# Documentation Technique : Installation et Configuration de Zabbix

## 1. Installation du serveur Zabbix

### 1.1 Préparer le serveur

Assurez-vous que votre système est à jour :

```
sudo apt update && sudo apt upgrade -y
```

Installez les prérequis :

```
sudo apt install wget curl gnupg2 software-properties-common -y
```

### 1.2 Installer le dépôt Zabbix

Téléchargez et installez le dépôt Zabbix correspondant à votre version Debian (Debian 12 dans cet exemple) :

```
wget
https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release
/zabbix-release_latest+debian12_all.deb
sudo dpkg -i zabbix-release_latest+debian12_all.deb
sudo apt update
```

### 1.3 Installer Zabbix et les dépendances

Installez Zabbix Server, le frontend web, le serveur Apache, MySQL, et l'agent Zabbix :

```
sudo apt install zabbix-server-mysql zabbix-frontend-php
zabbix-apache-conf zabbix-sql-scripts zabbix-agent  -y
```

### 1.4 Installer et configurer MariaDB

Installez MariaDB (ou MySQL si nécessaire) :

```
sudo apt install mariadb-server mariadb-client -y
```

Configurez MariaDB pour Zabbix :

Connectez-vous au serveur MariaDB :

```
sudo mysql -u root -p
```

1.

Créez une base de données et un utilisateur pour Zabbix :
sql

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY
'mot_de_passe_zabbix';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES;
EXIT;
```

2.

## 1.5 Initialiser le schéma de la base de données

Importez le schéma Zabbix dans la base de données :

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql
--default-character-set=utf8mb4 -uzabbix -p zabbix
```

Réinitialisez l'option `log_bin_trust_function_creators` après l'importation :

```
sudo mysql -uroot -p -e "SET GLOBAL log_bin_trust_function_creators
= 0;"
```

## 1.6 Configurer le serveur Zabbix

Éditez le fichier de configuration de Zabbix pour définir le mot de passe de la base de données :

```
nano /etc/zabbix/zabbix_server.conf
```
Trouvez la ligne suivante et renseignez le mot de passe de la base de données créé précédemment :

```
DBPassword=mot_de_passe_zabbix
```

1.

Redémarrez les services Zabbix et Apache :
bash
Copier le code
```
sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
```

2.

### 1.7 Configurer l'interface Web

1. Accédez à l'interface Zabbix via votre navigateur :
   **http://<IP_du_serveur_Zabbix>/zabbix**
2. Suivez l'assistant de configuration :
   - **Database Type** : MySQL
   - **Database Host** : localhost
   - **Database Name** : zabbix
   - **User** : zabbix
   - **Password** : mot_de_passe_zabbix
3. Une fois la configuration terminée, connectez-vous avec :
   - **Nom d'utilisateur** : `Admin`
   - **Mot de passe** : `zabbix`

# 2. Installation de l'agent Zabbix sur le serveur supervisé

### 2.1 Préparer le serveur

Assurez-vous que le serveur supervisé (Debian dans cet exemple) est à jour :

```
sudo apt update && sudo apt upgrade -y
```

### 2.2 Installer le dépôt Zabbix

Ajoutez le dépôt Zabbix :

```
wget
https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release
/zabbix-release_latest+debian12_all.deb
sudo dpkg -i zabbix-release_latest+debian12_all.deb
sudo apt update
```

## 2.3 Installer l’agent Zabbix

```
sudo apt install zabbix-agent -y
```

**en cas de probleme**

**Réinstallation propre de `zabbix-agent`**

Supprimez complètement le package pour corriger les erreurs de configuration :
bash
Copier le code

```
sudo apt remove --purge zabbix-agent
sudo apt autoremove
```

- 
- Réinstallez le package :
  bash
  Copier le code
  ```
  sudo apt install zabbix-agent
  ```

## 2.4 Configurer l'agent Zabbix

Éditez le fichier de configuration :

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

Modifiez les lignes suivantes pour correspondre à votre environnement :

```
Server=<IP_du_serveur_Zabbix>
ServerActive=<IP_du_serveur_Zabbix>
Hostname=<Nom_unique_du_serveur>
```

1. 

Redémarrez et activez l'agent Zabbix :

```
sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent
```

2.

# 3. Ajouter un hôte dans Zabbix

## 3.1 Accéder à l'interface web de Zabbix

Connectez-vous à l'interface Web de Zabbix via **http://<IP_du_serveur_Zabbix>/zabbix**.

## 3.2 Ajouter un nouvel hôte

1. Allez dans **Configuration** → **Hosts**.
2. Cliquez sur **Create host**.
3. Remplissez les champs suivants :
    - **Host name** : Correspond au champ `Hostname` défini dans le fichier de configuration de l'agent Zabbix.
    - **Groups** : Sélectionnez un groupe (ex. `Linux servers`).
    - **Interfaces** :
        - Type : **Agent**
        - IP Address : IP du serveur supervisé (ex. `192.168.182.128`)
        - Port : **10050** (par défaut pour l'agent Zabbix).
4. Cliquez sur **Add** pour enregistrer l'hôte.

# 4. Associer un template pour la supervision

1. Retournez dans **Configuration** → **Hosts** et sélectionnez l'hôte que vous venez de créer.
2. Allez dans l'onglet **Templates**.
3. Cliquez sur **Link new template**.
4. Recherchez et sélectionnez un template approprié (par ex. `Template OS Linux by Zabbix agent`).
5. Cliquez sur **Add**, puis sur **Update** pour enregistrer.

# 5. Vérifier la supervision

### 5.1 Vérifier les données collectées

1. Allez dans **Monitoring → Latest Data**.
2. Recherchez l’hôte ajouté et vérifiez les données collectées (CPU, RAM, disque, etc.).

### 5.2 Vérifier les problèmes

1. Allez dans **Monitoring → Problems**.
2. Vérifiez si des alertes ou problèmes sont détectés pour l’hôte supervisé.

# E-mail

---

## Aperçu

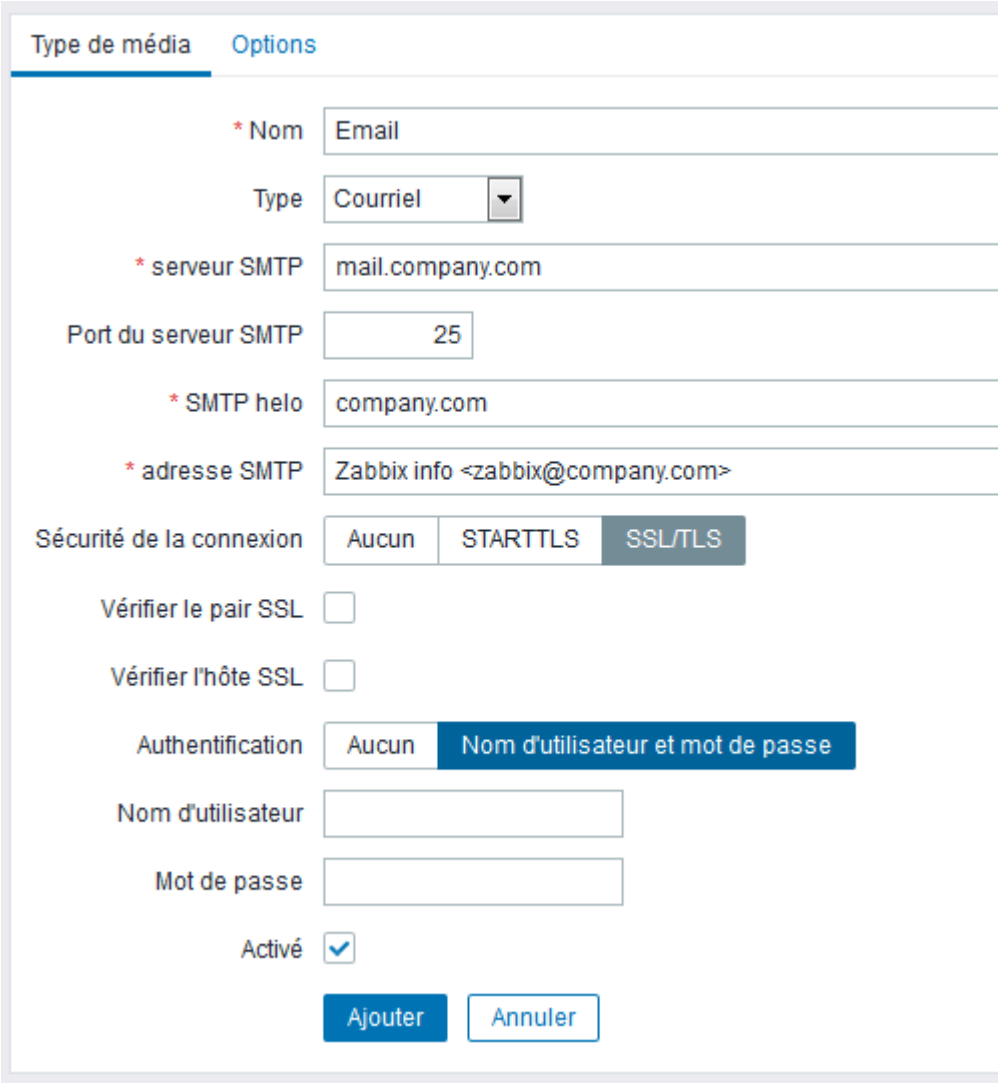
Pour configurer un e-mail en tant que canal de remise des messages, vous devez configurer l'e-mail en tant que type de média et attribuer des adresses spécifiques à des utilisateurs.

## Configuration

Pour configurer l'e-mail comme type de média :

- Allez dans *Administration → Types de média*
- Cliquez sur *Créer un type de média* (ou cliquez sur *Email* dans la liste des type de média pré-définis).

L'onglet **Type de média** contient les attributs généraux de type de média :




Tous les champs de saisie obligatoires sont marqués d'un astérisque rouge.

| Paramètre | Description |
|---|---|
| *Nom* | Nom du type de média. |
| *Type* | Sélectionnez *Courriel* comme type. |
| *serveur SMTP* | Configurez un serveur SMTP pour gérer les messages sortants. |
| *Port du serveur SMTP* | Définissez le port du serveur SMTP pour gérer les messages sortants.<br><br>Cette option est supportée *depuis Zabbix 3.0*. |

| | |
|---|---|
| *SMTP helo* | Définissez une valeur helo SMTP correcte, généralement un nom de domaine. |
| *adresse SMTP* | L'adresse entrée ici sera utilisée comme adresse **De** pour les messages envoyés.<br><br>L'ajout d'un nom d'affichage d'expéditeur (tel que "Zabbix info" dans *Zabbix info <zabbix@company.com>* dans la capture d'écran ci-dessus) avec l'adresse de messagerie réelle est pris en charge depuis la version Zabbix 2.2.<br><br>Il y a des restrictions sur l'affichage des noms dans les emails Zabbix par rapport à ce qui est autorisé par la RFC 5322, comme l'illustrent des exemples :<br><br>Exemples valides :<br><br>*zabbix@company.com* (pas besoin d'utiliser des signes inférieur et supérieur)<br><br>*Zabbix HQ <zabbix@company.com>* (nom d'affichage et adresse email entourée par les signes supérieur et inférieur)<br><br>*∑Ω-monitoring <zabbix@company.com>* (caractères UTF-8 dans le nom d'affichage)<br><br>Exemples non valides :<br><br>*Zabbix HQ zabbix@company.com* (le nom d'affichage est présent mais il n'y a pas de signes inférieur et supérieur autour de l'adresse e-mail)<br><br>*"Zabbix\@\<H(comment)Q\>" <zabbix@company.com>* (bien que valide par la RFC 5322, les guillemets doubles et les commentaires ne sont pas supportés dans les e-mails Zabbix) |
| *Sécurité de la connexion* | Sélectionnez le niveau de sécurité de la connexion :<br><br>**Aucun** - n'utilise pas l'option CURLOPT_USE_SSL<br><br>**STARTTLS** - utilise l'option CURLOPT_USE_SSL avec la valeur CURLUSESSL_ALL |

| | |
|---|---|
| | **SSL/TLS** - l'utilisation de l'option CURLOPT_USE_SSL est optionnelle<br><br>Cette option est supporté *depuis Zabbix 3.0*. |
| *Vérifier le pair SSL* | Cochez cette case pour vérifier le certificat SSL du serveur SMTP.<br><br>La valeur du paramètre de configuration du serveur "SSLCALocation" doit être placée dans CURLOPT_CAPATH pour la validation du certificat.<br><br>Ceci définit l'option cURL CURLOPT_SSL_VERIFYPEER.<br><br>Cette option est supportée *depuis Zabbix 3.0*. |
| *Vérifier l'hôte SSL* | Cochez cette case pour vérifier que le champs *Nom commun* ou le champs *Nom Alternatif* du certificat du serveur SMTP correspond.<br><br>Ceci définit l'option cURL CURLOPT_SSL_VERIFYHOST.<br><br>Cette option est supportée *depuis Zabbix 3.0*. |
| *Authentication* | Sélectionnez le niveau d'authentification :<br><br>**Aucun** - aucune option cURL n'est définie<br><br>(depuis 3.4.2) **Nom d'utilisateur et mot de passe** - implique "AUTH=*" laissant le choix du mécanisme d'authentification à cURL<br><br>(jusqu' 3.4.2) **Mot de passe normal** - CURLOPT_LOGIN_OPTIONS est défini sur "AUTH=PLAIN"<br><br>Cette option est supportée *depuis Zabbix 3.0*. |
| *Nom d'utilisateur* | Nom d'utilisateur à utiliser pour l'authentification.<br><br>Ceci définit la valeur de CURLOPT_USERNAME.<br><br>Cette option est supportée *depuis Zabbix 3.0*. |

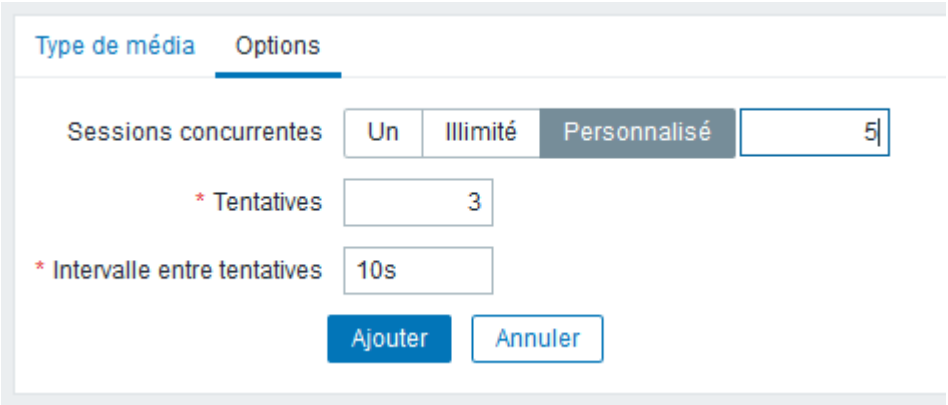
| | |
|---|---|
| *Mot de passe* | Mot de passe à utiliser pour l'authentification.<br><br>Ceci définit la valeur de CURLOPT_PASSWORD.<br><br>Cette option est supportée *depuis Zabbix 3.0*. |
| *Activé* | Cochez cette case pour activer le type de média. |

Pour rendre les options d'authentification SMTP disponibles, le serveur Zabbix doit être compilé avec l'option de compilation --with-libcurl avec cURL version 7.20.0 ou supérieure.

## Options

L'onglet **Options** de la configuration du type de média e-mail contient les paramètres de traitement des alertes. Le même ensemble d'options est également configurable pour d'autres types de média.

Tous les types de média sont traités en parallèle. Le nombre maximal de sessions simultanées est configurable par type de média, mais le nombre total de processus d'alertes sur le serveur ne peut être limité que par le paramètre StartAlerters. Les alertes générées par un déclencheur sont traitées de manière séquentielle.



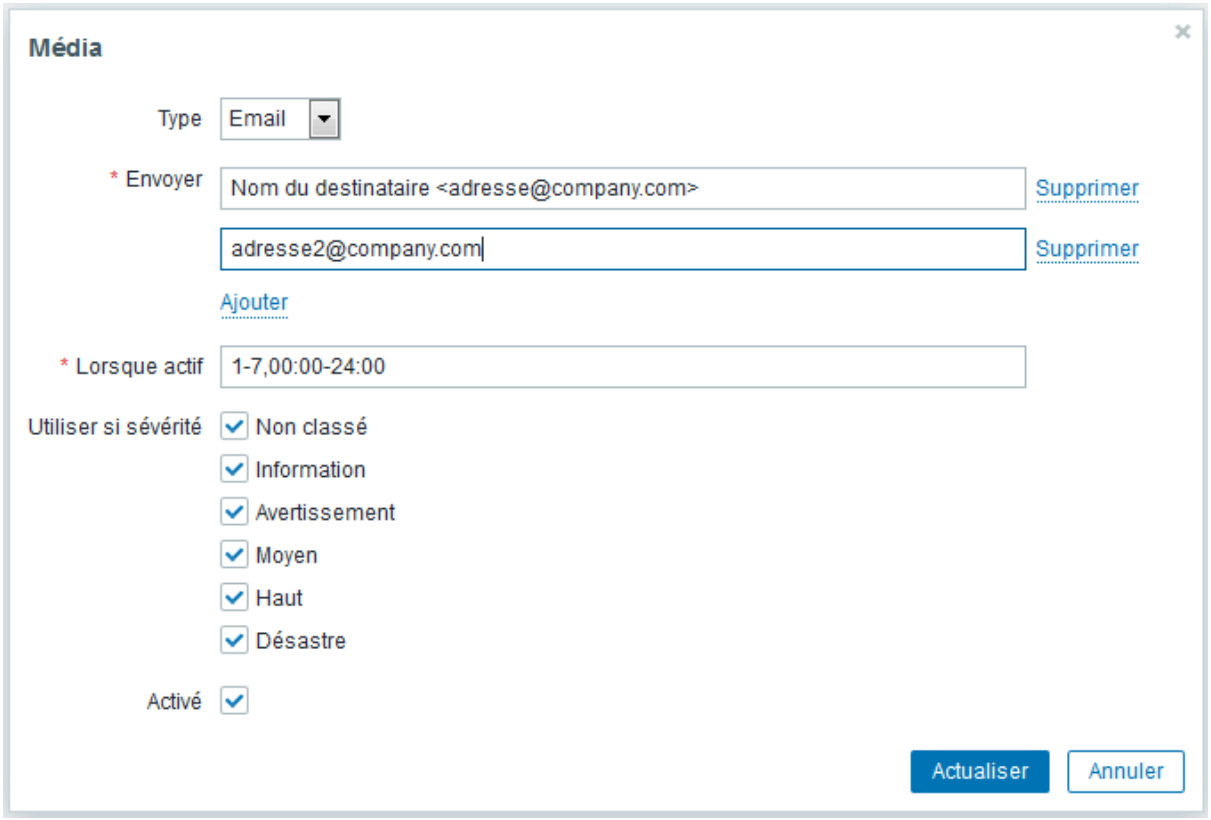

| Paramètre | Description |
|---|---|

| | |
|---|---|
| *Sessions concurrentes* | Sélectionnez le nombre de sessions d'alertes parallèles pour le type de média :<br><br>**Un** - une session<br><br>**illimité** - nombre de sessions illimité<br><br>**Personnalisé** - sélectionnez un nombre personnalisé de sessions.<br><br>Un nombre illimité ou des valeurs élevées signifient davantage de sessions parallèles et une capacité accrue d'envoi de notifications. Les valeurs illimitées et les valeurs élevées doivent être utilisées dans les grands environnements où de nombreuses notifications peuvent devoir être envoyées simultanément. |
| *Tentatives* | Nombre de tentatives pour l'envoie d'une notification. Vous pouvez spécifier jusqu'à 10 tentatives ; la valeur par défaut est '3'. Si '1' est spécifié, Zabbix n'enverra la notification qu'une seule fois et ne réessayera pas si l'envoi échoue. |
| *Intervalle entre tentatives* | Fréquence des tentatives de renvoi d'une notification en cas d'échec de l'envoi, en secondes (0 à 60). Si '0' est spécifié, Zabbix réessayera immédiatement.<br><br>Les suffixes temporels sont supportés, par exemple 5s, 1m. |

## Médias utilisateur

Pour attribuer une adresse spécifique à l'utilisateur:

- Allez dans *Administration* → *Utilisateurs*.
- Ouvrez le formulaire de propriétés de l'utilisateur.
- Dans l'onglet Media, cliquez sur *Ajouter*.




Attributs de média utilisateur :

| Paramètre | Description |
|---|---|
| *Type* | Sélectionnez *Email* comme type. |
| *Envoyer* | Spécifiez les adresses e-mails auxquelles envoyer les messages.<br><br>Pour ajouter plusieurs adresses, cliquez sur *Ajouter* sous le champ d'adresse. Si plusieurs adresses électroniques sont spécifiées, un seul e-mail sera envoyé à tous les destinataires spécifiés.<br><br>Vous pouvez ajouter le nom complet du destinataire (comme "Nom du destinataire" dans *Nom du destinataire <addresse@company.com>* dans la capture d'écran ci-dessus) avec l'adresse e-mail réelle. Voir les exemples et les restrictions sur le nom d'affichage et l'adresse e-mail dans la description de l'attribut de type de média e-mail SMTP. |

| | |
|---|---|
| *Lorsque actif* | Vous pouvez limiter le temps d'envoi des messages, par exemple, les jours ouvrables uniquement (1-5,09:00-18:00).<br><br>Voir la page de spécification de période pour la description du format. Les macros utilisateur sont supportées. |
| *Utiliser si sévérité* | Cochez les cases des sévérités de déclencheur pour lesquelles vous souhaitez recevoir des notifications.<br><br>*Notez* que la sévérité par défaut ('Non classé') **doit être** cochée si vous souhaitez recevoir des notifications pour des événements non basés sur les déclencheurs.<br><br>Après avoir enregistré, les niveaux de sévérité sélectionnés seront affichés dans les couleurs de niveau de sévérité correspondantes, tandis que les niveaux non sélectionnés seront grisés. |
| *Activé* | Cochez la case pour activer le média pour l'utilisateur. |

# Sécuriser zabbix avec https:

### 1.2. Ajouter un Nom de Domaine Local

On va donner un nom à ton serveur pour éviter d'utiliser une adresse IP.

Édite le fichier **/etc/hosts** :

sudo nano /etc/hosts

Ajoute cette ligne :

192.168.1.100  zabbix.local

Maintenant, ton serveur comprendra que `zabbix.local` correspond à son **IP locale**.

## 2. Générer un Certificat Auto-signé

On va créer un certificat SSL auto-signé pour **zabbix.local**.

### 2.1. Créer une Autorité de Certification (CA)

On va créer un **CA interne** qui signera les certificats SSL.

**Créer un dossier pour stocker les certificats** :
sudo mkdir -p /etc/ssl/zabbix
cd /etc/ssl/zabbix

1.

**Générer une clé privée pour le CA** :
sudo openssl genrsa -aes256 -out zabbix-ca.key 2048

2.

**Créer un certificat CA** :
sudo openssl req -x509 -new -nodes -key zabbix-ca.key -sha256 -days 3650 -out zabbix-ca.pem

3.
    - **Common Name (CN)** : `Zabbix-CA`
    - **Autres infos** : entre ton nom, ville, entreprise.

---

## 2.2. Créer un Certificat SSL pour Zabbix

**Générer une clé privée pour le serveur Zabbix** :
sudo openssl genrsa -out zabbix.key 2048

1.

**Créer une demande de certificat (CSR)** :
sudo openssl req -new -key zabbix.key -out zabbix.csr

2.
    - **Common Name (CN)** : `zabbix.local`

**Ajouter des noms alternatifs (SAN)** Crée un fichier `csr.ext` :
sudo nano csr.ext
Ajoute :
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = zabbix.local
IP.1 = 192.168.1.100  # Change selon ton IP locale

3.

**Signer le certificat avec le CA** :
sudo openssl x509 -req -in zabbix.csr -CA zabbix-ca.pem -CAkey zabbix-ca.key -CAcreateserial -out zabbix.crt -days 3650 -sha256 -extfile csr.ext

4.

## 2.3. Placer les certificats au bon endroit

Déplace les certificats et définis les permissions :

sudo mv zabbix.key /etc/ssl/private/
sudo mv zabbix.crt /etc/ssl/certs/
sudo mv zabbix-ca.pem /etc/ssl/certs/
sudo chmod 600 /etc/ssl/private/zabbix.key

## 3.1. Activer le module SSL

bash
Copier le code
```
sudo a2enmod ssl
```

### 3.2. Modifier la configuration Apache

Crée un fichier Apache :

```
sudo nano /etc/apache2/sites-available/zabbix.conf
```

Ajoute :

```
<VirtualHost *:80>
    ServerName zabbix.local
    Redirect permanent / https://zabbix.local/
</VirtualHost>

<VirtualHost *:443>
    DocumentRoot /usr/share/zabbix
    ServerName zabbix.local
    Alias /zabbix /usr/share/zabbix

    <Directory "/usr/share/zabbix">
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/zabbix_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/zabbix_ssl_access.log combined

    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/zabbix.crt
    SSLCertificateKeyFile /etc/ssl/private/zabbix.key
    SSLCertificateChainFile /etc/ssl/certs/zabbix-ca.pem
</VirtualHost>
```

### 3.3. Activer le site et redémarrer Apache

```
sudo a2ensite zabbix
sudo systemctl restart apache2
```

---

## 4. Tester l'Accès HTTPS

Depuis le serveur, ouvre un navigateur et accède à :

```
https://zabbix.local
```