搭建安全的 Web

1.安装 httpd 软件

```
[root@server0 ~]# yum -y install httpd
```

2.搭建基于域名的虚拟 Web 主机

```
[root@server0 ~]# vim /etc/httpd/conf.d/nsd01.conf
```

```
<Virtualhost *:80>
 ServerName server0.example.com
 DocumentRoot /var/www/html
</Virtualhost>
```

```
[root@server0 ~]# echo test01 > /var/www/html/index.html
[root@server0 ~]# systemctl restart httpd
```

```
[root@desktop0 ~]# elinks -dump server0.example.com 客户端验证
   test01
```

3.部署网站证书（营业执照）

```
[root@server0 ~]# cd /etc/pki/tls/certs      切换路径！
[root@server0 certs]# wget http://172.25.254.254/pub/tls/certs/server0.c
rt
```

4.部署网站根证书（公安局信息）

```
[root@server0 certs]# cd /etc/pki/tls/certs   路径！
[root@server0 certs]# wget http://172.25.254.254/pub/example-ca.crt
```

```
[root@server0 certs]# ls   查看
ca-bundle.crt   ca-bundle.trust.crt   example-ca.crt   make-dummy-cert   Mak
efile   renew-dummy-cert   server0.crt
```

5.部署私钥用于解密

```
[root@server0 certs]# cd /etc/pki/tls/private 切换路径！
[root@server0 private]# wget http://172.25.254.254/pub/tls/private/serve
r0.key
```

```
[root@server0 private]# ls
server0.key
```

6.安装支持 https 软件

```
[root@server0 private]# yum -y install mod_ssl
已加载插件：langpacks
```

7.修改配置文件

```
[root@server0 private]# cd /
[root@server0 /]# vim /etc/httpd/conf.d/ssl.conf
```

```
<VirtualHost _default_:443>

# General setup for the virtual host, inherited from global configuratio
n
#DocumentRoot "/var/www/html"
#ServerName www.example.com:443
```

去掉前面的#

////////////////

```
<VirtualHost _default_:443>

# General setup for the virtual host, inherited from global configuratio
n
DocumentRoot "/var/www/html"
ServerName server0.example.com:443
```

```
#   Server Certificate:                                          指定网站证书
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
```

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/server0.crt
```

```
#   Server Private Key:                                          指定私钥文件
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

```
#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/server0.key
```

```
#   Certificate Authority (CA):                                  指定根证书
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

```
#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt
```

8.重启 httpd 服务

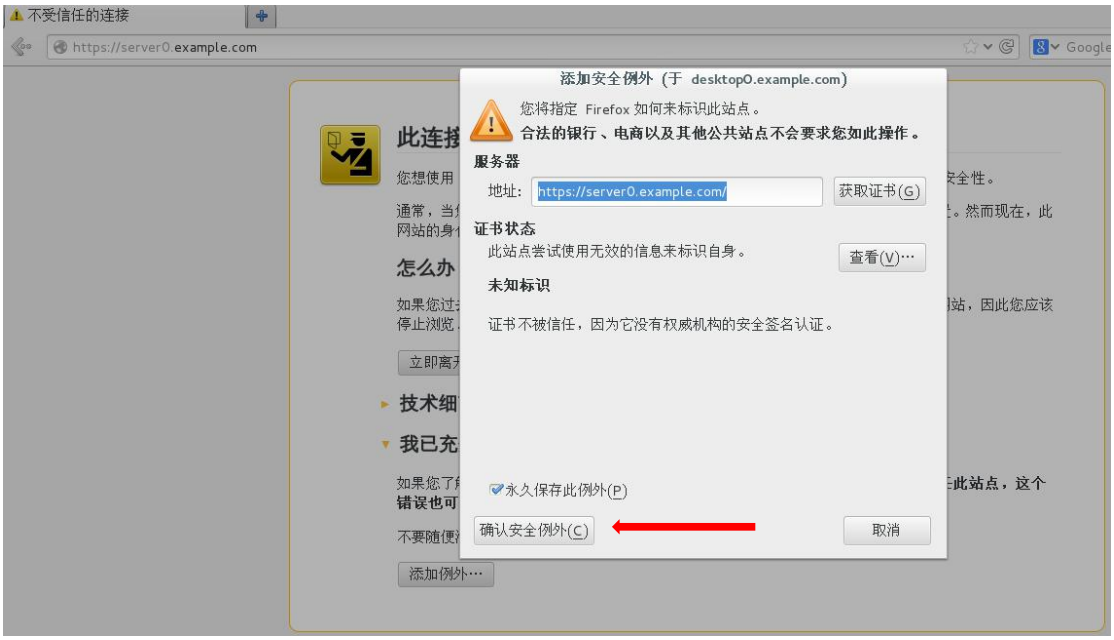
```
[root@server0 /]# systemctl restart httpd
```

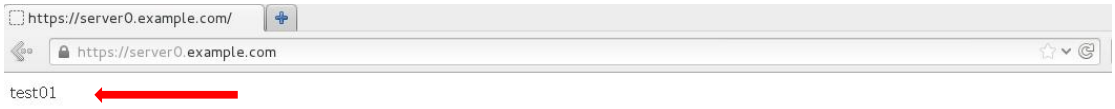
```
[root@desktop0 ~]# firefox https://server0.example.com          客户端验证

(process:30856): GLib-CRITICAL **: g_slice_set_config: assertion `sys_pa
ge_size == 0' failed
```


不受信任的连接
https://server0.example.com
Google
此连接不受信任
您想使用 Firefox 来安全连接至 server0.example.com，但是我们无法确认此连接的安全性。
通常，当您尝试安全连接时，站点会出示受信任的凭据，以证明您访问的是正确的位置。然而现在，此网站的身份无法核实。
怎么办？
如果您过去曾连接到此网站且没有遇到该问题，那么此错误表示可能有人试图冒充该网站，因此您应该停止浏览。
立即离开！
技术细节
我已充分了解可能的风险


不受信任的连接
https://server0.example.com
Google
此连接不受信任
您想使用 Firefox 来安全连接至 server0.example.com，但是我们无法确认此连接的安全性。
通常，当您尝试安全连接时，站点会出示受信任的凭据，以证明您访问的是正确的位置。然而现在，此网站的身份无法核实。
怎么办？
如果您过去曾连接到此网站且没有遇到该问题，那么此错误表示可能有人试图冒充该网站，因此您应该停止浏览。
立即离开！
技术细节
我已充分了解可能的风险
如果您了解现在所发生的一切，您可以让 Firefox 开始信任此站点的凭据。即便您信任此站点，这个错误也可能表明有人试图干涉您的连接。
不要随便添加例外，除非您知道并认同该网站不使用受信任标识的理由。
添加例外…


不受信任的连接
https://server0.example.com
Google
添加安全例外（于 desktop0.example.com）
您将指定 Firefox 如何来标识此站点。
合法的银行、电商以及其他公共站点不会要求您如此操作。
服务器
地址: https://server0.example.com/
获取证书(G)
证书状态
此站点尝试使用无效的信息来标识自身。
查看(V)…
未知标识
证书不被信任，因为它没有权威机构的安全签名认证。
永久保存此例外(P)
确认安全例外(C)
取消



邮件系统

用户发邮件的协议：smtp 端口 25

用户收邮件的协议：pop3 端口 110 imap 端口 143

1.安装 postfix 软件包，提供发邮件功能

```
[root@server0 /]# yum -y install postfix
已加载插件：langpacks
软件包 2:postfix-2.10.1-6.el7.x86_64 已安装并且是最新版本
```

2.修改配置文件

补充：**vim 末行模式 输入 ：set nu** 可以给每一行加上行号

```
# The default setting assumes that you use the default Postfix local
:set nu
```

```
[root@server0 /]# vim /etc/postfix/main.cf
```

```
83 #mydomain = domain.tld
84 #
85 # SENDING MAIL
86 #
87 # The myorigin parameter specifies the domain that locally-posted
88 # mail appears to come from.  The default is to append $myhostname,
89 # which is fine for small sites.  If you run a domain with multiple
90 # machines, you should (1) change this to $mydomain and (2) set up
91 # a domain-wide alias database that aliases each user to
92 # user@that.users.mailhost.
93 #
94 # For the sake of consistency between sender and recipient addresses,
95 # myorigin also specifies the default domain name that is appended
96 # to recipient addresses that have no @domain part.
97 #
98 #myorigin = $myhostname
99 #myorigin = $mydomain
```

```
83 #mydomain = domain.tld
84 #
85 # SENDING MAIL
86 #
87 # The myorigin parameter specifies the domain that locally-posted
88 # mail appears to come from.  The default is to append $myhostname,
89 # which is fine for small sites.  If you run a domain with multiple
90 # machines, you should (1) change this to $mydomain and (2) set up
91 # a domain-wide alias database that aliases each user to
92 # user@that.users.mailhost.
93 #
94 # For the sake of consistency between sender and recipient addresses,
95 # myorigin also specifies the default domain name that is appended
96 # to recipient addresses that have no @domain part.
97 #
98 #myorigin = $myhostname
99 myorigin = server0.example.com
```

默认补全域名后缀

```
113 #inet_interfaces = all
114 #inet_interfaces = $myhostname
115 #inet_interfaces = $myhostname, localhost
116 inet_interfaces = localhost
117
118 # Enable IPv4, and IPv6 if supported
119 inet_protocols = all
```

```
113 #inet_interfaces = all
114 #inet_interfaces = $myhostname
115 #inet_interfaces = $myhostname, localhost
116 inet_interfaces = all
117
118 # Enable IPv4, and IPv6 if supported
119 inet_protocols = all
```

本地所有网络接口均支

```
164 mydestination = $myhostname, localhost.$mydomain, localhost
165 #mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
166 #mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
167 #       mail.$mydomain, www.$mydomain, ftp.$mydomain
```

//////////////////////

```
164 mydestination = server0.example.com
165 #mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
166 #mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
167 #       mail.$mydomain, www.$mydomain, ftp.$mydomain
```

判断为本域邮件

3.重启服务

```
[root@server0 /]# systemctl restart postfix
```

4.测试

```
[root@server0 /]# useradd yg
[root@server0 /]# useradd xln
```

```
[root@server0 /]# mail -s '九阳豆浆机' -r yg xln
hahaxixihehelele
.
EOT
```

```
[root@server0 /]# mail -u xln
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/mail/xln": 1 message 1 new
>N  1 yg@server0.example.c  Fri Dec 29 12:01  18/611   "九阳豆浆机"
& 1
Message  1:
From yg@server0.example.com  Fri Dec 29 12:01:20 2017
Return-Path: <yg@server0.example.com>
X-Original-To: xln
Delivered-To: xln@server0.example.com
Date: Fri, 29 Dec 2017 12:01:20 +0800
From: yg@server0.example.com
To: xln@server0.example.com
Subject: 九阳豆浆机
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
Status: R

hahaxixihehelele

& quit
Held 1 message in /var/mail/xln
```