完整CentOS搭建OpenVPN服务详细教程

阿龙along 2018-01-24 原文

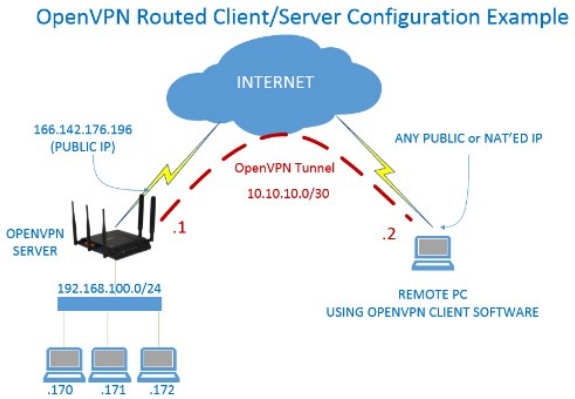
一、介绍

1、定义

① OpenVPN是一个用于创建虚拟专用网络加密通道的软件包，最早由James Yonan编写。OpenVPN允许创建的VPN使用公开密钥、电子证书、或者用户名 / 密码来进行身份验证。

② 它大量使用了OpenSSL加密库中的SSLv3/TLSv1协议函数库。

③ 目前OpenVPN能在Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X与Microsoft Windows以及Android和iOS上运行，并包含了许多安全性的功能。它并不是一个基于Web的VPN软件，也不与IPsec及其他VPN软件包兼容。



2、原理

① OpenVPN的技术核心是虚拟网卡，其次是SSL协议实现。

② OpenVPN中的虚拟网卡

虚拟网卡是使用网络底层编程技术实现的一个驱动软件。安装此类程序后主机上会增加一个非真实的网卡，并可以像其它网卡一样进行配置。服务程序可以在应用层打开虚拟网卡，如果应用软件（如网络浏览器）向虚拟网卡发送数据，则服务程序可以读取到该数据。如果服务程序写合适的数据到虚拟网卡，应用软件也可以接收得到。虚拟网卡在很多的操作系统中都有相应的实现，这也是OpenVPN能够跨平台使用的一个重要原因。

在OpenVPN中，如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN模式）或数据帧（TAP模式）发送到虚拟网卡上，服务程序接收该数据并进行相应的处理后，会通过SOCKET从外网上发送出去。这完成了一个单向传输的过程，反之亦然。当远程服务程序通过SOCKET从外网上接收到数据，并进行相应的处理后，又会发送回给虚拟网卡，则该应用软件就可以接收到。

3、加密和身份验证

（1）加密

OpenVPN使用OpenSSL库来加密数据与控制信息。这意味着，它能够使用任何OpenSSL支持的算法。它提供了可选的数据包HMAC功能以提高连接的安全性。此外，OpenSSL的硬件加速也能提高它的性能。2.3.0以后版本引入PolarSSL。

（2）身份验证

OpenVPN提供了多种身份验证方式，用以确认连接双方的身份，包括：

① 预享私钥

② 第三方证书

③ 用户名 / 密码组合

预享密钥最为简单，但同时它只能用于创建点对点的VPN；基于PKI的第三方证书提供了最完善的功能，但是需要额外维护一个PKI证书系统。OpenVPN2.0后引入了用户名 / 口令组合的身份验证方式，它可以省略客户端证书，但是仍需要一份服务器证书用作加密。

二、在服务器上搭建openvpn

声明，我的openvpn 是搭建在我自己的阿里云服务器上的

1、安装openvpn 和easy-rsa（该包用来制作ca证书）

（1）安装epel 仓库源

wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

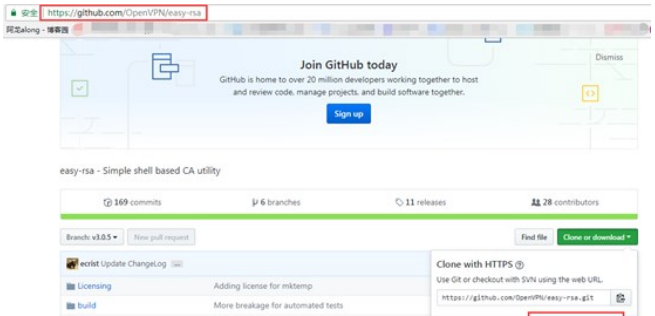
rpm -Uvh epel-release-6-8.noarch.rpm

（2）安装openvpn

[root@along ~]# yum install openvpn

（3）在github 上，下载最新的easy-rsa

① https://github.com/OpenVPN/easy-rsa 下载包



② 上传，解压缩

[root@along]# mkdir openvpn

[root@along openvpn]# unzip easy-rsa-3.0.5.zip

[root@along openvpn]# mv easy-rsa-3.0.5 easy-rsa

2、配置/etc/openvpn/ 目录

（1）创建目录，并复制easy-rsa 目录

[root@along ~]# mkdir -p /etc/openvpn/

[root@along openvpn]# cp -a easy-rsa /etc/openvpn/

（2）配置，编辑vars文件，根据自己环境配置

[root@along test]# cd /etc/openvpn/easy-rsa/easyrsa3

[root@along easyrsa3]# cp vars.example vars

[root@along easy-rsa3]# vim vars

```
set_var EASYRSA_REQ_COUNTRY     "CN"
set_var EASYRSA_REQ_PROVINCE    "Henan"
set_var EASYRSA_REQ_CITY        "Zhengzhou"
set_var EASYRSA_REQ_ORG         "along"
set_var EASYRSA_REQ_EMAIL       "along@163.com"
set_var EASYRSA_REQ_OU          "My OpenVPN"
```

3、创建服务端证书及key

进入/etc/openvpn/easy-rsa/easyrsa3/目录

① 初始化

[root@along ~]# cd /etc/openvpn/easy-rsa/easyrsa3/

[root@along easyrsa3]# ./easyrsa init-pki

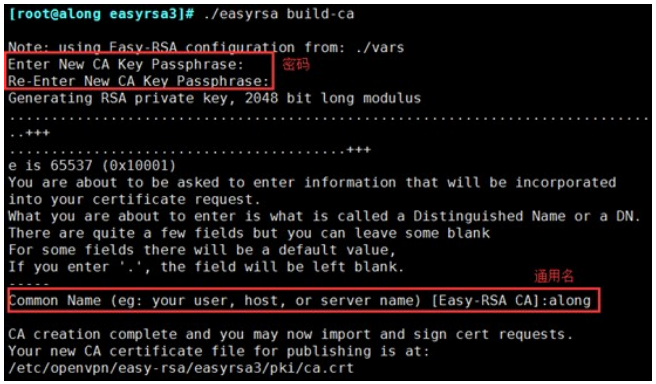
```
[root@along easyrsa3]# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/easyrsa3/pki
```

② 创建根证书

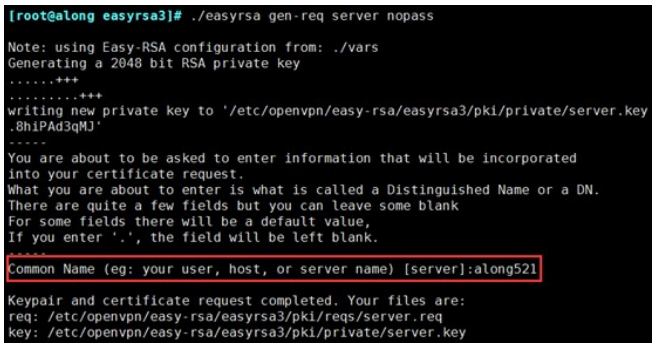
[root@along easyrsa3]# ./easyrsa build-ca



注意：在上述部分需要输入PEM密码 PEM pass phrase，输入两次，此密码必须记住，不然以后不能为证书签名。还需要输入common name 通用名，这个你自己随便设置个独一无二的。

③ 创建服务器端证书

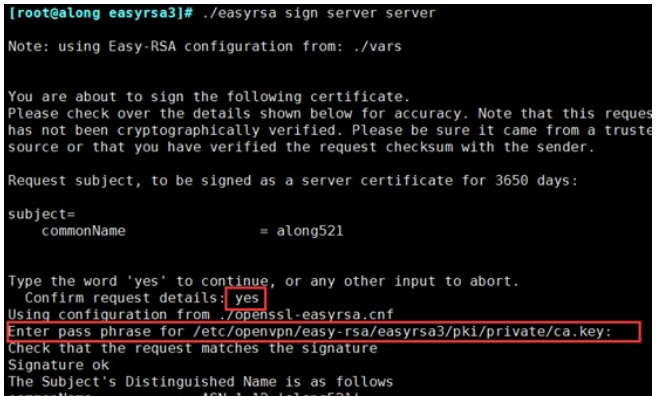
[root@along easyrsa3]# ./easyrsa gen-req server nopass



该过程中需要输入common name，随意但是不要跟之前的根证书的一样

④ 签约服务端证书

[root@along easyrsa3]# ./easyrsa sign server server



```
commonName              :ASN.1 12: 'along521'
Certificate is to be certified until Jan 20 02:50:41 2028 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/easyrsa3/pki/issued/server.crt
```

该命令中.需要你确认生成，要输入yes，还需要你提供我们当时创建CA时候的密码。如果你忘记了密码，那你就重头开始再来一次吧

⑤ 创建Diffie-Hellman，确保key穿越不安全网络的命令

[root@along easyrsa3]# ./easyrsa gen-dh

```
[root@along easyrsa3]# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
...............+.....+.................................................+..........
..................................................................................
.................................................+................................
.............................................+..................................+
```

4、创建客户端证书

① 进入root目录新建client文件夹，文件夹可随意命名，然后拷贝前面解压得到的easy-ras文件夹到client文件夹,进入下列目录

[root@along ~]# mkdir client

[root@along ~]# cp /etc/openvpn/easy-rsa client/

[root@along ~]# cd client/easy-rsa/easyrsa3/

② 初始化

[root@along easyrsa3]# ./easyrsa init-pki //需输入yes 确定

③ 创建客户端key及生成证书（记住生成是自己客户端登录输入的密码）

[root@along easyrsa3]# ./easyrsa gen-req along //名字自己定义

```
[root@along easyrsa3]# ./easyrsa gen-req along

Note: using Easy-RSA configuration from: ./vars
Generating a 2048 bit RSA private key
.....................................................+++
.+++
writing new private key to '/root/client/easy-rsa/easyrsa3/pki/private/along.key.
ezLLlC2DJT'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [along]:along

Keypair and certificate request completed. Your files are:
req: /root/client/easy-rsa/easyrsa3/pki/reqs/along.req
key: /root/client/easy-rsa/easyrsa3/pki/private/along.key
```

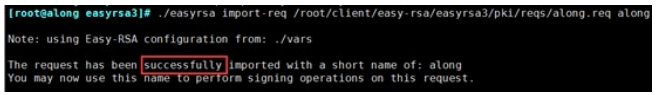
④ 将的到的qingliu.req导入然后签约证书

a. 进入到/etc/openvpn/easy-rsa/easyrsa3/

[root@along easyrsa3]# cd /etc/openvpn/easy-rsa/easyrsa3/

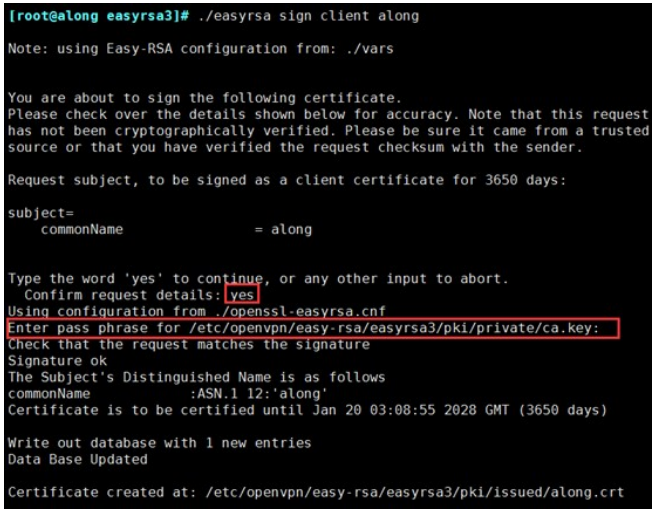
b. 导入req

[root@along easyrsa3]# ./easyrsa import-req /root/client/easy-rsa/easyrsa3/pki/reqs/along.req along



c. 签约证书

[root@along easyrsa3]# ./easyrsa sign client along



//这里生成client所以必须为client，along要与之前导入名字一致

上面签约证书跟server类似，就不截图了，但是期间还是要输入CA的密码

5、把服务器端必要文件放到etc/openvpn/ 目录下

ca的证书、服务端的证书、秘钥

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/**ca.crt** /etc/openvpn/

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/private/**server.key** /etc/openvpn/

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/issued/**server.crt** /etc/openvpn/

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/**dh.pem** /etc/openvpn/

6、把客户端必要文件放到root/openvpn/ 目录下

客户端的证书、秘钥

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/ca.crt /root/client/

[root@along ~]# cp /etc/openvpn/easy-rsa/easyrsa3/pki/issued/along.crt /root/client/

[root@along ~]# cp /root/client/easy-rsa/easyrsa3/pki/private/along.key /root/client

7、为服务端编写配置文件

（1）当你安装好了openvpn时候，他会提供一个server配置的文件例子，在/usr/share/doc/openvpn-2.3.2/sample/sample-config-files 下会有一个server.conf文件，我们将这个文件复制到/etc/openvpn

[root@along ~]# rpm -ql openvpn |grep server.conf

[root@along ~]# cp /usr/share/doc/openvpn-2.4.4/sample/sample-config-files/server.conf /etc/openvpn

（2）修改配置文件

[root@along ~]# vim /etc/openvpn/server.conf

[root@along ~]# grep '^[^#;]' /etc/openvpn/server.conf 修改的地方如下：

```
local 0.0.0.0     #监听地址
port 1194      #监听端口
proto tcp      #监听协议
dev tun      #采用路由隧道模式
ca /etc/openvpn/ca.crt       #ca证书路径
cert /etc/openvpn/server.crt        #服务器证书
key /etc/openvpn/server.key  # This file should be kept secret 服务器秘钥
dh /etc/openvpn/dh.pem      #密钥交换协议文件
server 10.8.0.0 255.255.255.0      #给客户端分配地址池，注意:不能和VPN服务器内网网段有相同
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"       #给网关
push "dhcp-option DNS 8.8.8.8"         #dhcp分配dns
client-to-client        #客户端之间互相通信
keepalive 10 120        #存活时间，10秒ping一次，120 如未收到响应则视为断线
comp-lzo       #传输数据压缩
max-clients 100      #最多允许 100 客户端连接
user openvpn        #用户
group openvpn       #用户组
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log         /var/log/openvpn/openvpn.log
verb 3
```

每个项目都会由一大堆介绍,上述修改，openvpn提供的server.conf已经全部提供，我们只需要去掉前面的注释#，然后修改我们自己的有关配置

（3）配置后的设置

[root@along ~]# mkdir /var/log/openvpn

[root@along ~]# chown -R openvpn.openvpn /var/log/openvpn/

[root@along ~]# chown -R openvpn.openvpn /etc/openvpn/*

8、iptables 设置nat 规则和打开路由转发

[root@along ~]# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j MASQUERADE

[root@along ~]# iptables -vnL -t nat

[root@along ~]# vim /etc/sysctl.conf //打开路由转发

net.ipv4.ip_forward = 1

[root@along ~]# sysctl -p

9、开启openvpn 服务

[root@along ~]# openvpn /etc/openvpn/server.conf 开启服务

[root@along ~]# ss -nutl |grep 1194

```
[root@along ~]# ss -nutl |grep 1194
tcp    LISTEN     0      1          *:1194                     *:*
```

如果开启后没有打开1194 端口，说明开启服务失败，可能是配置文件有错，也有可能是权限不够，自己查询日志解决。

三、客户端连接openvpn

1、下载openvpn客户端安装

windows客户端

mac客户端

2、解压安装，配置client 端配置文件

在sample-config 文件下，有client.ovpn 模板

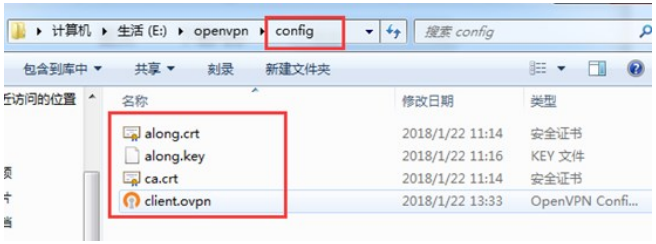
修改，并复制到config 目录下，修改内容如下

```
client
dev tun
proto tcp     //改为tcp
remote 39.xxx.xxx.xxx 1194    //OpenVPN服务器的外网IP和端口，ip和域名都行
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt     //client1的证书
key client.key        //client1的密钥
comp-lzo
```

```
verb 3
```

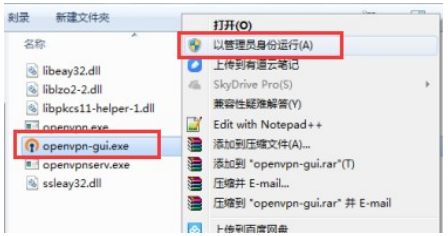
3、把服务器端的证书文件复制到config 目录下

ca.crt along.crt along.key //这三个文件

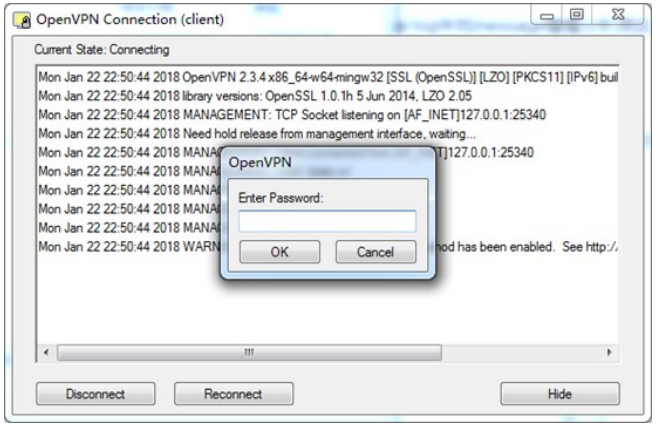


4、启动客户端

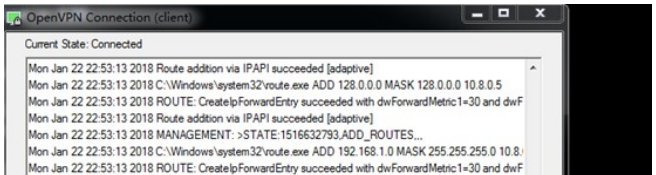
（1）启动，注意启动需以管理员权限启动



（2）输入自己设置的密码



（3）连接成功



5、测试是否成功

（1）在client 查询ip，确实是openvpn 给定的ip

（2）网页查询ip，确实是北京市阿里云的ip

完整CentOS搭建OpenVPN服务详细教程的更多相关文章

1. [linux] centos搭建openvpn服务，脚本颁发/吊销证书 (转载+原创)
   搭建过程转载:http://yestreenstars.blog.51cto.com/1836303/1429537 环境说明:服务端:CentOS 6.5_X64客户端:Windows 7 服务端配 ...
2. CentOS搭建OpenVPN服务(简易版)
   OpenVPN服务端配置 1. 安装OpenVPN软件包 默认的Centos软件源里面没有OpenVPN的软件包,我们可以添加rpmforge的repo,从而实现yum安装openvpn 针对Cent ...
3. CentOS搭建OpenVPN以及WIN&Android&iOS的安装连接
   OpenVPNhttp://info.swufe.edu.cn/vpn/openvpn/#2 苹果.安卓智能手机openvpn的设置_百度经验https://jingyan.baidu.com/art ...
4. centos搭建dns服务
   原文:(https://www.myjinji.top/articles/2020/04/02/1585800289945.html)[https://www.myjinji.top/articles ...
5. （转载）Centos下Elasticsearch安装详细教程
   原文地址:http://www.cnblogs.com/sunny1009/articles/7874251.html Centos下Elasticsearch安装详细教程 1.Elasticsear ...
6. GitHub+Hexo 搭建个人网站详细教程

原文链接 GitHub+Hexo 搭建个人网站详细教程 前言: 随着互联网浪潮的翻腾,国内外涌现出越来越多优秀的社交网站让用户分享信息更加便捷.然后,如果你是一个不甘寂寞的程序猿(媛),是否也想要搭建 ...

7. Centos下Elasticsearch安装详细教程
   Centos下Elasticsearch安装详细教程 1.Elasticsearch简介 ElasticSearch是一个基于Lucene的搜索服务器.它提供了一个分布式多用户能力的全文搜索引擎,基于 ...
8. CentOS搭建xfce桌面+VNC教程
   CentOS搭建xfce桌面+VNC教程 Linux的安全与性能向来为开发者所称道,你可以轻松地在搜索引擎中找到各种Linux优越性的说辞,其中不乏Linux的激进者.特别是当你步入VPS领域,更多地 ...
9. GitHub搭建个人网站详细教程
   GitHub搭建个人网站详细教程: http://blog.csdn.net/gane_cheng/article/details/52203759

随机推荐

1. 什么叫session和cookie-及其设置
   http的无状态? 保持状态, 是指当程序关闭后重启, 上一次操作的历史还能继续, 保持的. 如word中的 "选项"设置. 如windows系统的设置等等. http的设计目的, ...
2. java 查询 mongodb 中的objectid
   网上找了很久查询objectid的方法都是错的,用mongovue能查询出来,但就是用java不知道怎么查询 1.mongovue里的查询方式: {"_id" : ObjectId ...
3. POSIX 可移植操作系统接口
   在一些较老的c语言资料,经常会出现“POSIX标准”. 它的专业解释是: 可移植操作系统接口(英语:Portable Operating System Interface,缩写为POSIX),是IEE ...
4. Spring中@Autowired注解与自动装配
   1 使用配置文件的方法来完成自动装配我们编写spring 框架的代码时候.一直遵循是这样一个规则:所有在spring中注入的bean 都建议定义成私有的域变量.并且要配套写上 get 和 set方法. ...
5. 真机测试时的错误:No matching provisioning profiles found
   1.出现错误的原因是这种---- 公司接收一个外包项目,原来做真机测试的时候,用的是公司申请的苹果开发人员账号.如今项目结束了,准备上线,但客户要求使用客户自己的苹果开发人员是账号上线,于是就用客户的 ...
6. 12 PopupWindow
   PopupWindow创建方式 PopupWindow pop = new PopupWindow() PopupWindow pop = new PopupWindow(上下文, 填充宽, 填充高) ...
7. Oracle简单查询实例
   --查询不重复的职位 select distinct job from emp; --查询年薪,起别名,别名不要用单引号括起来 as nianxin from emp sal; --以这样的形式显示具 ...
8. Asp.net Core 打包发布 (Linux+Nginx)
   如果你觉得如下这些文章对你有帮助,请点击链接支持作者原创 http://www.cnblogs.com/savorboard/ .Net Core SDK 命令介绍 前言 本篇主要介绍 asp.n ...
9. 【leetcode】67-AddBinary
   problem AddBinary code class Solution { public: string addBinary(string a, string b) { string res; ; ...
10. 发邮件 文字+ 附件的方法(QQ or 网易 邮箱)
    #coding:utf-8import smtplibfrom email.mime.text import MIMETextfrom email.mime.multipart import MIME ...

热门专题

ARC10.5汉化包解压密码 | C# FORM SHOW CLOSE后不能 | LARAVEL 新建路由文件不生效 | LINUX IP访问日志 | LINUX修改NGINX配置文件

PHP CACHE自定义缓存驱动 TOMCAT上跑OFBIZ项目 多元回归 机器学习 R语言 IVEW的TREE获取父节点ID REACT 部署WINDOWS服务器

\UI\BIN\ROSLYN\CSC.EXE"的一部分 在NODEJS里执行NPM LINUX下杀死所有ORACLE进程 ALLEGRO与原理图无法交互 JAVA获取一个月所有天

JPA动态拼接WHERE条件 SQLI DUMPER 脱裤教程 C# 只查询有线网卡 PANDAS删除一列数据 SOURCEINSIGHT下面搜索框REFERENCES