SSL

https 443端口

配置https：

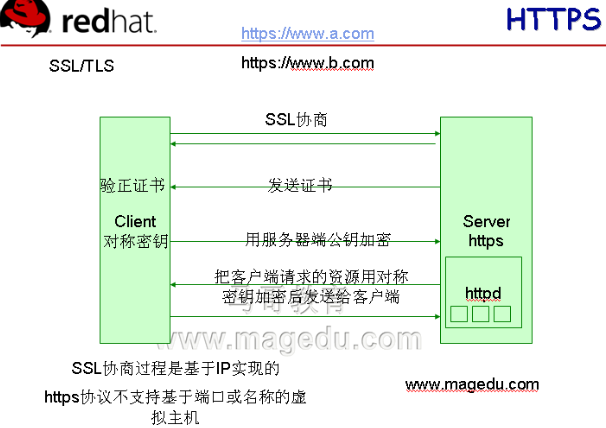
1、启用mod\_ssl模块

2、配置一个使用ssl的**虚拟主机 如果只有一个ip只能配置一个**

需要证书、私钥

3、客户端

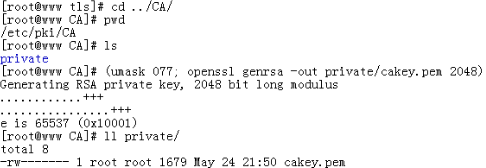
CA证书

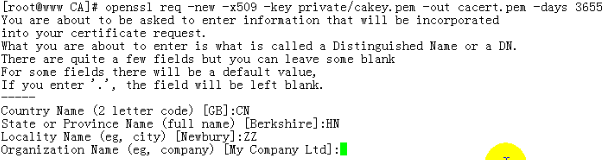


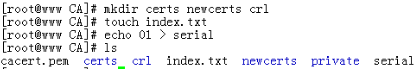
用证书要发证：



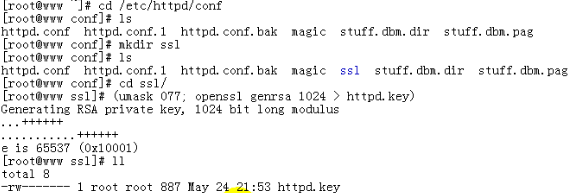






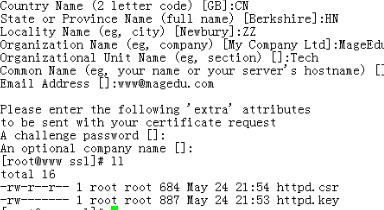


这样ca证书就生成好了



再生成一个证书颁发请求





直接当前主机签署：



这时候csr就没啥用了

然后支持ssl需要安装ssl模块

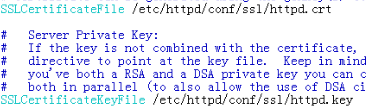


然后启动ssl功能

生成一个conf文件

ssl.conf

编辑 listen 443 主机名 主机什么的



其他应该就不用改什么了

模拟客户端看是否能显示会话建立过程：

openssl s\_client -host www.magedu.com -port 443

这时候还不知道ca证书 还需要 指定ca位置：

openssl s\_client -host www.magedu.com -port 443 -CAfile /usr/share/ssl/certs/ca-bundle.crt

openssl rsa -in server.key -pubout

<VirtualHost 172.16.100.1:80>

ServerName www.magedu.com

DocumentRoot /var/www/empty

RedirectPermanent / https://www.magedu.com/

</VirtualHost>

The ability to resume sessions has enormous impact on the performance of a web server. Using the openssl tool, you can check that your web server performs as expected:

$ openssl s\_client -connect www.thawte.com:443 -state -reconnect

ps -A -o pid,vsz,rsz,command