Ubuntu 24.04 + OpenVPN + AD (LDAP/RADIUS) ??????

? Ubuntu 24.04 + OpenVPN + AD ????? ????

??????

- **Ubuntu 24.04 LTS** 服务器一台（公网可访问，或 NAT 转发端口）。
- **Windows AD** 域控制器（域名如：`shuncom.local`，DC IP：192.168.1.10）。
- 客户端：Windows 10/11，macOS，Linux，移动端。

???? OpenVPN ? Easy-RSA

```
sudo apt update
sudo apt install openvpn easy-rsa -y
```

??????

1. 创建证书目录：

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
```

2. 初始化：

```
./easyrsa init-pki
./easyrsa build-ca
```

3. 生成服务器证书:

```
./easyrsa build-server-full server nopass
```

4. 生成客户端证书:

```
./easyrsa build-client-full user01 nopass
```

5. 拷贝到 OpenVPN 配置目录:

```
sudo cp pki/ca.crt pki/private/server.key pki/issued/server.crt /etc/openvpn/
```

???? OpenVPN ???

创建配置文件 `/etc/openvpn/server.conf`:

```
port 1194
proto udp
dev tun

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh none
auth SHA256
tls-crypt /etc/openvpn/tls-crypt.key

server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt

push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 192.168.1.10"   # AD DNS

keepalive 10 120
cipher AES-256-GCM
persist-key
```

```
persist-tun
user nobody
group nogroup
verb 3

# 启用 LDAP 插件
plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so openvpn
client-cert-not-required
username-as-common-name
```

???? PAM ? LDAP (AD)

安装 LDAP 认证模块:

```
sudo apt install libpam-ldapd nslcd -y
```

配置 `/etc/nslcd.conf`:

```
uri ldap://192.168.1.10/
base dc=shuncom,dc=local
binddn cn=vpnbind,ou=ServiceAccounts,dc=shuncom,dc=local
bindpw YourPassword
scope sub
filter passwd (sAMAccountName=%u)
```

> “□□ 建议在 AD 中创建一个只读账号 `vpnbind` 专门用于 LDAP 查询。

修改 PAM 配置 `/etc/pam.d/openvpn`:

```
auth    required        pam_unix.so
auth    sufficient      pam_ldap.so use_first_pass
account sufficient      pam_ldap.so
```

??????? OpenVPN

```
sudo systemctl enable openvpn@server
sudo systemctl start openvpn@server
sudo systemctl status openvpn@server
```

????? & NAT

```
sudo ufw allow 1194/udp
sudo ufw allow OpenSSH
```

启用 NAT 转发:

编辑 `/etc/sysctl.conf`, 取消注释:

```
net.ipv4.ip_forward=1
```

生效:

```
sudo sysctl -p
```

配置 NAT:

```
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

???????

生成客户端配置 `user01.ovpn`:

```
client
dev tun
proto udp
remote vpn.shuncom.org 1194
resolv-retry infinite
nobind
persist-key
persist-tun

remote-cert-tls server
auth-user-pass
```

```
cipher AES-256-GCM
verb 3
```

用户连接时输入 **AD** 域账号 **+**密码 即可。

????

在 OpenVPN 服务端日志 `/var/log/syslog` 或 `/var/log/openvpn.log` 中可以看到:

```
PAM_AUTH: user 'user01' authenticated via LDAP
```

? ????

1. 仅允许 VPN 用户组: 在 AD 中新建组 `VPN-Users`, 在 `/etc/nslcd.conf` 里加上 `filter` 限制。
2. 建议启用 **MFA** (可配合 FreeRADIUS + Google Authenticator) 。
3. 如果性能要求高, 可以考虑 **WireGuard + AD 集成**。

要不要我帮你写一份 限制只有 **AD** 中 **“VPN-Users”** 组成员能登录 **OpenVPN** 的配置示例 ? 这样就能精确控制谁能连 VPN。

Revision #1
Created 26 September 2025 08:47:01 by Admin
Updated 26 October 2025 09:58:33 by Admin