


```
[Install]
```

```
WantedBy=multi-user.target
```

जानकारी: 02000 05.22.0 स्थापित है।

```
:
```

```
:
```

```
```bash
```

```
apt purge curl unzip
```

---

## कॉन्फिगरेशन

02000 कॉन्फिगरेशन (config.json)

यह 0000 फ़ाइल 02000 के लिए इनबाउंड और आउटबाउंड सेटिंग्स को परिभाषित करती है।

```
{
 "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"
}
}

```

मुख्य बिंदु: - इनबाउंड: आने वाले कनेक्शन के लिए प्रवेश बिंदुओं को परिभाषित करता है। यहां, इसे पोर्ट 1080 पर vmess प्रोटोकॉल का उपयोग करने के लिए सेट किया गया है। - आउटबाउंड: यह निर्दिष्ट करता है कि ट्रैफ़िक को कहां भेजा जाना चाहिए। freedom प्रोटोकॉल ट्रैफ़िक को बिना किसी प्रतिबंध के गुजरने की अनुमति देता है। - लॉगिंग: डिबगिंग के उद्देश्य से एक्सेस और त्रुटि जानकारी को लॉग करने के लिए कॉन्फ़िगर किया गया है। - सुरक्षा: बेहतर एन्क्रिप्शन के लिए security फ़ील्ड को aes-256-gcm पर सेट किया गया है।

## प्रॉक्सी कॉन्फिगरेशन (config.yaml)

यह config.yaml फ़ाइल प्रॉक्सी सेटिंग्स, log, और ट्रैफ़िक रूटिंग के लिए नियमों को कॉन्फिगर करती है।

```
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: "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: "Proxy"
 type: select
 proxies:
 - "My VMess Proxy"

```

नियम: - ००-००००,192.168.0.0/16,०००००० - ००-००००,10.0.0.0/8,०००००० - ००-००००,127.0.0.0/8,०००००० - ०००००,००,०००००० - ०००००,००००००

```

:
- : HTTP, SOCKS,
- DNS: IP DNS
- : `aes-128-gcm` VMess
- :
- : IP

: `cipher`, `config.json` `security`

```

---

## V2Ray

```
, `systemctl` V2Ray
```

### V2Ray

```
V2Ray :
```

```
```bash
```

```
sudo systemctl enable v2ray
```

❏❏❏❏ सेवा शुरू करें:

```
sudo systemctl start v2ray
```

(नोट: यह एक कमांड है जिसे टर्मिनल में चलाया जाता है। इसे हिंदी में अनुवादित करने की आवश्यकता नहीं है।)

अपेक्षित आउटपुट:

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

सेवा स्थिति सत्यापित करें:

```
sudo systemctl status v2ray
```

(यह कमांड ❏❏❏❏ सेवा की स्थिति की जांच करने के लिए है। इसे हिंदी में अनुवाद करने की आवश्यकता नहीं है क्योंकि यह एक टर्मिनल कमांड है और इसे वैसे ही रहना चाहिए।)

नमूना आउटपुट:

```
v2ray.service - V2Ray
      :      (/etc/systemd/system/v2ray.service;      :  )
      :      (      )    2024-04-27 12:55:00 UTC ; 1    30
PID: 14425 (v2ray)
      : 8 (    : 4915)
      : 36.7M
CGroup: /system.slice/v2ray.service
        14425 /usr/local/bin/v2ray run -config /usr/local/etc/v2ray/config.json
```

सामान्य समस्याएं और समस्या निवारण

❏❏❏❏ सक्षम करते समय प्रमाणीकरण विफलता

त्रुटि संदेश:

```
==== org.freedesktop.systemd1.manage-unit-files      ====
```

```
: Ubuntu (ubuntu)
```

```
      :
polkit-agent-helper-1: pam_authenticate      :
=====
      :
```

समाधान:

सुनिश्चित करें कि आप प्रशासनिक विशेषाधिकारों की आवश्यकता वाले कमांड को निष्पादित करने के लिए `sudo` का उपयोग कर रहे हैं।

सही कमांड:

```
sudo systemctl enable v2ray
```

(यह कमांड `v2ray` सेवा को सिस्टम स्टार्टअप पर स्वचालित रूप से शुरू करने के लिए सक्षम करती है।)

सत्यापन

`v2ray` सेवा शुरू करने के बाद, यह सुनिश्चित करें कि यह सही ढंग से चल रहा है।

चल रही प्रक्रियाओं की जांच करें

```
ps aux | grep v2ray
```

(यह कमांड सिस्टम में चल रहे `v2ray` प्रक्रियाओं को खोजने के लिए है। इसे हिंदी में अनुवाद करने की आवश्यकता नहीं है क्योंकि यह एक टर्मिनल कमांड है।)

नमूना आउटपुट:

```
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
```

`v2ray` का उपयोग करके कनेक्टिविटी का परीक्षण करें

```
telnet your_server_ip 1080
```

अपेक्षित व्यवहार:

- यदि कनेक्शन सफल होता है, तो आपको □2□□□ सेवा से एक प्रतिक्रिया दिखाई देगी।
 - □□□□□□ से बाहर निकलने के लिए, Ctrl +] दबाएं और फिर quit टाइप करें।
-

निष्कर्ष

□□□□□□ सर्वर पर □2□□□ सेटअप करने में सॉफ्टवेयर इंस्टॉल करना, इनबाउंड और आउटबाउंड सेटिंग्स कॉन्फ़िगर करना, systemctl के साथ सेवा प्रबंधित करना, और इसके संचालन को सत्यापित करना शामिल है। इस गाइड का पालन करके, आपके पास एक कार्यात्मक □2□□□ सेटअप होना चाहिए जो आपकी नेटवर्क गोपनीयता को बढ़ाता है और प्रतिबंधों को प्रभावी ढंग से दरकिनार करता है।

यदि आपको कोई समस्या आती है या कोई प्रश्न है, तो बेझिझक नीचे टिप्पणी करें!

अतिरिक्त सुझाव

- सुरक्षा: हमेशा सुनिश्चित करें कि आपका □2□□□ □□□□ और पासवर्ड सुरक्षित रखे गए हैं।
- अपडेट: नवीनतम सुविधाओं और सुरक्षा पैचों का लाभ उठाने के लिए □2□□□ को नियमित रूप से अपडेट करें।
- मॉनिटरिंग: प्रदर्शन की निगरानी और समस्याओं का निवारण करने के लिए /var/log/v2ray/ पर स्थित लॉग्स का उपयोग करें।

खुश प्रॉक्सीइंग!