V2Ray を試してみよう：ステップバイステップガイド

V2Ray は、ネットワーク制限を回避し、オンラインプライバシーを強化するための多機能なプロキシ構築プラットフォームです。このガイドでは、Ubuntu サーバーに V2Ray をインストールし、設定する手順を説明します。インストール手順、設定ファイル、一般的な問題、およびすべてがスムーズに動作することを確認するための検証方法についてカバーします。

目次

インストール

まず、提供されているインストールスクリプトを使用して V2Ray をダウンロードし、インストールします。

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

このコマンドは、指定された URL から `install-release.sh` スクリプトをダウンロードし、`in.sh` という名前のファイルとして保存します。`curl` コマンドの`-L` オプションは、リダイレクトに従うことを意味します。

インストールスクリプトを実行:

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

このコマンドは、in.sh というスクリプトファイルに実行権限を付与し、その後、管理者権限でそのスクリプトを実行するものです。具体的には：

1. chmod +x in.sh：in.sh ファイルに実行権限を追加します。
2. sudo ./in.sh：管理者権限（sudo）で in.sh スクリプトを実行します。

インストール出力:

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

info: V2Ray v5.22.0 がインストールされました。

注：スクリプトは、必要に応じて依存ソフトウェアを削除することを提案しています：

```bash
apt purge curl unzip
```

このコマンドは、curl と unzip パッケージをシステムから完全に削除するために使用されます。apt purge コマンドは、指定されたパッケージとその設定ファイルを削除します。

設定

V2Ray 設定 (config.json)

この JSON ファイルは、V2Ray のインバウンドとアウトバウンドの設定を定義しています。

```
{
    "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"
    }
}
```

キーポイント: - **Inbounds**: 着信接続のエントリーポイントを定義します。ここでは、ポート 1080 で `vmess` プロトコルを使用するように設定されています。- **Outbounds**: トラフィックの送信先を指定します。`freedom` プロトコルは、制限なくトラフィックを通過させます。- **Logging**: デバッグ目的でアクセスとエラー情報をログに記録するように設定されています。- **Security**: セキュリティ強化のために、`security` フィールドが `aes-256-gcm` に設定されています。

プロキシ設定 (`config.yaml`)

この YAML ファイルは、プロキシ設定、DNS、およびトラフィックルーティングのルールを構成します。

```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
```

この YAML 設定は、ネットワークプロキシソフトウェア（おそらく Clash など）の設定ファイルの一部です。以下に各設定項目の説明を日本語で示します：

- `port: 7890`：HTTP プロキシのポート番号を 7890 に設定します。
- `socks-port: 7891`：SOCKS プロキシのポート番号を 7891 に設定します。
- `mixed-port: 7892`：HTTP と SOCKS の両方のプロキシをサポートする混合ポートを 7892 に設定します。
- `allow-lan: true`：ローカルエリアネットワーク（LAN）からの接続を許可します。

- `mode: Rule`：プロキシモードを「Rule」に設定します。これは、ルールに基づいてトラフィックをルーティングするモードです。
- `log-level: info`：ログレベルを「info」に設定します。これにより、情報レベルのログが記録されます。
- `external-controller: 0.0.0.0:9090`：外部コントローラーのアドレスを `0.0.0.0:9090` に設定します。これにより、外部からのコントロールが可能になります。
- `experimental:`：実験的な機能の設定セクションです。
  - `ignore-resolve-fail: true`：DNS 解決が失敗した場合でも無視して処理を続行します。

この設定は、ネットワークトラフィックをプロキシ経由でルーティングするための基本的な設定を提供します。

```
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"
```

この設定は、DNS 関連の設定を定義しています。以下に各項目の説明を日本語で示します。

- `enable: false`: DNS 機能を無効にします。
- `listen: 0.0.0.0:53`: DNS サーバーがすべてのネットワークインターフェースでポート 53 をリッスンします。

- enhanced-mode: fake-ip: ファイアウォールやプロキシをバイパスするために、偽の IP アドレスを使用するモードを有効にします。
- fake-ip-range: 198.18.0.1/16: 偽の IP アドレスの範囲を指定します。
- default-nameserver: デフォルトの DNS サーバーを指定します。ここでは 119.29.29.29 と 223.5.5.5 が指定されています。
- nameserver: DNS クエリを送信するための DNS サーバーを指定します。ここでは https://223.5.5.5/dns-query と https://1.12.12.12/dns-query が指定されています。
- fake-ip-filter: 偽の IP アドレスを使用しないドメインを指定します。ここでは *.lan、*.localdomain、*.example、*.invalid、*.localhost、*.test、*.local が指定されています。

```
proxies:
  - name: "My VMess Proxy"
    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: " プロキシ"
    type: select
    proxies:
      - "My VMess Proxy"

rules:
  - 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
```

キーポイント: - ポート: HTTP、SOCKS、および混合トラフィック用のさまざまなポートを設定します。- DNS: 偽の IP 範囲と指定されたネームサーバーを使用して DNS 設定を行います。- プロキシ: aes-128-gcm を使用した暗号化で VMess プロキシを定義します。- プロキシグループ: 異なるプロキシオプション間での選択を可能にします。- ルール: IP 範囲と地理的位置に基づいてトラフィックを誘導します。

注：プロキシ設定の `cipher` が `config.json` の `security` 設定と一致していることを確認してください。

V2Ray サービスの管理

インストールと設定が完了したら、`systemctl` を使用して V2Ray サービスを管理する必要があります。

V2Ray の有効化と起動

V2Ray を起動時に自動起動するように設定する:

```
sudo systemctl enable v2ray
```

V2Ray サービスを開始:

```
sudo systemctl start v2ray
```

期待される出力:

シンボリックリンク `/etc/systemd/system/multi-user.target.wants/v2ray.service → /etc/systemd/system/v2ra`

サービスステータスの確認:

```
sudo systemctl status v2ray
```

このコマンドは、V2Ray サービスの現在のステータスを確認するために使用されます。`systemctl` は、Linux システムでサービスを管理するためのコマンドで、`status` オプションを指定することで、指定したサービスの状態（実行中かどうか、エラーが発生しているかどうかなど）を表示します。`v2ray` は、ここでは確認したいサービスの名前です。`sudo` は、管理者権限でコマンドを実行するために使用されます。

サンプル出力:

```
 v2ray.service - V2Ray サービス
   Loaded: loaded (/etc/systemd/system/v2ray.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-04-27 12:55:00 UTC; 1分30秒前
 Main PID: 14425 (v2ray)
    Tasks: 8 (limit: 4915)
   Memory: 36.7M
   CGroup: /system.slice/v2ray.service
           14425 /usr/local/bin/v2ray run -config /usr/local/etc/v2ray/config.json
```

よくある問題とトラブルシューティング

V2Ray を有効にした際の認証失敗

エラーメッセージ:

```
==== org.freedesktop.systemd1.manage-unit-files の認証中 ====
システムサービスまたはユニットファイルを管理するには認証が必要です。
認証ユーザー: Ubuntu (ubuntu)
パスワード:
polkit-agent-helper-1: pam_authenticate が失敗しました: 認証失敗
==== 認証失敗 ====
ユニットの有効化に失敗しました: アクセスが拒否されました
```

解決策：

管理者権限を必要とするコマンドを実行する際は、`sudo` を使用していることを確認してください。

正しいコマンド:

```
sudo systemctl enable v2ray
```

このコマンドは、V2Ray サービスを有効にして、システムの起動時に自動的に開始されるように設定します。`systemctl enable` コマンドを使用することで、指定したサービス（この場合は `v2ray`）がシステムの起動時に自動的に開始されるようになります。

検証

V2Ray サービスを起動した後、正しく動作しているか確認します。

実行中のプロセスを確認する

```
ps aux | grep v2ray
```

このコマンドは、実行中のプロセスを表示し、その中から「v2ray」という文字列を含むプロセスを検索します。`ps aux` はシステム上のすべてのプロセスを表示し、`grep v2ray` はその出力から「v2ray」を含む行だけを抽出します。これにより、V2Ray 関連のプロセスが実行中かどうかを確認できます。

サンプル出力:

```
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
```

上記のコードブロックは、システム上で実行されているプロセスを表示する `ps` コマンドの出力例です。この出力は、`v2ray` という名前のプロセスが実行されていることを示しています。具体的には、`nobody` ユーザーとして実行されている `v2ray` プロセスと、`ubuntu` ユーザーが実行している `grep` コマンドが表示されています。`grep` コマンドは、`v2ray` という文字列を検索するために使用されています。

Telnet を使用して接続をテストする

```
telnet your_server_ip 1080
```

期待される動作:

- 接続が成功すると、V2Ray サービスからの応答が表示されます。
- Telnet を終了するには、`Ctrl + ]` を押してから `quit` と入力します。

結論

Ubuntu サーバーに V2Ray を設定するには、ソフトウェアのインストール、インバウンドとアウトバウンドの設定の構成、`systemctl` を使用したサービスの管理、および動作確認が含まれます。このガイドに従うことで、ネットワークのプライバシーを強化し、制限を効果的に回避する機能的な V2Ray のセットアップができるはずです。

何か問題が発生したり、質問がある場合は、お気軽に下記にコメントを残してください！

追加のヒント

- セキュリティ: V2Ray の UUID とパスワードは常に安全に保管してください。
- アップデート: 最新の機能とセキュリティパッチを活用するために、定期的に V2Ray を更新してください。
- 監視: `/var/log/v2ray/`にあるログを使用して、パフォーマンスを監視し、問題をトラブルシューティングしてください。

プロキシを楽しんでください！