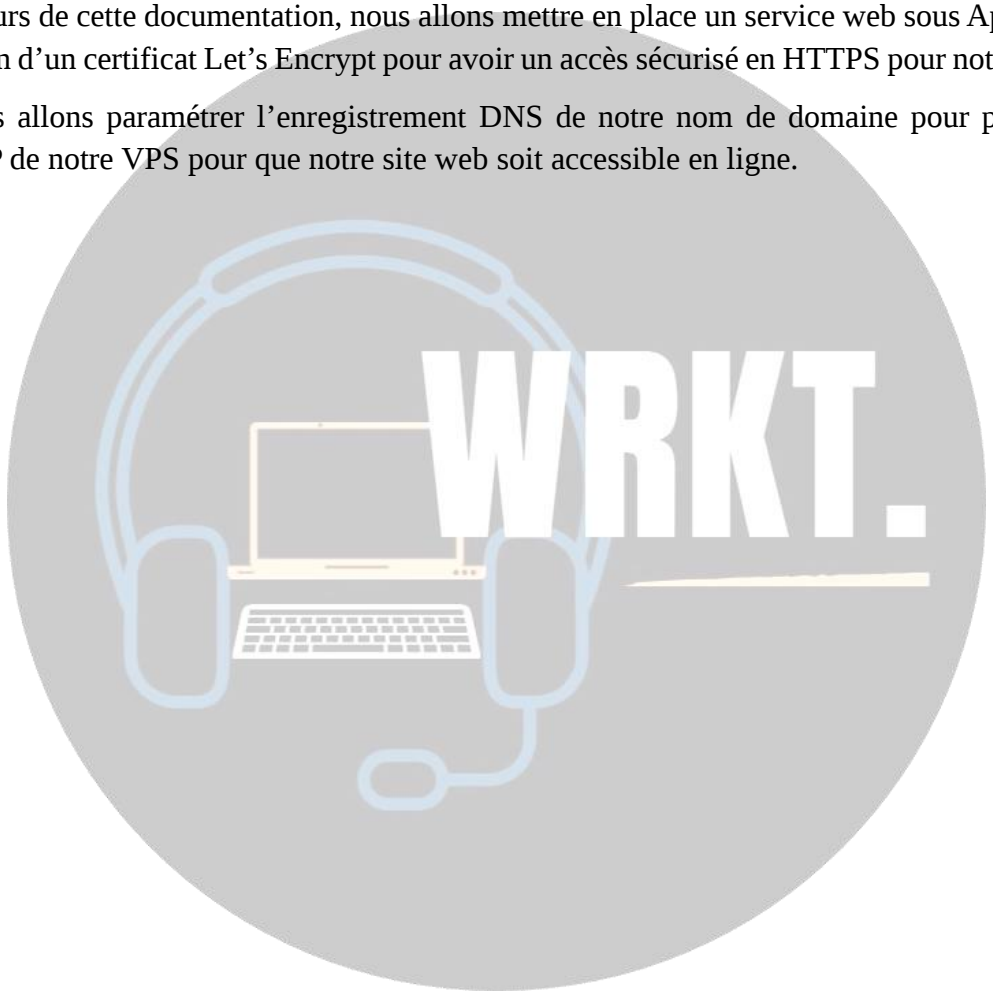


TABLE DES MATIERES

I- Sécurisation du serveur Linux

Un serveur sous Linux, par défaut n'est pas forcément sécurisé et peut facilement être assujetti à des cyberattaques. Ainsi, pour pallier ces problèmes de sécurité, nous allons appliquer les configurations suivantes :

- Configuration du service SSH avec certificat
- Mise en place d'un IPS avec Fail2Ban pour se protéger des attaques bruteforce

1) Configuration du service SSH

Par défaut, notamment sur les VPS, les accès SSH s'effectuent par **mot de passe** et même parfois autorise l'accès root directement par SSH. Ces paramétrages par défaut présentent des risques sur les services offertes par votre VPS, et nécessitent un point d'attention.

Pour modifier les configurations de service SSH, éditez le fichier de configuration suivant **`/etc/ssh/sshd_config`** avec un éditeur de texte (vim, nano, emacs)

```
sudo vim /etc/ssh/sshd_config
```

Puis, éditez les lignes suivantes :

```
# Numéro de port personnalisé qui sera utilisé par SSH
Port 7859

# Désactiver l'accès root par SSH
Permit RootLogin no

# Activer l'authentification par certificat (clé publique/clé privé)
PubKeyAuthentication yes

# N'autoriser que les clés publiques listés dans le fichier suivant
AuthorizedKeysFile      .ssh/autorized_keys  .ssh/authorized_keys2

# Désactiver toute authentification par mot de passe
PasswordAuthentication no
```

Ensuite, avant de redémarrez le service SSH, assurez-vous que votre clé publique soit présente sur le serveur, auquel cas vous **perdrez tout accès distant** sur votre serveur.

Pour ce faire, vous devez tout d'abord générer un couple bi-clé puis le transférer dans le fichier **`/home/user/.ssh/authorized_keys`** du VPS. Pour ce faire, vous avez diverses méthodes selon votre système d'exploitation (opération à effectuer sur l'ordinateur qui souhaite accéder au VPS) :

- Sous l'invite de commande Windows

```
# Générer le couple clé publique/privé
ssh-keygen -b 4096

# Copiez la clé vers le VPS
type $env:USERPROFILE\.ssh\id_rsa.pub | ssh user@adresse_IP_VPS
"cat >> .ssh/authorized_keys"
```

- Sous un terminal Linux

```
# Générer le couple clé publique/privé
ssh-keygen -b 4096

# Copiez la clé vers le VPS
ssh-copy-id user@adresse_IP_VPS
```

- Sous un terminal Mac

```
# Générer le couple clé publique/privé
ssh-keygen -b 4096

# Copiez la clé vers le VPS
scp ~/.ssh/id_rsa.pub user@adresse_IP_VPS
```

Vérifiez que la clé publique est bien transféré vers le serveur (opération à effectuer sur le VPS):

```
debian@[redacted]:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCfxRY//gdFbMngZA17KBmLLxgbb0MPabL1MPT0N4sTVrFtri
T7ZGbqsMH6N+RmAVzp0HU2aH0i8vw+Pf35zx2q5hDX/RTAO+b3XevVCV9ZcdueuLS+Zr6ac5M152M7WydjcKb2
0dRsJmac2diNLEcPvGw4183GNi2fn5JtbrS80plBgC9dtw3zNUyPurLKiKVJmQFlIX/6lsgzDZRvlvhX2foHGx
0e3Oulrlb/WtoyQNDPd1zl/mhM90cZKc8fQIWuwi4P+hrh9w4iV2hBoIkc0Mmzff2es0JKmtbnXqalwvOtlfMG
vvX+K0H/Q7QtWB44aA/N6vN8lJjbFsMM3Ayk1scAHgs/3FgpdGa8vlm+nYqurrxT1CLrOhg3j8F3wb6SN5sglQ
yeAD2/flYLeomiOM3rw6YSxXgLeQ5m+/U+EjwMI/u3k3biaQKk4wKoK7TsmvRrebzVhSuuSrNDFO+AcfKfE/e3
8zwqsbi/8ddN6KS1bn0t4WscGq3JnQHKPliAh3ZmAZ0gNvEgNJMFeIvize9UelCs0irt92uqymANcScfePFPU8
lPu47BM1JqNBspPWelpui8bnRxQZhn8Hzy/wCRM2+W4Tz5bExbYpq7skYYOlRkb1/AQwuLmfCnZPDVmCQGTCQk
+DxTGVKjomWGXMaTm+RGaHLbD2ng7hMqnw== wrkt@Legion-Y540
```

Enfin, redémarrez le service SSH sur le VPS :

```
sudo systemctl restart sshd
```

A présent, effectuez un test d'accès SSH. En temps normal, vous n'aurez pas à saisir un mot de passe, et vous aurez normalement accès directement au VPS.

```
ssh -p num_port user@adresse_IP_VPS
```

```
wrkt@Legion-Y540:~$ ssh -p [redacted] debian@vps-debian
Linux [redacted] 5.10.0-21-cloud-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar 13 17:41:20 2023 from [redacted]
debian@[redacted]:~$
```

L'accès SSH est à présent sécurisé, nous allons à présent, rajouter un IPS qui permettra de bannir des adresses IP suite à des connexions intrusives non autorisées.

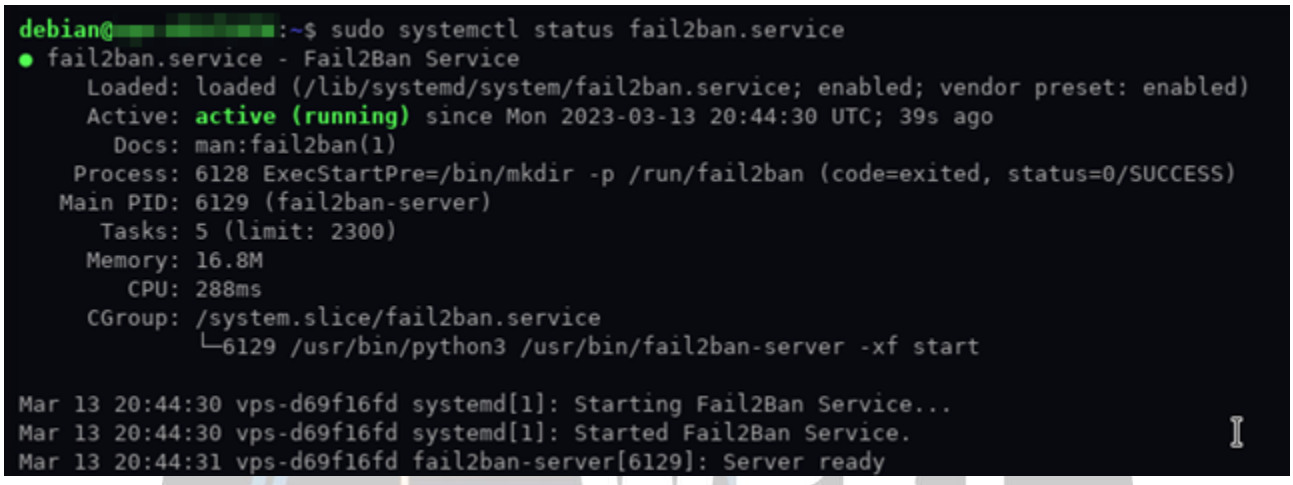
2) Installation d'IPS fail2ban

Pour installer fail2ban, il suffit de lancer la commande suivante :

```
sudo apt -y install fail2ban
```

Vérifiez que le service est bien installé en lançant la commande suivante :

```
sudo systemctl status fail2ban.service
```



Par défaut, des mesures de sécurité sont mises en place par fail2ban qui permettront de bloquer des connexions intrusives en SSH, ou sur formulaire http :

```
#
# SSH servers
#

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s


[dropbear]

port     = ssh
logpath  = %(dropbear_log)s
backend  = %(dropbear_backend)s


[selinux-ssh]

port     = ssh
logpath  = %(auditd_log)s


#
# HTTP servers
#

[apache-auth]

port     = http,https
logpath  = %(apache_error_log)s
```

Pour vérifier l'état de l'IPS et de déterminer les statistiques des adresses IP bloquées par notre service ssh par exemple, lancez la commande suivante :

```
sudo fail2ban-client status sshd
```

```
debian@[redacted]:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
├ Filter
|  ├ Currently failed: 0
|  ├ Total failed:     0
|  `- File list:       /var/log/auth.log
`- Actions
   ├ Currently banned: 0
   ├ Total banned:     0
   `- Banned IP list:
```

Pour l'instant donc, aucune tentative intrusive a été détectée par l'IPS, mais au fur et à mesure de la production, ces statistiques pourraient varier considérablement.

A présent, nous allons passer à l'installation du serveur web Apache ainsi que sa sécurisation avant sa mise en production.

II- Installation du serveur web Apache

Pour installer le serveur web, lancez la commande suivante :

```
sudo apt install apache2 -y
```

L'installation terminée, modifies les fichiers de configuration d'apache comme ci-dessous pour des mesures de sécurité (**/etc/apache2/conf-available/security.conf**) :

```
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
ServerSignature Off
#ServerSignature On
```

Par cette configuration, le serveur web renverra moins d'information lorsque qu'une requête non autorisée est effectuée sur une page web hébergé sur le serveur.

Ajout de la connexion sécurisée https

Pour ajouter un certificat valide sur votre serveur web, nous allons utiliser l'outil certbot, la nouvelle version du paquet letsencrypt sous Linux, permettant d'automatiser la création du certificat et la redirection des requêtes http vers https.

Pour l'installer, lancez la commande suivante :

```
sudo apt install certbot python3-cerbot-apache -y
```

L'installation terminée, lancez la commande suivante pour que l'outil certbot paramètre de lui-même l'ajout des certificat https sur votre serveur web :

```
sudo certbot --apache
```

```
debian@[redacted]:/var/www/winness-rakotozafy.fr$ sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): winness.rakotozafy@outlook.fr 1

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y 2

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y 3
Account registered.
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated)  (Enter 'c' to cancel): winness-rakotozafy.fr 4
Requesting a certificate for winness-rakotozafy.fr
Performing the following challenges:
http-01 challenge for winness-rakotozafy.fr
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-available/winness-rakotozafy.fr-le-ssl.conf
Deploying Certificate to VirtualHost /etc/apache2/sites-available/winness-rakotozafy.fr-le-ssl.conf
Enabling available site: /etc/apache2/sites-available/winness-rakotozafy.fr-le-ssl.conf
Enabled Apache rewrite module
Redirecting vhost in /etc/apache2/sites-enabled/winness-rakotozafy.fr.conf to ssl vhost in /etc/apac

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://winness-rakotozafy.fr 5
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Subscribe to the EFF mailing list (email: winness.rakotozafy@outlook.fr).

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/winness-rakotozafy.fr/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/winness-rakotozafy.fr/privkey.pem
   Your certificate will expire on 2023-07-14. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again with the "certonly" option. To non-interactively
   renew *all* of your certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

(1) Tout d'abord, le script vous demandera de renseigner une adresse de messagerie pour le renouvellement des certificats qui ne sont valides par défaut que pendant 3 mois.

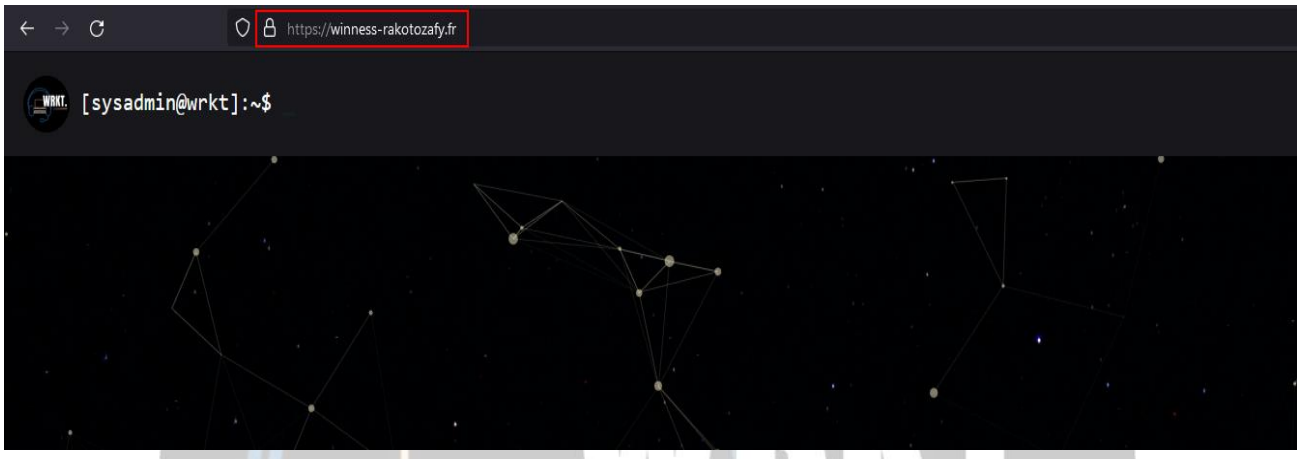
(2) Acceptez les conditions de services et d'utilisation

(3) Nous pouvons ici accepter ou refuser de participer au développement de certbot par des donations

(4) Renseignez ici votre nom de domaine

(5) Vous avez réussi de mettre en place les certificats SSL/TLS pour votre serveur web.

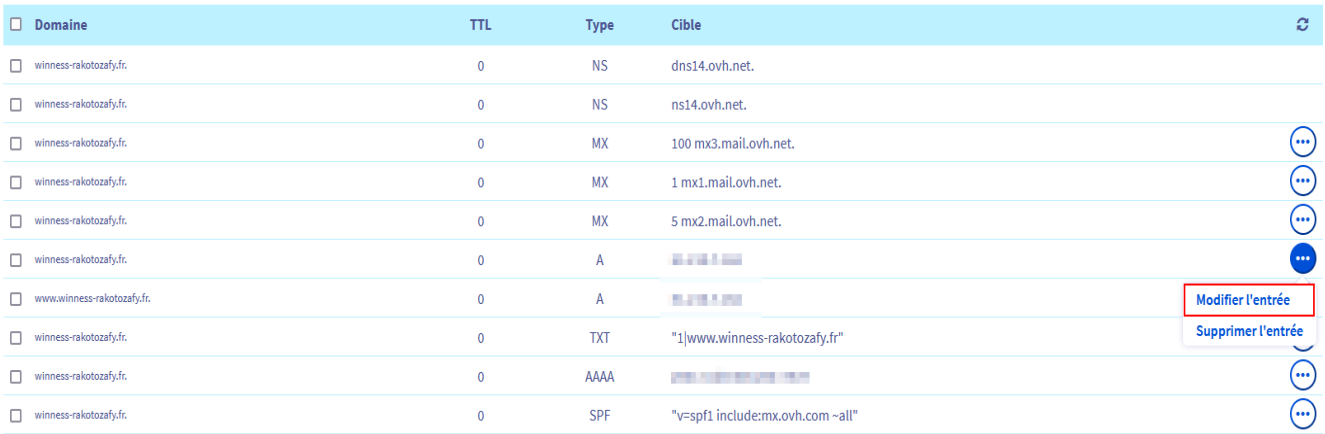
Vérifiez à présent que le site hébergé est bien publié en ouvrant un navigateur et s'y rendre :



 # Hébergement site web OK

III- Paramétrez vos zones DNS

Selon votre hébergeur, il vous suffit d'aller dans le menu de **Zone DNS**. Sélectionnez l'entrée DNS sur votre nom de domaine avec le type A puis sélectionnez **Modifiez l'entrée**.



Puis, renseignez l'adresse IP de votre VPS sous adressage IP et sauvegardez la configuration.

La prise en compte de la modification apportée peut prendre plusieurs minutes, et il vous suffira donc de patienter pour profiter de nouveau site web hébergé sur le VPS.