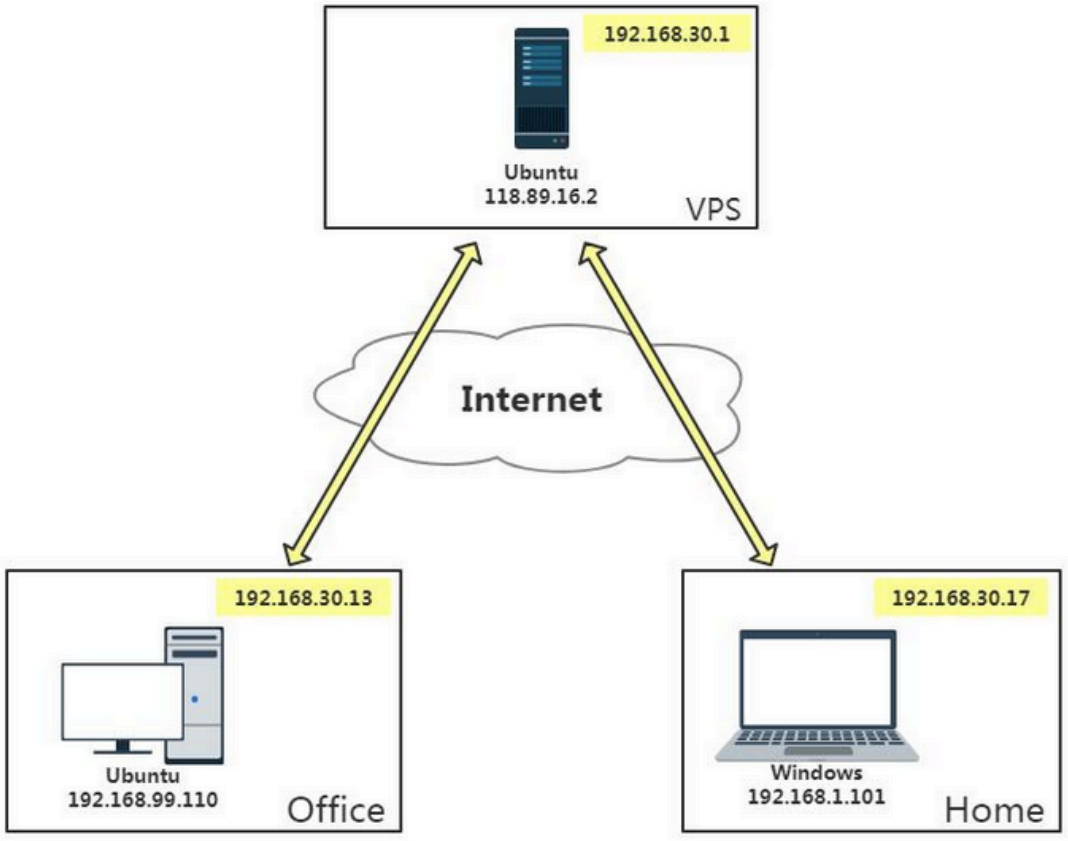
CentOS 7.9 部署 ov ， 助力居家办公

1、自动部署服务，并创建一个demo账号，拨通vpn后访问 `http://10.10.10.1` 即可以查看所有登录的用户，以及分配的IP地址，因为开启了 client-to-client 功能，所以这个客户端直接可以直接访问。实现下图效果：

连接成功后的网络拓扑如下：



客户端通过 VPN 隧道连接到了服务器的虚拟 HUB 上，共同组成了一个 `192.168.30.0/24` 的局域网，客户端直接可以想局域网内一样相互访问，在家里电脑上 ping 办公室内的电脑：

一、服务部署

部署脚本

```
#!/bin/bash

# 设置公网IP和OpenVPN服务端口（必须修改为你的云服务器公网IP）
IP=117.117.117.119            # 公网IP地址（需替换为实际地址）
PORT=19397                    # OpenVPN服务监听端口（UDP协议）

# 配置阿里云 epel 源（CentOS扩展软件源）
curl -o /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-7.repo

# 安装基础软件：
# openvpn - VPN服务主体
# easy-rsa - 证书生成工具
# lrzsz - 文件传输工具（用于sz命令）
# httpd - Web服务（用于显示客户端状态）
yum install -y openvpn easy-rsa lrzsz httpd

# 复制easy-rsa工具到OpenVPN配置目录（版本号自动匹配）
cp -a /usr/share/easy-rsa/[[:digit:]]*.[[:digit:]]*.[[:digit:]]* /etc/openvpn/easy-rsa

# 进入工作目录
cd /etc/openvpn/easy-rsa

# 初始化PKI目录结构（生成pki子目录）
./easyrsa init-pki

# 创建根证书机构（CA），nopass参数表示无密码保护
./easyrsa build-ca nopass

# 生成服务器端证书和私钥（名称为server）
./easyrsa build-server-full server nopass

# 生成迪菲-赫尔曼密钥交换文件（增强安全性）
./easyrsa gen-dh

# 生成证书吊销列表（CRL）
./easyrsa gen-crl

# 将服务器所需证书文件集中存储
cp pki/ca.crt /etc/openvpn/server/          # CA证书
cp pki/dh.pem /etc/openvpn/server/          # DH密钥
cp pki/issued/server.crt /etc/openvpn/server/  # 服务器证书
cp pki/private/server.key /etc/openvpn/server/ # 服务器私钥

# 生成OpenVPN服务端配置文件
echo 'local 0.0.0.0             # 监听所有本地地址
port '$PORT'                   # 服务监听端口
proto udp                     # 使用UDP协议
dev tun                       # 使用路由模式
ca /etc/openvpn/server/ca.crt  # CA证书路径
```

```
cert /etc/openvpn/server/server.crt  # 服务器证书路径
key /etc/openvpn/server/server.key   # 服务器私钥路径
dh /etc/openvpn/server/dh.pem        # DH文件路径
server 10.10.10.0 255.255.255.0  # 分配给客户端的虚拟IP段
client-to-client            # 允许客户端间直接通信
duplicate-cn                # 允许一个证书多次连接
keepalive 10 120            # 心跳检测
cipher AES-256-CBC          # 加密算法
max-clients 100             # 最大客户端数
persist-key                 # 持久化密钥
persist-tun                 # 持久化隧道
status /var/www/html/index.txt  # 状态文件（供web显示）
log-append /var/log/openvpn.log # 日志文件
verb 3                      # 日志详细级别
mute 20                     # 限制重复日志数量
explicit-exit-notify 1      # UDP连接关闭时通知客户端
crl-verify /etc/openvpn/easy-rsa/pki/crl.pem  # 证书吊销检查
' > /etc/openvpn/service.conf

# 设置服务开机自启并立即启动
systemctl enable openvpn@service --now

# 生成客户端证书（名称为demo）
./easyrsa build-client-full demo nopass

# 创建客户端配置文件模板
echo 'client                    # 客户端模式
dev tun                  # 使用路由模式
proto udp                # 匹配服务端协议
remote '$IP' '$PORT'     # 服务端公网IP和端口
nobind                   # 不绑定本地端口
persist-key              # 持久化密钥
persist-tun              # 持久化隧道
remote-cert-tls server   # 校验服务端证书
cipher AES-256-CBC       # 加密算法匹配服务端
verb 3                   # 日志级别
' > /etc/openvpn/client/demo.ovpn

# 将CA证书嵌入客户端配置文件
echo '<ca>' >> /etc/openvpn/client/demo.ovpn
cat /etc/openvpn/easy-rsa/pki/ca.crt >> /etc/openvpn/client/demo.ovpn
echo '</ca>' >> /etc/openvpn/client/demo.ovpn

# 将客户端证书嵌入配置文件
echo '<cert>' >> /etc/openvpn/client/demo.ovpn
cat /etc/openvpn/easy-rsa/pki/issued/demo.crt >> /etc/openvpn/client/demo.ovpn
echo '</cert>' >> /etc/openvpn/client/demo.ovpn

# 将客户端私钥嵌入配置文件
echo '<key>' >> /etc/openvpn/client/demo.ovpn
cat /etc/openvpn/easy-rsa/pki/private/demo.key >> /etc/openvpn/client/demo.ovpn
echo '</key>' >> /etc/openvpn/client/demo.ovpn

```

```
# 配置HTTP服务显示客户端连接状态
chmod +r /var/www/html/index.txt       # 允许访问状态文件
sed -i 's/index.html/index.txt/' /etc/httpd/conf/httpd.conf  # 修改默认页面
echo 'ServerName 10.10.10.1:80' >> /etc/httpd/conf/httpd.conf  # 解决域名警告
systemctl enable httpd && systemctl start httpd  # 启动Web服务

# 使用sz命令发送客户端配置到本地（需XShell等终端支持）
sz /etc/openvpn/client/demo.ovpn
```

二、服务维护

1）一键创建用户

使用方法 `sh create.sh usera`

```
#!/bin/bash

# 设置OpenVPN服务端的公网IP和端口
IP=117.117.117.119     # 服务端公网IP（必须修改为实际IP）
PORT=11947              # OpenVPN服务端口（需与主配置文件一致）
USER=$1                # 从命令行参数获取用户名

# 切换到证书管理目录
cd /etc/openvpn/easy-rsa

# 生成客户端证书和密钥（无密码保护） 注意：nopass参数表示私钥不加密，生产环境建议移除该参数
./easyrsa build-client-full $USER nopass

# 创建客户端配置文件模板
echo 'client           # 客户端模式
dev tun            # 使用路由模式
proto udp          # 与服务端协议一致
remote '$IP' '$PORT'   # 服务端公网地址和端口
nobind             # 不绑定本地端口
persist-key        # 持久化密钥文件
persist-tun        # 持久化隧道接口
remote-cert-tls server  # 强制验证服务端证书
cipher AES-256-CBC # 加密算法需与服务端一致
verb 3             # 日志详细级别
' > /etc/openvpn/client/$USER.ovpn

# 将CA证书嵌入配置文件
echo '<ca>' >> /etc/openvpn/client/$USER.ovpn
cat /etc/openvpn/easy-rsa/pki/ca.crt >> /etc/openvpn/client/$USER.ovpn
echo '</ca>' >> /etc/openvpn/client/$USER.ovpn

# 将用户证书嵌入配置文件
echo '<cert>' >> /etc/openvpn/client/$USER.ovpn
cat /etc/openvpn/easy-rsa/pki/issued/$USER.crt >> /etc/openvpn/client/$USER.ovpn
echo '</cert>' >> /etc/openvpn/client/$USER.ovpn

# 将用户私钥嵌入配置文件
```

```
echo '<key>' >> /etc/openvpn/client/$USER.ovpn
cat /etc/openvpn/easy-rsa/pki/private/$USER.key >> /etc/openvpn/client/$USER.ovpn
echo '</key>' >> /etc/openvpn/client/$USER.ovpn

# 使用sz命令发送配置文件（需要ZModem协议支持）
sz /etc/openvpn/client/$USER.ovpn
```

2）一键删除用户

吊销用户证书,使用方法 `sh delete.sh useraaa`

```
#!/bin/bash

USER=$1  # 从命令行参数获取要吊销的用户名

# 切换到证书管理目录
cd /etc/openvpn/easy-rsa

# 吊销指定用户的证书，注意：需要输入"yes"确认操作（非交互式自动确认）
echo "yes" | ./easyrsa revoke $USER

# 重新生成证书吊销列表（CRL）,该文件被OpenVPN服务用来拒绝已吊销证书的连接
./easyrsa gen-crl

# 重要：不需要重启服务，OpenVPN会自动重新加载CRL,可通过以下命令验证CRL加载：
# tail -f /var/log/openvpn.log | grep CRL
```

三、固定用户分配的IP

1）修改配置文件，重启服务

```
# 持久化IP分配记录（关键配置）
cat "ifconfig-pool-persist /etc/openvpn/server/ipp.txt" >>/etc/openvpn/service.conf

# 重启服务，使得配置生效
systemctl restart openvpn@service
```

2）自动维护 hosts文件

server上访问客户端服务的时候直接访问用户名就可以了，不用查ip，再访问ip

功能：自动更新hosts文件，将OpenVPN客户端用户名与虚拟IP绑定

```
vim /opt/vpn_update_hosts.sh

#!/bin/bash

# 保留系统基础hosts配置
echo '127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
' > /etc/hosts

```

```
# 从持久化IP池文件提取用户与虚拟IP（格式：用户名,10.10.10.x） 注意：ifconfig-pool-persist生成的ipp.txt每行格式为 "用户名,IP"
cat /etc/openvpn/server/ipp.txt | grep '^[a-zA-Z]' | awk -F ',' '{print $2" "$1}' >> /etc/hosts

# 可选：同时记录客户端公网IP（需OpenVPN配置status日志）
# cat /var/www/html/index.txt | grep 10.10.10 | awk -F '[:,]' '{print $1,$2}' >> /etc/hosts
```

3）添加定时任务，自动执行脚本

```
# 赋予执行权限
chmod +x /opt/vpn_update_hosts.sh

# 添加crontab任务（root用户执行）
(crontab -l 2>/dev/null; echo "*/5 * * * * /bin/bash /opt/vpn_update_hosts.sh") | crontab -

# 查看任务列表
crontab -l
```

FAQ:

1) 日志监控

实时查看连接日志：

```
tail -f /var/log/openvpn.log
```

监控在线用户：

```
cat /var/www/html/index.txt
```

2）网络配置

- 云服务器安全组需放行UDP端口（示例中为11947）
- 如修改端口，需同步调整两个脚本中的 `PORT` 变量

3）证书问题

```
# 检查证书有效期
openssl x509 -in /etc/openvpn/server/server.crt -noout -dates
```

4）路由配置

```
# 查看iptables规则
iptables -L -n -v

# 若需放通VPN网段
iptables -A INPUT -s 10.10.10.0/24 -j ACCEPT
```