Windows版OpenVPN安装、配置教程

原因：外网不能访问学校内网

**OpenVPN安装**

在Windows上安装OpenVPN是比较简单的，因为OpenVPN官方直接为我们提供了可执行的安装程序(.exe)，不管是在OpenVPN服务器端还是在客户端上，安装步骤都没有什么差别。

在这里，我们以目前最新的openvpn-install-2.3.4-I001-i686.exe来介绍如何在Windows上安装OpenVPN。

下载地址：<http://www.softown.cn/soft/openvpn/windows>

经测试64位系统也最好安装32位的版本

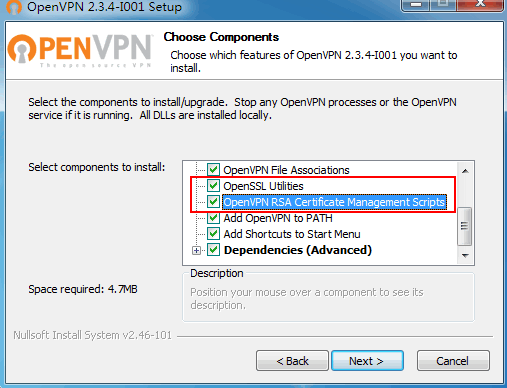
注意：101.201.81.34 安装在E盘 师姐电脑安装在F盘

下面的截图来来自于网上，有特殊说明我会标出

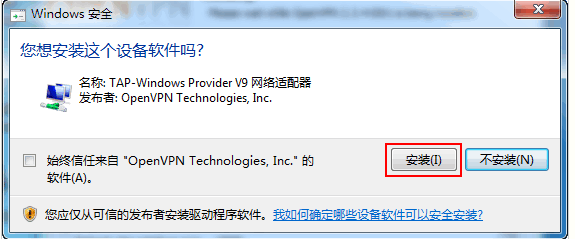
首先，直接双击该安装文件。看到下面这个界面就应该不会感到陌生了——"还是熟悉的配方，还是熟悉的味道"，我们也就不再一步步赘述安装步骤了，只是对某些关键步骤进行简要说明。



如下图所示，在选择安装哪些OpenVPN组件的配置界面中，如果你的OpenVPN是2.3及以上版本，请确保勾选下图所示的两个组件选项(该组件在OpenVPN 2.2中已默认选中，主要用于生成加密证书、密钥等)。



此外，在安装OpenVPN的过程中，系统会提示类似如下信息。这里安装的其实就是OpenVPN将要使用到的虚拟网卡，请点击【安装】按钮以允许安装。



**OpenVPN创建证书和密钥**

在OpenVPN运行原理一文中我们已经提到，OpenVPN除了安装虚拟网卡来创建虚拟专用网络外，还要做的就是使用SSL协议以及相应的用户密码、证书密钥等手段进行数据加密、身份验证等。

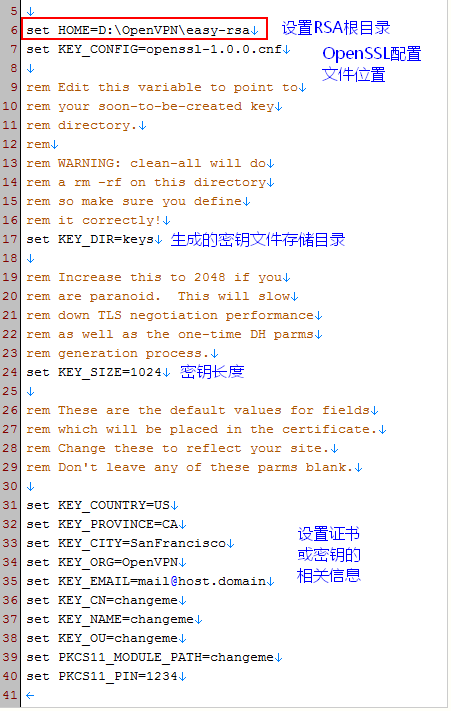
因此，在安装完OpenVPN后，我们就需要生成一些证书给服务器以及客户度使用。当然，我们还需要给服务器和客户端创建一个配置文件，否则的话，我们无法对服务器和客户端进行细粒度的控制。更何况，使用OpenVPN的用户如此之多，你的客户端和服务器怎么才能知道哪些是它的"同伙"的呢。

首先，我们需要在OpenVPN服务器端创建证书和密钥(服务器端和客户端使用的证书和密钥，都由服务器端负责创建)。

1、使用文本编辑器打开OpenVPN安装目录/easy-rsa/vars.bat.sample文件(这实际上是一个批处理文件的模板，用于设置初始化的用户变量)。

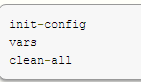
如下图所示，我们只需要将红色矩形框中的HOME变量值改为文件夹easy-rsa的所在路径即可（注意服务端、客户端路径都必须修改）。至于其他变量，你可以不作修改，也可以根据个人需要，按照我们给出的蓝色文字提示进行修改。

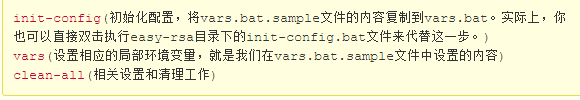
建议更改图中31~35行内容处的变量值，因为后面每次生成证书都需要输入相关信息，设置默认值可以避免重复输入。（我没有修改，后面每次自己输入的：但修改更好）



**初始化命令行**

接着，我们打开命令提示符窗口，并转到easy-rsa目录，然后依次执行如下命令完成初始化工作：





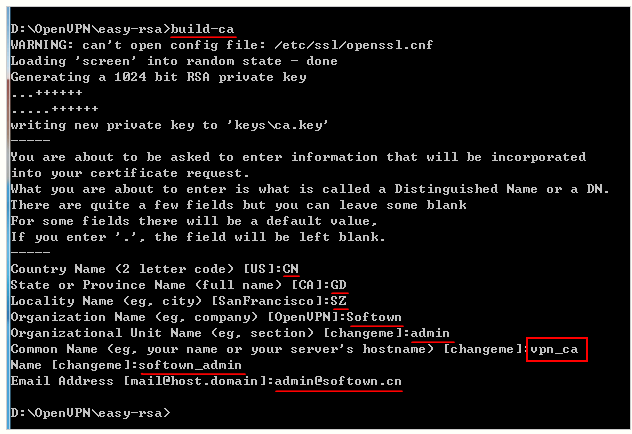


第一次执行clean-all时，提示"系统找不到指定的文件"是正常的，不用管它。该命令会删除掉之前生成的所有证书和密钥文件，以避免与之后全新生成的证书和密钥发生冲突。

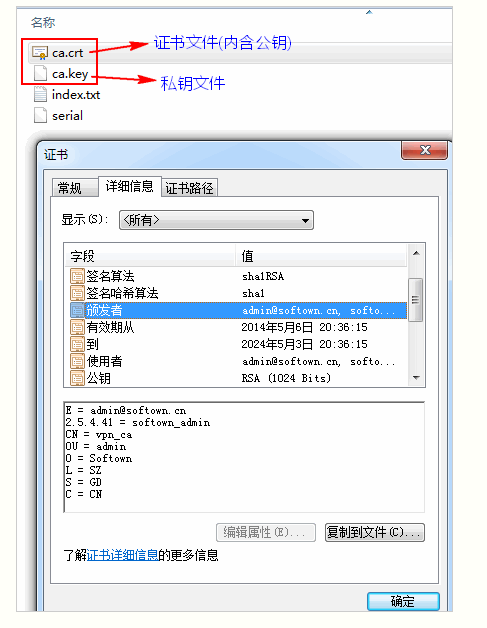
**创建CA证书**

就在上述命令提示符窗口中，我们继续执行命令build-ca来生成CA根证书密钥对。

如下图所示，除了build-ca命令外，其他输入主要用于设置根证书的签名信息，包括国家、省、市、组织名称、单位名称、通用名、名称、邮箱地址等，请根据个人需要自行输入。输入框前面"[]"中的内容表示默认值，如果你不输入、直接按回车，则表示使用默认值；如果你输入"."则表示该字段信息留空。其中Common Name(通用名称)比较重要，相当于我们常说的"账号"(此处设为vpn\_ca)。

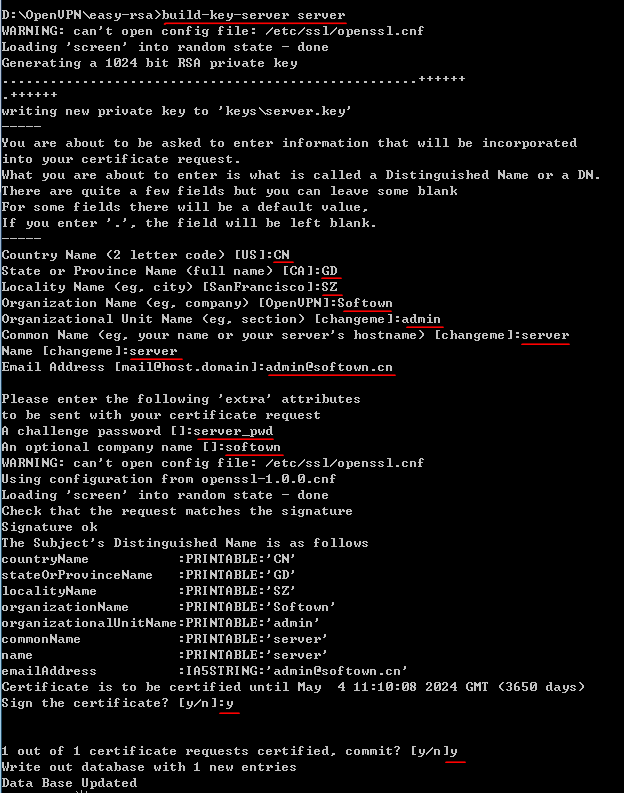


此时，我们就可以在证书存放目录中看到生成的CA证书和私钥文件了。双击该证书，我们还可以看到刚才输入的相关信息。



#### 创建服务器端证书

接着，我们使用命令build-key-server server来创建服务器端证书和私钥。整个创建过程与前面创建CA根证书的流程比较类似，我们只需要注意Comman Name的参数值为"server"并随后设置相应的密码(这里设为"server\_pwd"，一般不会用到密码（我设置为zhonglan）)，最后输入两次"y"进行确认即可。



#### 创建客户端证书

服务器端证书创建完毕后，我们就可以为所有的客户端分别创建证书了。创建命令为build-key clientName，例如build-key client1、build-key client2。

创建客户端证书的流程和创建服务器端证书的流程完全一致，只需要注意Common Name字段即可(该字段值我设为client,密码设为zhonglan2)，在这里就不再赘述了。

#### 创建迪菲·赫尔曼密钥

此外，我们还需要为OpenVPN的服务器端创建迪菲·赫尔曼交换密钥，命令为build-dh。迪菲·赫尔曼交换密钥是一种安全协议，用以对数据进行加密。

#### 创建迪菲·赫尔曼密钥开启tls-auth(可选)

这一步是可选操作。OpenVPN提供tls-auth功能，可以防御DoS、UDP淹没等恶意攻击。执行命令openvpn --genkey --secret keys/ta.key即可生成开启tls-auth所需的密钥文件ta.key。如果你不需要，可以忽略此步骤。

#### 开启tls-auth

到这里我们的证书和密钥的创建操作就基本上完成了，如果你以后还想要创建新的客户端，只需要先执行vars命令，再执行build-key clientName命令即可(每次打开新的命令提示符窗口，都必须先执行vars命令，才能执行其他命令)。

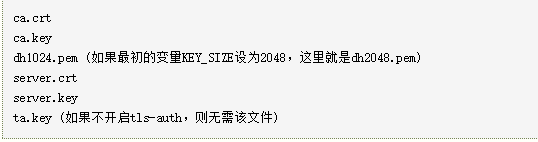
在这里，我们打开easy-rsa目录下的keys文件夹，看看我们都创建了哪些证书和密钥。

#### 创建的证书和密钥一览

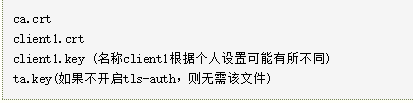
**OpenVPN配置**

下面，我们就开始进行OpenVPN的相关配置工作。现在，我们从easy-rsa/keys目录中拷贝出服务器端和客户端所需的文件，分别将其放在自己的OpenVPN安装路径/config目录中。

其中，服务器端需要用到的文件有：



客户端client1需要用到的文件有：



当然，我们还需要在config目录中各自放置一个配置文件，服务器端的配置文件名为server.ovpn，客户端的配置文件为client.ovpn。

这两个配置文件该如何编写呢？OpenVPN已经在sample-config目录中为我们提供了相关的示例文件server.ovpn和client.ovpn，并且配置文件中的每个配置选项均有详细的英文说明(配置文件中"#"或";"开头的均为注释内容)

在这里，我们先给出server.ovpn的详细配置，并注明每项配置的作用。

local 101.201.81.34    #指定监听的本机IP(因为有些计算机具备多个IP地址)，该命令是可选的，默认监听所有IP地址。  
port 1194             #指定监听的本机端口号  
proto udp             #指定采用的传输协议，可以选择tcp或udp  
dev tun               #指定创建的通信隧道类型，可选tun或tap  
ca ca.crt             #指定CA证书的文件路径  
cert server.crt       #指定服务器端的证书文件路径  
key server.key    #指定服务器端的私钥文件路径  
dh dh1024.pem         #指定迪菲赫尔曼参数的文件路径  
server 10.8.0.0 255.255.255.0   #指定虚拟局域网占用的IP地址段和子网掩码，此处配置的服务器自身占用10.0.0.1。  
ifconfig-pool-persist ipp.txt   #服务器自动给客户端分配IP后，客户端下次连接时，仍然采用上次的IP地址(第一次分配的IP保存在ipp.txt中，下一次分配其中保存的IP)。  
tls-auth ta.key 0     #开启TLS-auth，使用ta.key防御攻击。服务器端的第二个参数值为0，客户端的为1。  
keepalive 10 120      #每10秒ping一次，连接超时时间设为120秒。  
comp-lzo              #开启VPN连接压缩，如果服务器端开启，客户端也必须开启  
client-to-client      #允许客户端与客户端相连接，默认情况下客户端只能与服务器相连接  
persist-key  
persist-tun           #持久化选项可以尽量避免访问在重启时由于用户权限降低而无法访问的某些资源。  
status openvpn-status.log    #指定记录OpenVPN状态的日志文件路径  
verb 3                #指定日志文件的记录详细级别，可选0-9，等级越高日志内容越详细

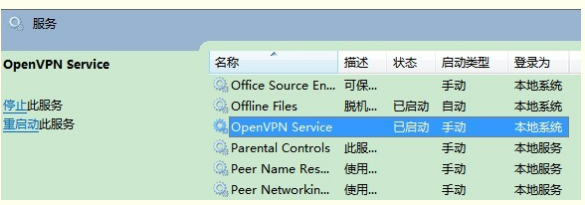
接着是client.ovpn

client         #指定当前VPN是客户端  
dev tun        #必须与服务器端的保持一致  
proto udp      #必须与服务器端的保持一致  
remote 101.201.81.34 1194      #指定连接的远程服务器的实际IP地址和端口号  
resolv-retry infinite    #断线自动重新连接，在网络不稳定的情况下(例如：笔记本电脑无线网络)非常有用。  
nobind         #不绑定特定的本地端口号  
persist-key  
persist-tun  
ca ca.crt      #指定CA证书的文件路径  
cert client1.crt       #指定当前客户端的证书文件路径  
key client1.key    #指定当前客户端的私钥文件路径  
ns-cert-type server      #指定采用服务器校验方式  
tls-auth ta.key 1     #如果服务器设置了防御DoS等攻击的ta.key，则必须每个客户端开启；如果未设置，则注释掉这一行；  
comp-lzo              #与服务器保持一致  
verb 3                #指定日志文件的记录详细级别，可选0-9，等级越高日志内容越详细

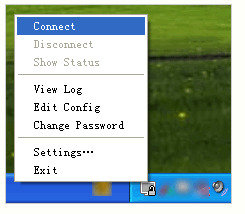
实际上，将两个模板文件中与IP地址有关的配置修改一下，就可以直接拿来使用。  
关于OpenVPN配置文件的更多信息请参考[server.ovpn配置详解](http://www.softown.cn/post/137.html" \t "_blank)和[client.ovpn配置详解](http://www.softown.cn/post/138.html)。

到这里，我们的OpenVPN配置就完成了，现在该是收获的时候了。

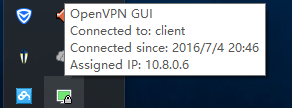
我们先进入服务器端所在计算机的Windows服务界面(【开始】->【运行】->【services.msc】)，然后启动OpenVPN Service服务，从而启动服务器端的OpenVPN。



然后，我们切换到客户端计算机，双击安装OpenVPN时在桌面上生成的OpenVPN GUI图标，此时任务栏右下角会出现如下图所示的托盘图标，右键该图标，点击【connect】即可启动OpenVPN客户端，并尝试连接服务器。



如果连接成功，该托盘图标将会变为绿色，如下图所示：

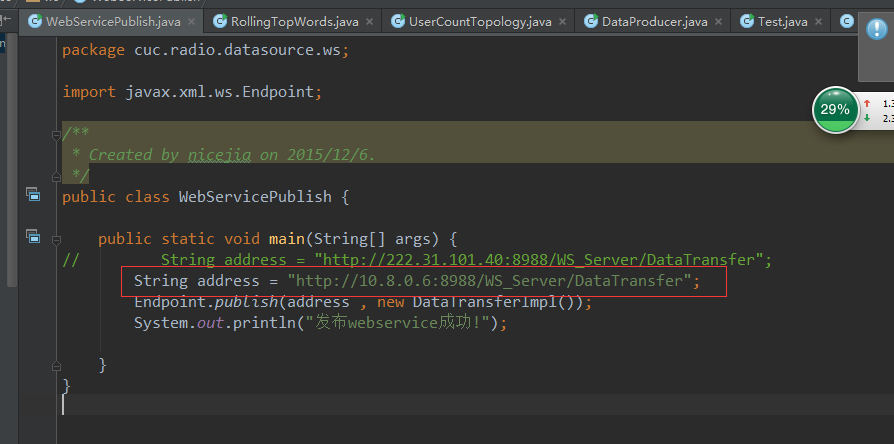


该ip地址是服务器自动分配

到这里，我们的OpenVPN配置都已经大功告成了~！现在，你就可以使用10.8.0.\*等虚拟IP来访问包括服务器在内的其他OpenVPN成员了。

**连通大数据平台**

将webservicepublish中代码修改如下：

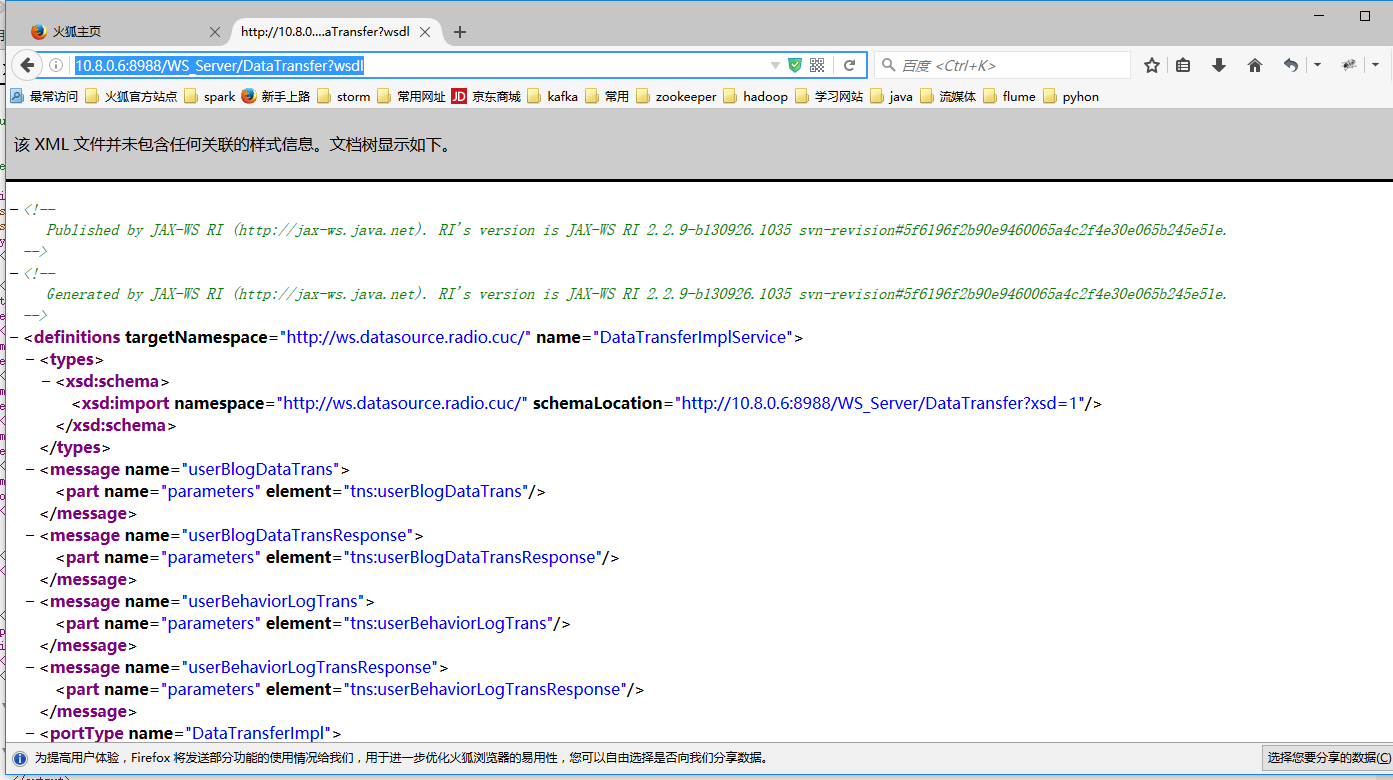


重新发布

输入网址：

<http://10.8.0.6:8988/WS_Server/DataTransfer?wsdl>

显示界面



连接成功

参考文档：

<http://www.softown.cn/post/136.html>

http://www.365mini.com/page/14.htm