Essayez V2Ray : Un Guide Étape par Étape

V2Ray est une plateforme polyvalente pour créer des proxies afin de contourner les restrictions réseau et d'améliorer la confidentialité en ligne. Dans ce guide, nous vous expliquerons comment installer et configurer V2Ray sur un serveur Ubuntu. Nous aborderons les étapes d'installation, les fichiers de configuration, les problèmes courants et les méthodes de vérification pour s'assurer que tout fonctionne correctement.

Table des matières

Installation

Commencez par télécharger et installer V2Ray en utilisant le script d'installation fourni.

```
ubuntu@ip-172-26-0-236:~$ curl -L https://raw.githubusercontent.com/v2fly/fhs-install-v2ray/master/insta
```

Exécutez le Script d'Installation :

```
chmod +x in.sh
sudo ./in.sh
```

Sortie de l'installation :

```
[Install]
WantedBy=multi-user.target
```

info: V2Ray v5.22.0 est installé.

Remarque : Le script suggère de supprimer les logiciels dépendants si nécessaire :

```bash
apt purge curl unzip
```

Configuration

Configuration de V2Ray (`config.json`)

Ce fichier JSON définit les paramètres d'entrée et de sortie pour V2Ray.

```
{
    "inbounds": [
        {
            "port": 1080,
            "listen": "0.0.0.0",
            "protocol": "vmess",
            "settings": {
                "clients": [
                    {
                        "id": "9f02f6b2-1d7d-4b10-aada-69e050f1be6b",
                        "level": 0,
                        "alterId": 0,
                        "email": "example@v2ray.com",
                        "security": "auto"
                    }
                ]
            },
            "streamSettings": {
                "network": "tcp"
            },
            "sniffing": {
                "enabled": true,
```

```
                "destOverride": [
                    "http",
                    "tls"
                ]
            },
            "tag": "vmess-inbound",
            "udp": true
        }
    ],
    "outbounds": [
        {
            "protocol": "freedom",
            "settings": {},
            "tag": "outbound-freedom",
            "udp": true
        }
    ],
    "log": {
        "loglevel": "debug",
        "access": "/var/log/v2ray/access.log",
        "error": "/var/log/v2ray/error.log"
    },
    "stats": {
        "enabled": false
    },
    "environment": {
        "v2ray.vmess.aead.forced": "false"
    }
}
```

Points clés : - Inbounds : Définit les points d'entrée pour les connexions entrantes. Ici, il est configuré pour utiliser le protocole `vmess` sur le port `1080`. - Outbounds : Spécifie où le trafic doit être envoyé. Le protocole `freedom` permet au trafic de passer sans restrictions. - Logging : Configuré pour enregistrer les informations d'accès et d'erreur à des fins de débogage. - Sécurité : Le champ `security` est défini sur `aes-256-gcm` pour un chiffrement renforcé.

Configuration du Proxy (`config.yaml`)

Ce fichier YAML configure les paramètres du proxy, le DNS et les règles de routage du trafic.

```yaml
port: 7890
socks-port: 7891
mixed-port: 7892
allow-lan: true
mode: Rule
log-level: info
external-controller: 0.0.0.0:9090
experimental:
  ignore-resolve-fail: true

dns:
  enable: false
  listen: 0.0.0.0:53
  enhanced-mode: fake-ip
  fake-ip-range: 198.18.0.1/16
  default-nameserver:
    - 119.29.29.29
    - 223.5.5.5
  nameserver:
    - https://223.5.5.5/dns-query
    - https://1.12.12.12/dns-query
  fake-ip-filter:
    - "*.lan"
    - "*.localdomain"
    - "*.example"
    - "*.invalid"
    - "*.localhost"
    - "*.test"
    - "*.local"

proxies:
  - name: "Mon Proxy VMess"
    type: vmess
```

```
    server: 54.254.0.0
    port: 1080
    uuid: "9f02f6b2-1d7d-4b10-aada-0000"
    alterId: 0
    cipher: "aes-128-gcm"
    udp: true

proxy-groups:
  - name: "Proxy"
    type: select
    proxies:
      - "My VMess Proxy"
```

règles: - IP-CIDR,192.168.0.0/16,DIRECT - IP-CIDR,10.0.0.0/8,DIRECT - IP-CIDR,127.0.0.0/8,DIRECT - GEOIP,CN,DIRECT - MATCH,Proxy

Points clés :
- Ports : Configure divers ports pour le trafic HTTP, SOCKS et mixte.
- DNS : Configure les paramètres DNS avec des plages d'adresses IP fictives et des serveurs de noms spé
- Proxies : Définit un proxy VMess avec chiffrement utilisant `aes-128-gcm`.
- Groupes de proxies : Permet de choisir entre différentes options de proxy.
- Règles : Dirige le trafic en fonction des plages d'adresses IP et des localisations géographiques.

Remarque : Assurez-vous que le `cipher` dans la configuration du proxy correspond au paramètre `securit

---

Gestion du service V2Ray

Démarrage du service V2Ray

Pour démarrer le service V2Ray, utilisez la commande suivante :

```bash
sudo systemctl start v2ray
```

Arrêt du service V2Ray

Pour arrêter le service V2Ray, utilisez la commande suivante :

```
sudo systemctl stop v2ray
```

Redémarrage du service V2Ray

Pour redémarrer le service V2Ray, utilisez la commande suivante :

```
sudo systemctl restart v2ray
```

Vérification du statut du service V2Ray

Pour vérifier le statut du service V2Ray, utilisez la commande suivante :

```
sudo systemctl status v2ray
```

Activation du service V2Ray au démarrage

Pour activer le service V2Ray afin qu'il démarre automatiquement au démarrage du système, utilisez la commande suivante :

```
sudo systemctl enable v2ray
```

Désactivation du service V2Ray au démarrage

Pour désactiver le service V2Ray afin qu'il ne démarre pas automatiquement au démarrage du système, utilisez la commande suivante :

```
sudo systemctl disable v2ray
```

Affichage des logs du service V2Ray

Pour afficher les logs du service V2Ray, utilisez la commande suivante :

```
sudo journalctl -u v2ray
```

Ces commandes vous permettront de gérer efficacement le service V2Ray sur votre système.

Après l'installation et la configuration, vous devez gérer le service V2Ray en utilisant `systemctl`.

Activation et démarrage de V2Ray

Activer V2Ray pour qu'il démarre au démarrage :

```
sudo systemctl enable v2ray
```

Démarrer le service V2Ray :

```
sudo systemctl start v2ray
```

Sortie attendue :

```
Symlink créé /etc/systemd/system/multi-user.target.wants/v2ray.service → /etc/systemd/system/v2ray.servi
```

Vérifier l'état du service :

```
sudo systemctl status v2ray
```

Exemple de sortie :

```
 v2ray.service - Service V2Ray
   Loadé : chargé (/etc/systemd/system/v2ray.service; activé; paramètre fournisseur : activé)
   Actif : actif (en cours d'exécution) depuis lun. 2024-04-27 12:55:00 UTC; il y a 1min 30s
 PID principal : 14425 (v2ray)
    Tâches : 8 (limite : 4915)
   Mémoire : 36.7M
   CGroup : /system.slice/v2ray.service
            14425 /usr/local/bin/v2ray run -config /usr/local/etc/v2ray/config.json
```

Problèmes courants et dépannage

Échec de l'authentification lors de l'activation de V2Ray

Message d'erreur :

```
==== AUTHENTIFICATION POUR org.freedesktop.systemd1.manage-unit-files ====
Une authentification est requise pour gérer les services système ou les fichiers d'unités.
Authentification en tant que : Ubuntu (ubuntu)
Mot de passe :
polkit-agent-helper-1: pam_authenticate a échoué : Échec de l'authentification
==== ÉCHEC DE L'AUTHENTIFICATION ====
Échec de l'activation de l'unité : Accès refusé
```

Solution :

Assurez-vous d'utiliser `sudo` pour exécuter les commandes qui nécessitent des privilèges administratifs.

Commande correcte :

```
sudo systemctl enable v2ray
```

Vérification

Après avoir démarré le service V2Ray, vérifiez qu'il fonctionne correctement.

Vérifier les processus en cours d'exécution

```
ps aux | grep v2ray
```

Exemple de sortie :

```
nobody     14425  4.4  8.6 5460552 36736 ?       Ssl  12:55   0:00 /usr/local/bin/v2ray run -config /usr
ubuntu     14433  0.0  0.5   7076  2176 pts/1    S+   12:55   0:00 grep --color=auto v2ray
```

Tester la connectivité avec Telnet

```
telnet votre_adresse_ip_serveur 1080
```

Comportement attendu :

- Si la connexion est réussie, vous verrez une réponse du service V2Ray.
- Pour quitter Telnet, appuyez sur `Ctrl + ]` puis tapez `quit`.

Conclusion

La configuration de V2Ray sur un serveur Ubuntu implique l'installation du logiciel, la configuration des paramètres entrants et sortants, la gestion du service avec `systemctl`, et la vérification de son fonctionnement. En suivant ce guide, vous devriez disposer d'une installation fonctionnelle de V2Ray qui améliore votre confidentialité réseau et contourne efficacement les restrictions.

Si vous rencontrez des problèmes ou avez des questions, n'hésitez pas à laisser un commentaire ci-dessous !

Conseils supplémentaires

- **Sécurité** : Assurez-vous toujours que votre UUID V2Ray et vos mots de passe sont conservés en toute sécurité.
- **Mises à jour** : Mettez régulièrement à jour V2Ray pour bénéficier des dernières fonctionnalités et des correctifs de sécurité.
- **Surveillance** : Utilisez les journaux situés dans `/var/log/v2ray/` pour surveiller les performances et résoudre les problèmes.

Bonne navigation avec votre proxy !