

OpenVPN + AD



1. 安装 Windows Server 2025 + AD 域控制器
 2. 安装 OpenVPN 服务器
 3. 配置 OpenVPN 服务器
 4. 配置 Windows Server 2025 + AD 域控制器
 5. 配置 Windows Server 2025 + AD 域控制器
 6. 配置 Windows Server 2025 + AD 域控制器
 7. 配置 Windows Server 2025 + AD 域控制器
 8. 配置 Windows Server 2025 + AD 域控制器
 9. 配置 Windows Server 2025 + AD 域控制器
 10. 配置 Windows Server 2025 + AD 域控制器

安装 OpenVPN + AD



1. 安装 Windows Server 2025 域控制器
 - 安装 Windows Server 2025 域控制器
 - 安装 Windows Server 2025 域控制器
2. 安装 AD 域控制器
 - 安装 AD 域控制器
3. 配置 OpenVPN 服务器
 - 配置 OpenVPN 服务器
4. 配置 IP 地址 NAT 规则

安装 OpenVPN Server

1. 安装 OpenVPN 服务器
 - <https://openvpn.net/community-downloads/>
2. 配置 OpenVPN 服务器
 - EasyRSA 生成密钥
 - OpenVPN Service 配置
3. 配置 Windows 防火墙
 - UDP 1194 端口开放

- 00000000



CA Server Client



C:\Program Files\OpenVPN\easy-rsa 0000

```
# 0000 CA
EasyRSA-Start.bat
./easyrsa init-pki
./easyrsa build-ca

# 00000000
./easyrsa build-server-full server nopass

# 000000000000 user01
./easyrsa build-client-full user01 nopass
```

0000 pki 00000000 C:\Program Files\OpenVPN\config 0000



OpenVPN 0000

C:\Program Files\OpenVPN\config\server.ovpn 0000

```
port 1194
proto udp
dev tun

ca ca.crt
cert server.crt
key server.key
dh dh.pem

server 10.8.0.0 255.255.255.0
```

```
ifconfig-pool-persist ipp.txt
```

```
push "redirect-gateway def1"
```

```
push "dhcp-option DNS 192.168.1.10" # 服务器/DNS 服务器 IP
```

```
keepalive 10 120
```

```
cipher AES-256-GCM
```

```
auth SHA256
```

```
persist-key
```

```
persist-tun
```

```
verb 3
```

```
# 启用 AD 认证
```

```
plugin "C:\\Program Files\\OpenVPN\\lib\\openvpn-auth-ldap.dll" "C:\\Program  
Files\\OpenVPN\\config\\auth-ldap.conf"
```



AD 认证



☐ C:\Program Files\OpenVPN\config\auth-ldap.conf ☐

<LDAP>

URL ldap://192.168.1.10:389

BindDN CN=vpnbind,OU=ServiceAccounts,DC=shuncom,DC=local

Password YourBindPassword

Timeout 15

FollowReferrals yes

</LDAP>

<Authorization>

BaseDN "OU=Users,DC=shuncom,DC=local"

SearchFilter "(sAMAccountName=%u)"

RequireGroup false

</Authorization>

☐ ☐

• BindDN

vpnbind

• BaseDN

OU



OpenVPN

services.msc

OpenVPNService →

net start openvpnservice



Windows/Linux/Mac

user01.ovpn

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

ca ca.crt
cert user01.crt
key user01.key

auth-user-pass
cipher AES-256-GCM
auth SHA256
verb 3
```



```
"C:\Program Files\OpenVPN\bin\openvpn.exe" --show-status
```

□□□□ C:\Program Files\OpenVPN\log\server.log □



```
LDAP: User user01 authenticated.
```



- 1. □ **MFA**□□□ AD FS + Azure MFA □ Duo□
- 2. □□ VPN □□□□□ → □ `auth-ldap.conf` □□ `RequireGroup true` □
- 3. □□□ **IKEv2** □ **WireGuard** □□ OpenVPN□□□□□

□□□□□□□ **auth-ldap.conf** □□□□□ **AD** □□□□ **VPN** □□□□
□□□□□□□□□ AD □□□□□□ VPN□