原创

linux下生成https的crt和key证书

古城寨主 2017-12-20 11:38:00 3148人阅读 0人评论

今天在配置kibana权限设置时，kibana要求使用https链接。
于是总结了一下linux下openssl生成 签名的步骤：

x509证书一般会用到三类文，key，csr，crt

Key 是私用密钥openssl格，通常是rsa算法。
Csr 是证书请求文件，用于申请证书。在制作csr文件的时，必须使用自己的私钥来签署申，还可以设定一个密钥。
crt是CA认证后的证书文，（windows下面的，其实是crt），签署人用自己的key给你签署的凭证。

1.key的生成

```
1 openssl genrsa -des3 -out server.key 2048
```

这样是生成rsa私钥，des3算法，openssl格式，2048位强度。server.key是密钥文件名。为了生成这样的密钥，需要一个至少四位的密码。可以通过以下方法生成没有密码的key:

```
1 openssl rsa -in server.key -out server.key
```

server.key就是没有密码的版本了。

2. 生成CA的crt

```
1 openssl req -new -x509 -key server.key -out ca.crt -days 3650
```

生成的ca.crt文件是用来签署下面的server.csr文件。

3. csr的生成方法

```
1 openssl req -new -key server.key -out server.csr
```

需要依次输入国家，地区，组织，email。最重要的是□有一个common name，可以写你的名字或者域名。如果为了https申请，这个必须和域名吻合，否则会引发浏览器警报。生成的csr文件交给CA签名后形成服务端自己的证书。

4. crt生成方法

CSR文件必须有CA的签名才可形成证书，可将此文件发送到verisign等地方由它验证，要交一大笔钱，何不自己做CA呢。

```
1 openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey server.key -CAcreat
```

输入key的密钥后，完成证书生成。-CA选项指明用于被签名的csr证书，-CAkey选项指明用于签名的密钥，-CAserial指明序列号文件，而-CAcreateserial指明文件不存在时自动生成。
最后生成了私用密钥：server.key和自己认证的SSL证书：server.crt
证书合并：

```
1 cat server.key server.crt > server.pem
```


openssl https 运维相关

上一篇：Python :check大文件... 下一篇：上网限制和×××基本原理

古城寨主

76篇文章，7W+人气，0粉丝

提问和评论都可以，用心的回复会被更多人看到和认可

Ctrl+Enter 发布 取消 发布

推荐专栏

负载均衡高手炼成记

高并发架构之路

共15章 | sery

￥51.00 130人订阅

订阅

老司机网络运维干货集锦（含路由交换安全…

新西兰资深网工运维之道

共16章 | 姜汁啤酒

￥51.00 426人订阅

订阅

带你玩转高可用

前百度高级工程师的架构高可用实战

共15章 | 曹林华

￥51.00 235人订阅

订阅

猜你喜欢

paramiko基础

在C#用HttpWebRequest中发送GET/HTTP/HTTPS请求

openssl生成证书和自签证书

jboss-as-7.1.0.CR1b域集群和会话复制环境部署

CentOS6.5升级autoconf版本，解决"Autoconf version 2.…

CURL使用HTTPS的技术小结

容器技术 | Docker三剑客之docker-machine

Samba共享服务：匿名共享、身份验证、账户映射、访…

1 0 0 分享

古城寨主