

首先安装OpenVPN服务

首先安装OpenVPN服务

```
root@Z2vC5kb6fq9q7F5uI2:~# cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04 LTS"
NAME=Ubuntu
VERSION=22.04 LTS (Jammy Jellyfish)
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-conditions"
VERSION_ID="22.04"
UBUNTU_CODENAME=jammy

root@Z2vC5kb6fq9q7F5uI2:~# apt-get -y install opel-release
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
opel is already the newest version (2.6.9-lubuntu1).
opel is already the newest version (3.0.13-nubuntu1.4).
openssl set to manually installed.
Suggested packages:
libssl-dev
The following NEW packages will be installed:
libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 3 disk not upgraded.
Need to get 2,488 kB of archives.
After this operation, 13.3 MB of additional disk space will be used.
Get http://mirrors.cloud.aliyuncs.com/ubuntu noble-updates/main amd64 libssl-dev amd64 3.0.13-nubuntu1.4 [2,488 kB]
Fetched 2,488 kB in 0s (4,953 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 94335 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.0.13-nubuntu1.4_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-nubuntu1.4) ...
Setting up libssl-dev:amd64 (3.0.13-nubuntu1.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

root@Z2vC5kb6fq9q7F5uI2:~# openssl -version
OpenSSL 2.6.9 x86_64 pc.linux.gnu fips (OpenSSL) [LZO] [LZ4] [EPOLL] [PROCRNG] [MMIO/PKTRNG] [AEAD] [XCR0]
library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 1.0
cc0 version: N/A
Originally developed by James Yonan
Copyright (C) 2002-2023 OpenVPN Inc. 
Compile time defines: enable_aead yesno enable_crypto off enable_dco yesno enable_dco_args yesno enable_debugger yesno enable_dependency_tracking no enable_dlopen self unknown enable_dlopen_self static no
enable_fips install needed yes enable_fragment yes enable_iproute no enable_libtcl lock yes enable_lz4 yes enable_lz4osx enable_mbedtls yesno enable_management yesno enable_option checking no enable_pam dlopen no enable_pedantic no enable_posix_compat yesno enable_plugins yesno enable_port_shares yesno enable_selinux no enable_shared yesno enable_shared_with_static_runtimes no enable_silent rules no enable_snmalloc no enable_static yesno enable_strict no enablestrict options no enable_systemd yesno enable_unit_tests no enable_warning no enable_win32_dll yes enable_wolfssl options_hyes enable_x509 alt_username yesno with aix soname aix with crypto library openssl with gnu_ld yesno with non_check
enable_engine auto with systemcrypto
root@Z2vC5kb6fq9q7F5uI2:~#
```

[illegible]


```
1.root@iZ2vc5jkbvf6r9q7f5r1rLZ: ~$ cd /etc/openvpn/easy-rsa/
2.root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ./easyrsa build-server-full yukikaze nopass
CA creation complete. Your new CA certificate is at:
* /etc/openvpn/easy-rsa/pki/ca.crt

root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ls
easyrsa  openssl-easyrsa.cnf  pki  vars  vars.example  e88f-types
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ./easyrsa build-server-full yukikaze nopass
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
.....
-----
Notice
-----
Private-Key and Public-Certificate-Request files created.
Your files are:
* Req: /etc/openvpn/easy-rsa/pki/reqs/yukikaze.req
* Key: /etc/openvpn/easy-rsa/pki/private/yukikaze.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for 825 days:

subject=
commonName = yukikaze

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature OK
The Subject's Distinguished Name is as follows
commonName : c=CN, o=132'yukikaze'
Certificate is to be certified until Jan  9 14:37:09 2027 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/yukikaze.crt
```

```
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ls pki/issued/
yukikaze.crt
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ls pki/private/
ca.key  yukikaze.key
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa#
```

客户端证书

```
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ./easyrsa build-client-full kangzihao nopass
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
.....
-----
Notice
-----
Private-Key and Public-Certificate-Request files created.
Your files are:
* Req: /etc/openvpn/easy-rsa/pki/reqs/kangzihao.req
* Key: /etc/openvpn/easy-rsa/pki/private/kangzihao.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for 825 days:

subject=
commonName = kangzihao

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature OK
The Subject's Distinguished Name is as follows
commonName : c=CN, o=132'kangzihao'
Certificate is to be certified until Jan  9 14:40:05 2027 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/kangzihao.crt

Notice
-----
Inline file created:
* /etc/openvpn/easy-rsa/pki/inline/kangzihao.inline

root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa#
```

```
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ls pki/issued/
kangzihao.crt  yukikaze.crt
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa# ls pki/private/
ca.key  kangzihao.key  yukikaze.key
root@iZ2vc5jkbvf6r9q7f5r1rLZ:/etc/openvpn/easy-rsa#
```

生成DH文件

```
root@iZ2vc5jkbvf6r9q7f5rirlZ:/etc/openssl/easy-rsa# ls pki/dh.pem -l
-rw----- 1 root root 424 Oct  6 22:42 pki/dh.pem
root@iZ2vc5jkbvf6r9q7f5rirlZ:/etc/openssl/easy-rsa#
```

```

C:\Users\root@47.109.199.22> cd /d %cd%
C:\Users\root@47.109.199.22> cd /d C:\Program Files\OpenVPN\bin
C:\Program Files\OpenVPN\bin> copy ..\..\openvpn.conf .
C:\Program Files\OpenVPN\bin> type openvpn.conf
# This file is for the server side
# of a many-clients (-> one-server
# OpenVPN configuration.
#
# OpenVPN also supports
# single-machine -> single-machine
# configurations (See the examples page
# on the web site for more info).
#
# This config should work on Windows
# or Linux/OSX systems. Remember on
# Windows to quote pathnames and use
# double backslashes, e.g.:
# "C:\\Program Files\\OpenVPN\\config\\foo.key"
#
# Comments are preceded with '#' or ';'
#####
# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d
#
# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one. You will need to
# open up this port on your firewall.
port 1194
#
# TCP or UDP server?
proto tcp
;proto udp
#
# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap" if you are ethernet bridging
# and have precreated a tap's virtual interface
# and bridged it with your ethernet interface.
#
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap
dev tun
#
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one. On XP SP2 or higher,
# --INSERT--

```

日志显示

日志显示

大概就是这样，但是现在报出来就是ECS连不上[UNKNOWN ERROR]，基本的设置应该是没问题，服务器的我是弄好了的

