

## 局域网SSL认证



什么什么尧

5 人赞同了该文章

### 局域网内ssl配置

目的:

在局域网内部使用https会弹出不是私密连接，我们想取消这一步骤，使得https在局域网中是信任的

#### 1.现状描述

测试访问内网的https网址，效果如下：



- 1. 左上方有不安全的标识
- 2. 必须点击高级-->点击继续前往-->才能访问到内容



我们想达到的效果：

- 1. 左上角不显示不安全
- 2. 访问的时候不弹出这个警告页面，直接访问图片，如下：

×

登录即可查看 **超5亿** 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册



2.工具介绍

如果要在局域网达到效果需要满足以下几点要求：

- 1. 证书由可信任的CA机构颁发
- 2. 证书在有效期
- 3. 访问地址和证书的认证地址一致

说明：

- 1. 需要在局域网内构建CA机构
- 2. 证书的有效期建议设置长一点，毕竟在内网使用，升级比较麻烦
- 3. 生成的自签证书其中包含的域名或ip要和浏览器中访问的域名或ip保持一致

2.1 mkcert

mkcert是一个使用go语言编写的生成本地自签证书的小程序，具有跨平台，使用简单，支持多域名，自动信任CA等一系列方便的特性可供本地开发时快速创建https环境使用。

mkcert的浏览器根据操作系统的不同生效也不同：

mkcert supports the following root stores:

- macOS system store
- Windows system store
- Linux variants that provide either
  - update-ca-trust (Fedora, RHEL, CentOS) or
  - update-ca-certificates (Ubuntu, Debian, OpenSUSE, SLES) or
  - trust (Arch)
- Firefox (macOS and Linux only)
- Chrome and Chromium
- Java (when JAVA\_HOME is set)

我这里用windows演示，google浏览器可以支持，firefox不支持

2.1.1安装

由于go的跨平台的特性，所以直接安装即可

[github.com/FiloSottile/...](https://github.com/FiloSottile/...)

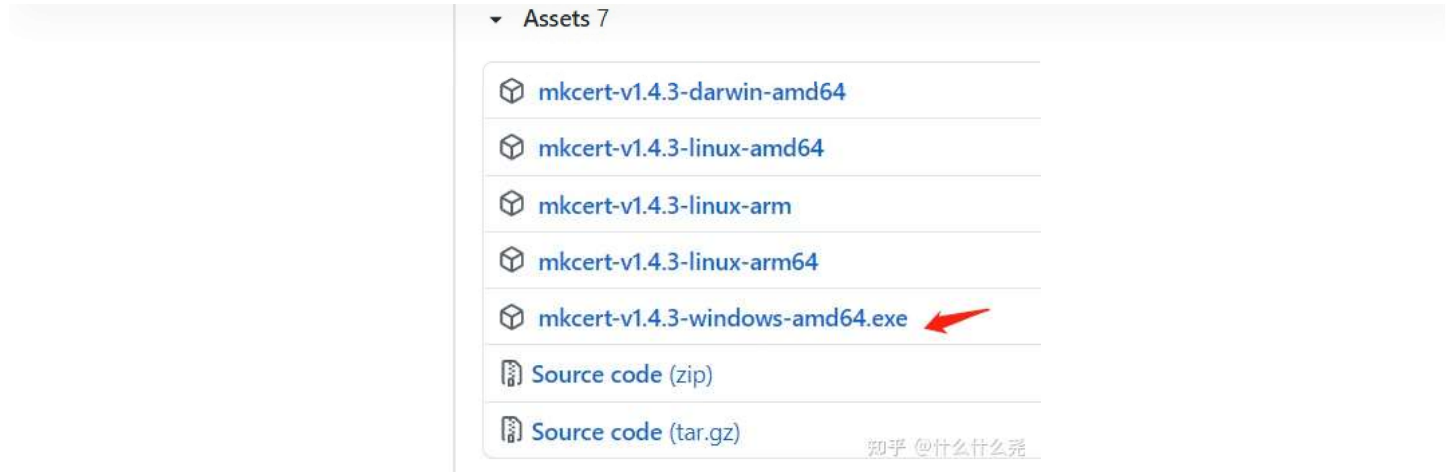
我这里已windows安装包为示例

×

登录即可查看 超5亿 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册



2.1.2 使用

- 1. 下载后将mkcert-v1.4.3-windows-amd64.exe更名为mkcert.exe（为了在控制台少打字）  
在控制台输入 mkcert 可看到

```
D:\个人资料\12.ssl>mkcert
Note: the local CA is not installed in the system trust store.
Note: the local CA is not installed in the Java trust store.
Run "mkcert -install" for certificates to be trusted automatically
Usage of mkcert:

    $ mkcert -install
    Install the local CA in the system trust store.

    $ mkcert example.org
    Generate "example.org.pem" and "example.org-key.pem".

    $ mkcert example.com myapp.dev localhost 127.0.0.1 ::1
    Generate "example.com+4.pem" and "example.com+4-key.pem".

    $ mkcert "*.example.it"
    Generate "_wildcard.example.it.pem" and "_wildcard.example.it-key.pem".

    $ mkcert -uninstall
    Uninstall the local CA (but do not delete it).

For more options, run "mkcert -help".
```

其中明确了 -install -uninstall 的语义

- 1. 将CA证书加入本地可信CA  
在控制台 `mkcert -install`，就帮助我们将mkcert使用的根证书加入了本地可信CA中，以后由该CA签发的证书在本地都是可信的。
- 2. 查看Windows的可信CA列表  
IE浏览器中，选择设置==>Internet选项==>内容==>证书==>mkcert证书

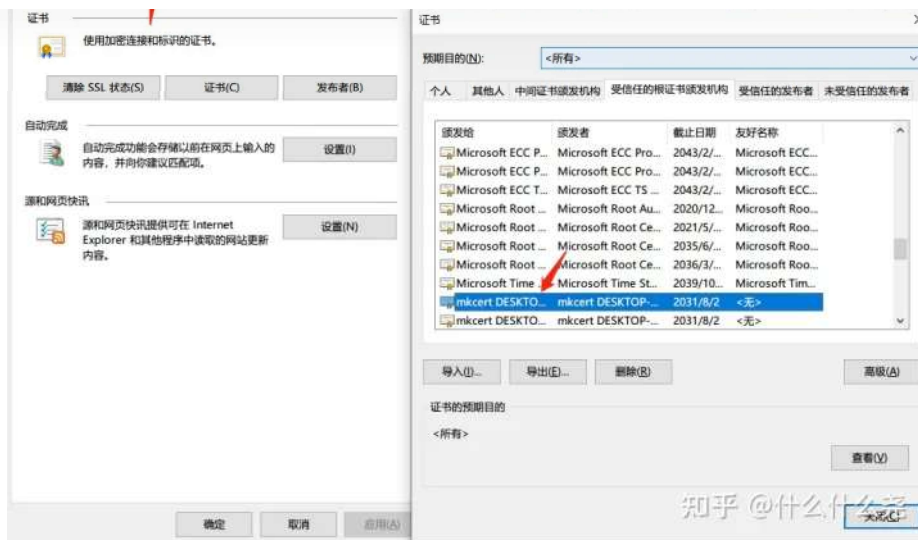
×

登录即可查看 超5亿 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册

知乎

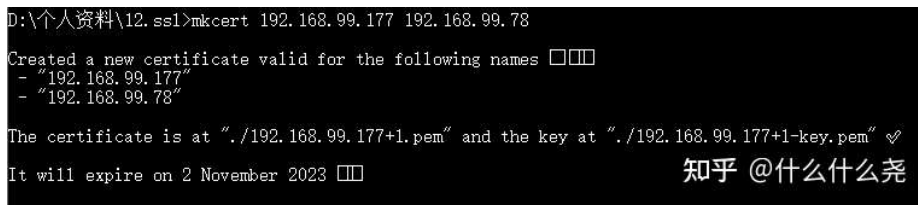


至此标识当前CA已被信任

## 2.2 自签证书

### 1. 生成自签证书

1. 在控制台中命令行输入: `mkcert 192.168.99.177 192.168.99.78`



这里我的ip是177所以以此为例。如果有多个ip地址用空格隔开, 表示该证书支持多个ip的认证, 也就是浏览器访问地址的ip。

控制台中表明生成了192.168.99.177+1.pem证书文件和192.168.99.177+1-key.pem私钥文件

### 1. 使用自签证书

1. 在nginx中配置ssl用于测试
 

```
server { listen 9888 ssl; ssl_certificate
E:\Nginx\1.15.11\conf\ssl\mkcert\192.168.99.177+1.pem; ssl_certificate_key
E:\Nginx\1.15.11\conf\ssl\mkcert\192.168.99.177+1-key.pem; location / { root E:/; } }
```

 这里开启9888的ssl端口。映射E盘来做测试, E盘根目录下有一张名为hzw.PNG的图片。
2. 现在访问 [192.168.99.177/hzw.PNG](http://192.168.99.177/hzw.PNG)会出现警告△页面

## 2.3 发放证书

1. 现在局域网访问测试地址会出现警告页面, 我们需要将我们的CA证书发放给局域网内其他的用户, 其他用户安装即可。
2. 查找本机的CA证书
  1. 命令行查看mkcert的CA证书所在位置
 

```
mkcert -CAROOT
C:\Users\fanya\AppData\Local\mkcert
```
  2. 打开C:\Users\fanya\AppData\Local\mkcert其中包含rootCA.key.pem密钥文件。我们将 rootCA.pem 拷贝一个副本, 并命名(并不识别 pem 扩展名)
 

```
2021/08/02 15:08 2,484 rootCA-key.pem
2021/08/02 15:08 1,797 rootCA.crt
2021/08/02 15:08 1,797 rootCA.pem
```

登录即可查看 **超5亿** 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册

2.4 安装证书

双击rootCA.crt



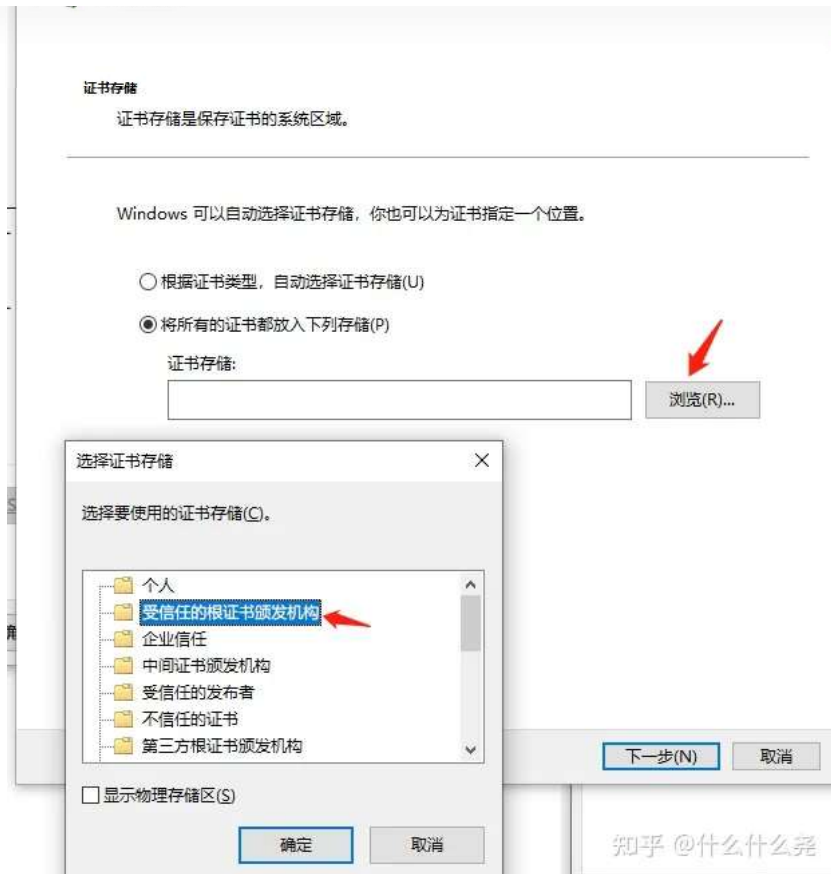
安装证书==>证书存储==>受信任的根证书颁发凭证

登录即可查看 **超5亿** 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册

知乎



## 2.5 测试

浏览器访问 192.168.99.177:9888/hzw...



可以看到左上角变成安全标识，警告△页面也不会弹出。至此局域网就的ssl认证就完成了。

### 3.总结

局域网的ssl通过mkcert和本机安装CA证书即可解决，不过需要用户安装一个证书的操作确实麻烦。但在内网中也只有如此。

下次见

欢迎关注公众号： BugProvider

发布于 2021-08-03 09:17

该图展示了知乎网站的登录提示界面。顶部有一个关闭按钮（X）。主要标题为“登录即可查看 超5亿 专业优质内容”，其中“超5亿”为蓝色。下方文字说明“超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。”。底部有一个带蓝色边框的按钮，文字为“立即登录/注册”。右侧有一个卡通柴犬形象，正拿着一个巨大的白色问号。

知乎

暂无评论

推荐阅读



免费SSL证书申请，给网站添加HTTPS安全加密

格林



SSL：证书文件

大川搬砖      发表于SSL（T...

3分钟了解域名S

3分钟了解域名SSL工作中，我们经常求把web访问协议议，这就要求我们SSL证书申请并应F  
http://www.aliyu

黑马程序员

×

登录即可查看 **超5亿** 专业优质内容

超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。

立即登录/注册

