

SECURISER UN SITE EN HTTPS AVEC CERTBOT (pour Apache)

A LIRE AVANT DE REALISER CE TUTORIEL :

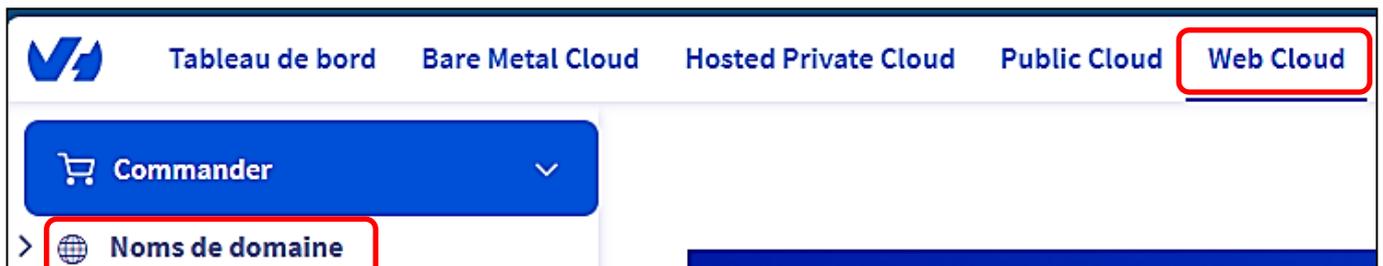
La réalisation de ce tutoriel suppose que vous avez installé un site web Apache sur un serveur externalisé et que vous avez accès à la zone DNS de votre hébergeur web afin de pouvoir créer un sous-domaine (champ de type "A").

1 – INSTALLER CERTBOT POUR APACHE 2.4

Dans notre cas, nous avons installé le logiciel de supervision Zabbix sur un serveur Apache 2.4 fonctionnant sur une machine Debian 12.5. La machine Debian a été créée **sur un serveur externalisé**. **Nous souhaitons accéder à notre logiciel de supervision en https et en utilisant le sous-domaine "zabbix.tutos-info.fr"**.

Actuellement, notre domaine "tutos-info.fr" est hébergé chez OVH. Notre hébergement OVH nous permet de créer un sous-domaine ("zabbix.tutos-info.fr") pointant vers notre serveur externalisé. Pour créer le sous-domaine, nous avons procédé ainsi (procédure valable chez OVH) :

- Se connecter à la console de gestion de l'hébergeur (ici OVH)
- On clique sur le menu "Web Cloud" et "Noms de domaine" :



- **Dans le volet de gauche de la console OVH**, on clique sur le nom du domaine hébergé
- On clique ensuite sur "Zone DNS" et "Ajouter une entrée" :



- On clique sur le **champ de pointage de type "A"** ici :



Un champ de pointage de type "A" permet le pointage d'un nom de domaine vers une adresse IP statique (en général un serveur), type A pour une IPv4 et AAAA pour IPv6. C'est la méthode généralement utilisée pour rediriger votre nom de domaine vers l'adresse IP du serveur Web sur lequel est hébergé votre site Web.

- On saisit le nom du sous-domaine souhaité (ici "zabbix"), **on cible ce sous-domaine vers l'adresse IP publique de notre serveur externalisé** et on clique le bouton "Suivant" :

Ajouter une entrée à la zone DNS Étape 2 sur 3

* Les champs suivis d'un astérisque sont obligatoires.

Sous-domaine .tutos-info.fr.

TTL

Cible *

Le champ A actuellement généré est le suivant :

zabbix IN A 44.44.44.44

Il faut saisir, ici, le sous-domaine souhaité ("zabbix" par exemple).

Il faut saisir, ici, l'adresse IP publique de votre serveur externalisé.

- On clique le bouton "Valider" pour ajouter l'entrée à la zone DNS :

Ajouter une entrée à la zone DNS Étape 3 sur 3

Vous allez ajouter l'entrée suivante dans votre zone DNS :

Type de champ A

Domaine zabbix.tutos-info.fr.

Cible 44.44.44.44

! L'ajout sera immédiat dans la zone DNS, mais veuillez prendre en compte le temps de propagation (maximum 24h).

Une fois la validation effectuée, il faut patienter le temps que les serveurs DNS soient synchronisés (de quelques minutes à plusieurs heures selon l'hébergeur).

Le "ciblage" étant fait, il faut parfois patienter plusieurs minutes (ou heures) selon l'hébergeur pour que la redirection soit opérationnelle. Dans notre cas, celle-ci est fonctionnelle quasi instantanément.

Il faut également créer une règle dans le routeur (ou votre box) permettant d'ouvrir le port "443" à destination de la machine Debian. Dans notre cas, nous avons un routeur IPFIRE et avons créé la règle DNAT suivante :

Règles de pare-feu

Source

Adresse source (adresse MAC/IP ou réseau)

Réseaux standards : ROUGE

Localisation : A1 - Anonymous Proxy

NAT

Utiliser la traduction d'adresses réseau (NAT)

Destination NAT (redirection de port)

Source NAT

Interface pare-feu: - Automatique -

Destination

Adresse IP de destination (adresse IP ou réseau) : 192.168.100.114

Réseaux standards : ROUGE

Localisation : A1 - Anonymous Proxy

Protocole

Services : HTTPS

Groupes de service

Sur IPFIRE, la source est l'interface "wan" dite "RED".

On active la redirection vers une machine du réseau LAN (DNAT).

On indique l'IP (privée) de la machine Debian connectée au réseau LAN et qui héberge Zabbix.

On "ouvre" ici le port HTTPS (TCP/443).

La règle s'affiche dans IPFIRE ; n'oubliez pas de l'activer :

| # | Protocole | Source | Journal | Destination | Action |
|---|-----------|--------|--------------------------|--|---|
| 1 | TCP | ROUGE | <input type="checkbox"/> | Pare-feu : 443 ->192.168.100.114: HTTPS | <input checked="" type="checkbox"/>     |

Votre système est maintenant préparé et nous pouvons poursuivre avec les modifications sur la machine Debian hébergeant le site web Zabbix.

INSTALLATION DE CERTBOT POUR APACHE 2.4

Certbot est un **client utilisé pour demander un certificat à partir de Let's Encrypt et le déployer sur un serveur Web**. Let's Encrypt utilise le protocole **ACME** pour émettre des certificats, et Certbot est un client activé pour ACME qui interagit avec Let's Encrypt. Les certificats, gratuits, sont délivrés pour une période de 3 mois et sont renouvelés automatiquement lorsqu'ils arrivent à expiration.

- Connectez-vous à votre machine Debian sur laquelle le site web Zabbix a été installé avec un utilisateur disposant des droits "sudo" (ou alors en "root" mais cela est déconseillé en production).
- Mettez à jour les paquets de votre distribution Debian :

apt update
apt upgrade -y

- Installez Cerbot pour Apache :

apt install certbot python3-certbot-apache

2 – FICHER DE CONFIGURATION APACHE 2.4 POUR LE SITE WEB PAR DEFAULT

Actuellement, le site web Zabbix est accessible via : http://ip_ou_zabbix.tutos-info.fr/zabbix

MODIFICATION DU FICHER DE CONFIGURATION PAR DEFAULT D'APACHE 2.4

Ici, notre machine Debian n'héberge que le logiciel Zabbix. Il n'y a pas d'autres sites hébergés sur Apache ; en conséquence, nous utilisons le fichier de configuration par défaut d'Apache nommé "000-default.conf".

- Éditez le fichier de configuration par défaut d'Apache (fichier "000-default.conf") :

nano /etc/apache2/sites-available/000-default.conf

- Modifiez le "DocumentRoot" par /usr/share/zabbix (emplacement des fichiers du site web Zabbix)
- Ajoutez la directive "ServerName" : saisissez le sous-domaine créé chez votre hébergeur et qui pointe sur la machine Debian

Le fichier de configuration par défaut d'Apache ("000-default.conf") doit être modifié comme ci-dessous (attention, **adaptez le nom de votre sous-domaine en saisissant le sous-domaine que vous avez déclaré chez votre hébergeur**) :

```
ServerAdmin webmaster@localhost
DocumentRoot /usr/share/zabbix
ServerName zabbix.mondomaine.fr
```

Dans notre cas, on indique ici le sous-domaine créé chez OVH : zabbix.tutos-info.fr

- Relancez Apache avec la commande suivante :

`systemctl restart apache2`

DEMANDE DE CERTIFICAT LET'S ENCRYPT

- Saisissez la commande suivante pour obtenir un certificat pour votre sous-domaine (par exemple "zabbix.mondomaine.fr") :

`certbot --apache`

- Si vos paramètres sont corrects, Certbot affiche le "virtualhost" Apache avec votre sous-domaine précédé d'un chiffre ("1: zabbix.mondomaine.fr" ici)
- Saisissez le chiffre "1" et pressez la touche "**Entrée**" pour lancer la procédure ; un écran affiche la demande de certificat :

```
root@zabbix:/etc/apache2/sites-enabled# certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
We recommend selecting either all domains, or all domains in a VirtualHost/server block.
-----
1:  zabbix.mondomaine.fr
-----
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
Requesting a certificate for  zabbix.mondomaine.fr

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/zabbix.mondomaine.fr  llchain.pem
Key is saved at:      /etc/letsencrypt/live/zabbix.mondomaine.fr  ivkey.pem
This certificate expires on 2024-09-25.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for zabbix.mondomaine.fr  /etc/apache2/sites-available/000-default-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://zabbix.mondomaine.fr

-----
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
-----
```

Si le sous-domaine est validé, le certificat est généré et vous possédez maintenant un accès HTTPS à l'interface web de Zabbix.

Note : n'oubliez pas d'ouvrir le port "443" (HTTPS) dans votre routeur afin que l'accès soit opérationnel depuis l'extérieur de votre réseau !