

Ce guide permet de générer et de configurer des certificats **SSL/TLS** pour le serveur **Zulip** en utilisant **OpenSSL**.

OpenSSL offre un contrôle total sur le processus de génération et de gestion des certificats **SSL/TLS**. On peut personnaliser les paramètres tels que la longueur de la clé, les algorithmes de chiffrement, etc., en fonction des besoins spécifiques. Cela permet une adaptation précise des certificats à l'infrastructure et aux exigences de sécurité.

1. Génération de la clé privée de l'autorité de certification (CA) :

```
openssl genrsa -aes256 -out ca.key 4096
```

2. Génération du certificat autosigné pour l'autorité de certification (CA) :

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3000 -out ca.crt
```

3. Génération de la clé privée du serveur Zulip :

```
openssl genrsa -aes256 -out zulip.key 4096
```

4. Création de la demande de signature de certificat (CSR) pour le serveur Wazuh :

```
openssl req -new -key zulip.key -out zulip.csr
```

5. Signature du certificat du serveur Zulip par l'autorité de certification (CA) :

```
openssl x509 -req -in zulip.csr -CA ca.crt -CAkey ca.key -out zulip.crt -days 300 -sha256
```

6. Modification des permissions de la clé privée du serveur Wazuh :

```
chmod 644 zulip.key
```

7. Copie des certificats dans les répertoires appropriés :

```
cp *.key /etc/ssl/private/  
cp *.csr /etc/ssl/certs/  
cp *.crt /etc/ssl/certs/
```

8. Déchiffrement de la clé privée du serveur Zulip :

```
openssl rsa -in /etc/ssl/private/zulip.key -out /etc/ssl/private/zulip_decrypted.key
```

9. Configuration du fichier de configuration Zulip : On ouvre le fichier de configuration de **Nginx** pour les certificats de **Zulip** à l'aide d'un éditeur de texte :

```
nano /etc/nginx/sites-enabled/zulip-enterprise
```

10. Puis, on modifie les lignes suivantes pour refléter les chemins vers les certificats et clés :

```
server {  
    ...  
    ssl_certificate /etc/ssl/certs/zulip.crt;  
    ssl_certificate_key /etc/ssl/private/zulip_decrypted.key;  
    ...  
}
```

11. Redémarrage du service nginx : Après avoir effectué les modifications nécessaires, on redémarre le service **nginx** pour appliquer les changements :

```
systemctl restart nginx
```

Une fois ces étapes suivies, le serveur **Zulip** devrait être configuré pour utiliser des certificats **SSL/TLS** sécurisés générés à l'aide d'**OpenSSL**.

Lecteur du certificat : zulip.local

Général Détails

Émis pour

Nom commun (CN)	zulip.local
Organisation (O)	AIST21
Unité d'organisation (OU)	certs

Émis par

Nom commun (CN)	ca.zulip.local
Organisation (O)	AIST21
Unité d'organisation (OU)	certs

Durée de validité

Émis le	lundi 18 mars 2024 à 11:55:13
Expire le	dimanche 12 janvier 2025 à 11:55:13