coturn

Un serveur TURN permet d'assurer la connectivité des clients même s'ils sont derrière des routeurs NAT ou des pare-feux restrictifs, en utilisant un relais tiers pour transférer les paquets de données. **coturn** remplie ce rôle.

Installation de coturn

Pour installer un service TURN sur Debian, vous pouvez suivre les étapes suivantes.

Ouvrez un terminal et mettez à jour votre système avec la commande suivante :

```
sudo apt-get update
```

Installez le service TURN en utilisant la commande suivante :

```
sudo apt-get install coturn
```

Une fois l'installation terminée, vous pouvez éditer le fichier de configuration de TURN en utilisant la commande suivante :

```
sudo nano /etc/turnserver.conf
```

Modifiez les paramètres de configuration selon vos besoins.

Démarrez le service TURN avec la commande suivante :

```
sudo systemctl start coturn
```

Vérifiez que le service est en cours d'exécution avec la commande suivante :

```
sudo systemctl status coturn
```

Vous pouvez également configurer le service TURN pour qu'il démarre automatiquement au démarrage du système en utilisant la commande suivante :

```
sudo systemctl enable coturn
```

Paramètres de coturn

La configuration de turnserver.conf dépend des besoins de votre environnement et des fonctionnalités que vous souhaitez activer ou désactiver pour votre serveur TURN. Cependant, voici quelques paramètres de configuration courants que vous pouvez modifier dans le fichier turnserver.conf :

- listening-port : le port sur lequel le serveur TURN écoute les connexions entrantes.
- relay-ip : l'adresse IP que le serveur TURN utilisera pour relayer les flux de données.
- realm : le nom de domaine utilisé pour identifier le service de relais.
- user et userdb : les paramètres utilisés pour configurer l'authentification des utilisateurs et le stockage des informations d'identification.
- min-port et max-port : les ports utilisés pour relayer les flux de données.
- lt-cred-mech : un mécanisme d'authentification qui exige une preuve de l'identité de l'utilisateur à chaque connexion.
- cert et pkey : les chemins d'accès aux certificats SSL/TLS utilisés pour sécuriser les connexions.
- fingerprint : le type de hachage utilisé pour générer les empreintes digitales de certificat.
- no-udp : une option qui désactive le protocole UDP pour les connexions entrantes.

Ressources

- man turnserver
- wiki corturn

— *CPT*