

SECURISER L'ACCES AU FRONTEND ZABBIX 7



SOMMAIRE

- 1. INSTALLATION DE CERTBOT POUR APACHE 2.4**
- 2. CONFIGURATION HTTPS APACHE 2.4 POUR ZABBIX**
 - a. Modification du fichier de configuration par défaut**
 - b. Demande de certificat Let's Encrypt avec Certbot**
- 3. SECURISATION DE L'ACCES A LA CONSOLE WEB DE ZABBIX 7**
 - a. Modification de l'identification au compte "Admin"**
 - b. Création d'un compte utilisateur**
- 4. SECURISATION DE LA MACHINE DEBIAN HEBERGEANT ZABBIX 7**

© tutos-info.fr - 07/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

A LIRE AVANT DE REALISER CE TUTORIEL :

La réalisation de ce tutoriel suppose que vous avez installé Zabbix 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").

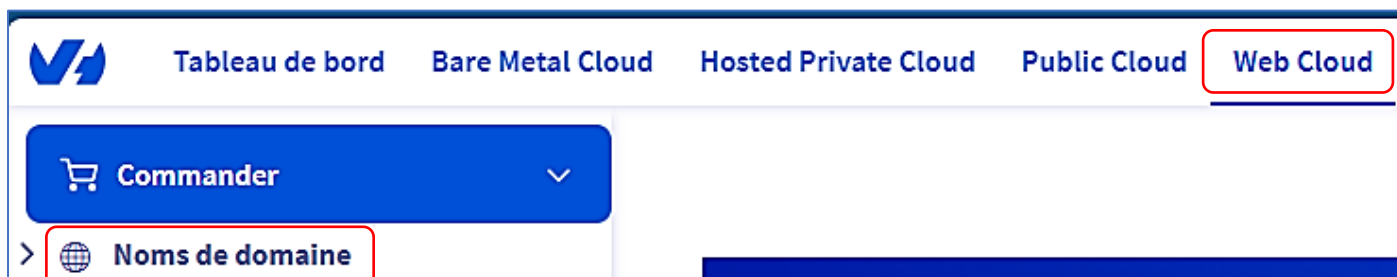
1 – INSTALLER CERTBOT POUR APACHE 2.4

Par défaut, l'interface web de Zabbix est accessible via un navigateur en HTTP (non sécurisé). Si vous avez installé Zabbix en local et en suivant nos tutoriels ce n'est pas grave et le changement du mot de passe du compte administrateur par défaut améliorera la sécurité. Cependant, si l'installation a été réalisée sur un serveur externalisé, il convient de configurer un accès à l'interface web de Zabbix via le protocole HTTPS.

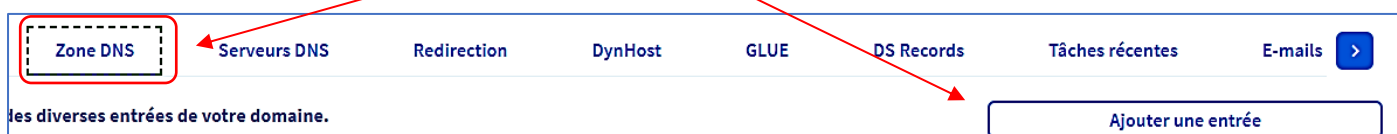
Dans notre cas, **Zabbix a été installé** avec le serveur web Apache 2.4 (voir tutoriel 1) **sur un serveur externalisé. Nous avons créé un sous-domaine "zabbix.mondomaine.fr" qui pointe vers notre serveur et notre machine Debian.**

Pour notre tutoriel, nous utilisons un hébergement OVH qui nous permet de créer un sous-domaine pointant vers notre serveur. Nous possédons un routeur configuré en mode "Red + Green" de type IPFIRE. Pour créer le sous-domaine, nous avons procédé ainsi (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" :

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 :

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 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 :





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 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 serveur 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 – CONFIGURATION APACHE 2.4 POUR ZABBIX

Actuellement, l'interface web de Zabbix est accessible via : http://ip_ou_nomdomaine/zabbix

MODIFICATION DU FICHIER DE CONFIGURATION PAR DEFAUT D'APACHE 2.4

- 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
- 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
```

- 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/fullchain.pem
Key is saved at: /etc/letsencrypt/live/zabbix.mondomaine.fr/privkey.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 !

3 – SECURISATION DE L'ACCES A LA CONSOLE DE GESTION WEB DE ZABBIX 7

MODIFICATION DE L'IDENTIFICATION DU COMPTE ADMINISTRATEUR PAR DEFAUT

La configuration de l'accès à la console avec le protocole HTTPS est une première étape de sécurisation. Il convient, également, de modifier les paramètres d'identification pour le compte administrateur Zabbix par défaut. En effet, le compte par défaut "Admin" avec le mot de passe "zabbix" est très connu et doit être impérativement modifié pour éviter toutes tentatives d'intrusion.

- Connectez-vous à l'interface web de Zabbix avec les identifiants par défaut (Admin/zabbix)
- Dans le volet de gauche, cliquez "**Utilisateurs**" – "**Utilisateurs**"
- Cliquez sur l'utilisateur "**Admin**"; une fenêtre s'affiche
- **Modifiez le nom d'utilisateur** 'Admin' par défaut par le nom désiré et **changez le mot de passe** par défaut par un mot de passe fort
- Validez vos paramètres en cliquant le bouton "Actualiser" :

Utilisateurs

Utilisateur
Média
Permissions

* Nom d'utilisateur

Prénom

Nom de famille

Groupes Sélectionner
taper ici pour rechercher

Mot de passe

Langue ⓘ

Fuseau horaire

Thème

Connexion automatique

Auto-déconnexion

* Rafraîchir

* Lignes par page

URL (après connexion)

Il est recommandé de **créer**, également, **un compte utilisateur** qui servira de compte "courant". On affectera à ce compte des **permissions qui lui permettront d'administrer Zabbix**.

En effet, il est préférable d'utiliser un compte utilisateur dédié plutôt que le compte administrateur qui dispose des droits de "SuperAdmin".

CREATION D'UN COMPTE UTILISATEUR "ADMIN" POUR ZABBIX 7

- Dans le volet de gauche de l'interface web de Zabbix, cliquez "Utilisateurs" – "Utilisateurs"
- En haut à droite de la fenêtre, cliquez sur le bouton bleu "Créer un utilisateur"
- Complétez la fenêtre (voir page suivante) :

Utilisateurs

Utilisateur Média Permissions

* Nom d'utilisateur

Prénom

Nom de famille

Groupes Sélectionner

* Mot de passe ?

* Mot de passe (une autre fois)

Le mot de passe n'est pas obligatoire pour le type d'authentification non interne.

Langue ⓘ

Fuseau horaire

Thème

Connexion automatique

Auto-déconnexion 15m

* Rafraîchir

* Lignes par page

URL (après connexion)

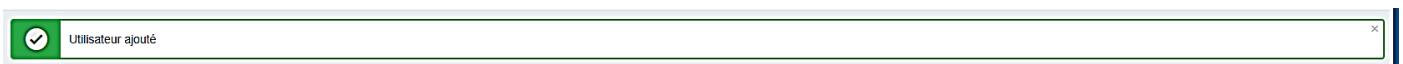
Ajouter Annuler

- Cliquez, ensuite, le lien bleu "**Permissions**" et sélectionnez le rôle "Admin rôle" en cliquant le bouton "**Sélectionner**" :

Permissions

* Rôle Sélectionner

- Cliquez le bouton "**Ajouter**", dans le bas de la fenêtre, pour valider la création de l'utilisateur :



La liste des utilisateurs se présente ainsi :

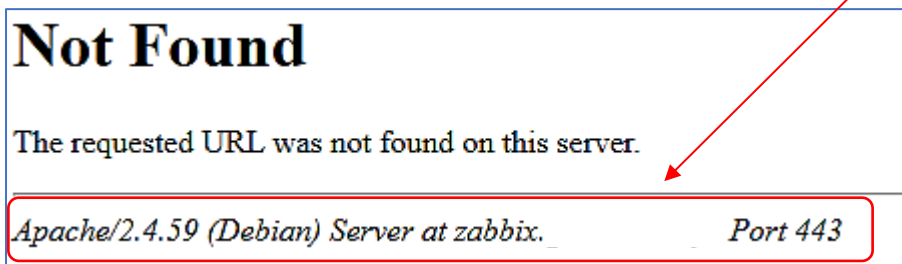
<input type="checkbox"/> Nom d'utilisateur ▲	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État	Provisionné
<input type="checkbox"/> administrateur	tutos-info	Info	Super admin role	Internal, Zabbix administrators	Oui (27/06/2024 13:22:50)	Ok	Interne	Activé	Désactivé	Activé	
<input type="checkbox"/> guest			Guest role	Disabled, Guests, Internal	Non	Ok	Interne	Désactivé	Désactivé	Désactivé	
<input type="checkbox"/> zabbix-user			Admin role		Non	Ok	Valeur système par défaut	Activé	Désactivé	Activé	

4 – SECURISATION DE LA MACHINE DEBIAN HEBERGEANT ZABBIX 7

Comme pour toute machine externalisée hébergeant un serveur web, il convient d'assurer une sécurisation minimale de la machine afin d'éviter les tentatives d'intrusion et de brute force.

SECURISER APACHE

Avec Apache, lorsqu'une page n'est pas trouvée, des informations s'affichent telles que la version du serveur Apache et la distribution Linux utilisée par le serveur web (exemple ci-dessous) :



Il convient de ne pas afficher ces informations en effectuant les manipulations suivantes :

- Éditez le fichier de configuration :

`nano /etc/apache2/conf-available/security.conf`

- Modifiez la valeur des paramètres ci-dessous :

* **server tokens = Prod**

* **server signature = OFF**

* **trace enable = OFF**

```
# 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 Off

#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of: On | Off | extended
TraceEnable Off
#TraceEnable On
```

- Sauvegardez les modifications : **CTRL + X --- O(ui) et "Entrée"**
- Relancez Apache : `systemctl reload apache2`

Si vous saisissez une adresse Zabbix erronée comme <https://zabbix.mondomaine.fr/page> vous constaterez maintenant que les informations de serveur ne s'affichent plus :



INSTALLATION DE FAIL2BAN

Fail2ban est un outil que l'on peut installer sur Debian. Il va se charger de lire et parcourir les logs de différentes applications pour vérifier et détecter des comportements qualifiés de "**suspects**". Il va par exemple savoir détecter un nombre important de tentatives d'authentification infructueuses sur un service **FTP** ou **SSH** et pourra les bannir ou détecter des requêtes anormales sur un services web tel qu'Apache.

1 – Installer Fail2ban sur Debian 12 (depuis la console)

```
apt update
apt upgrade -y
apt install fail2ban -y
```

2 – Copier le fichier modèle "jail.conf" en "jail.local"

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

3 – Éditer le fichier "jail.local" et ajouter les éléments donnés ci-dessous :

```
nano /etc/fail2ban/jail.local
```

Éléments à ajouter dans le fichier "**jail.local**", puis quitter en sauvegardant les modifications :

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = journal
backend = systemd
maxretry = 2
findtime = 300
banaction = iptables-allports
bantime = 86400
ignoreip = 127.0.0.1
```

4 – Redémarrer Fail2ban et vérifier le statut

```
systemctl restart fail2ban
systemctl status fail2ban
```

COMMANDES UTILES FAIL2BAN

Bannir une IP

```
fail2ban-client set [nom du jail] banip [IP à bannir]
```

Enlever le ban d'une IP

```
fail2ban-client set [nom du jail] unbanip [IP concerné]
```

Lister les règles

```
fail2ban-client status
```

Afficher les détails d'une règle

```
fail2ban-client status sshd
```

Lister les tentatives de connexion

```
tail /var/log/auth.log
```

Lister les tentatives de connexion (en temps réel)

```
tail -f /var/log/auth.log
```

Si nécessaire créer le fichier auth.log avec droits 640 :

```
touch /var/log/auth.log
```

```
chmod 640 /var/log/auth.log
```

Si les adresses IPv6 ne sont pas gérées, la désactivation se fait au niveau du groupe [Définitions] du fichier « fail2ban.conf » :

```
nano /etc/fail2ban/fail2ban.conf
```

- Décommentez la ligne "allowipv6"
- Saisissez le paramètre "no"
- Quittez et sauvegardez le fichier

Redémarrer Fail2ban et vérifier le statut (statut « active » sans erreur)

```
systemctl restart fail2ban
```

```
systemctl status fail2ban
```

```
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 20:05:40 CET; 21h ago
     Docs: man:fail2ban(1)
  Main PID: 1194316 (fail2ban-server)
    Tasks: 7 (limit: 76819)
   Memory: 65.5M
         CPU: 1min 30.503s
   CGroup: /system.slice/fail2ban.service
           └─1194316 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```