普通用户接入--802.1x+证书认证（EAP-TLS）

2019年12月12日　14:12

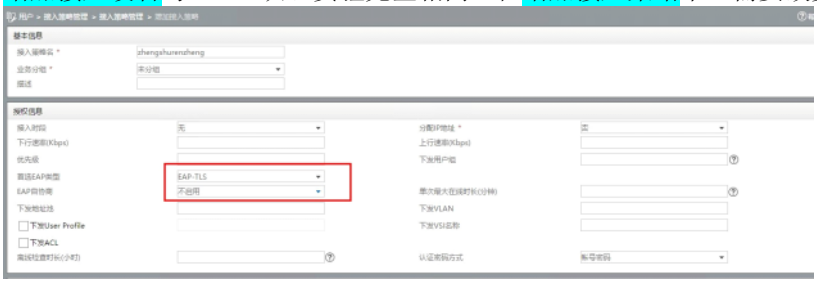

证书认证
imc


证书认证
client

802.1x+证书认证的配置过程包括：配置imc服务器--配置接入设备--客户端配置，与直接802.1x认证相比，证书认证过程中需要在接入服务中配置服务器证书及配置客户端证书

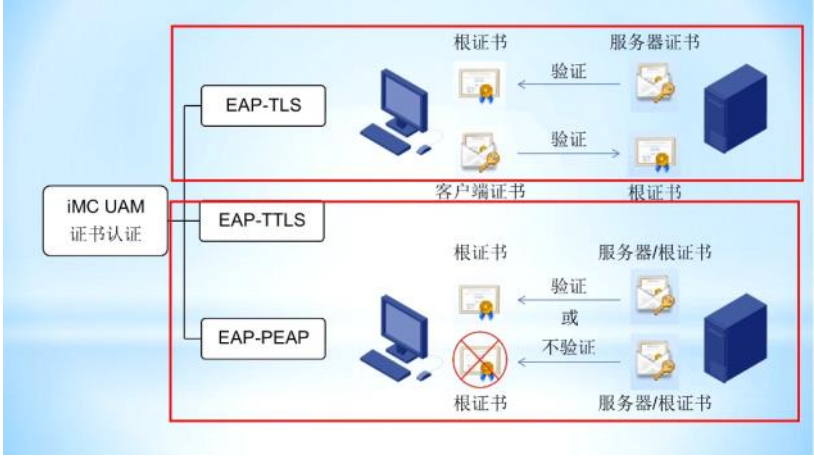
配置iMC服务器：

增加接入设备与802.1x认证实验完全相同，在增加接入策略中，需要改变“首选EAP类型”



- 首选EAP类型/子类型：进行EAP认证时，RADIUS服务器优先下发给客户端的EAP类型。包括：EAP-MD5、EAP-TLS、EAP-TTLS和EAP-PEAP。当首选EAP类型为EAP-TTLS和EAP-PEAP时，还需要首选EAP-MSCHAPv2，EAP-MD5和EAP-GTC其中的一种子类型。
  - EAP-MD5：一种EAP认证方式，使用CHAP方式进行认证。
  - EAP-TLS：是一种基于证书的身份认证，它需要PKI的部署来管理证书。它推荐进行服务器和客户端之间双向认证，认证双方是用证书来标识自己的身份。在认证通过之后，TLS的认证双方会协商出一个共享密钥、Session id以及整套的加密套件（加密，压缩和数据完整性校验），这样认证双方就建立了一个安全可靠的数据传输通道。EAP-TLS是客户端和AAA服务器借助接入设备的透传，通过TLS协议进行的身份认证。EAP-TLS可以利用Session id进行快速重认证，简化认证流程，加快认证速度，还对较大的TLS报文进行了分片处理。
  - EAP-TTLS：是一种基于证书的身份认证，利用TLS认证在客户端和AAA服务器之间建立起一个安全通道，在安全通道内部再承载子类型。它具有保护用户标识和EAP认证的协商过程的作用。隧道内的子类型可以是EAP类型，也可以是非EAP类型。目前UAM支持TTLS下三个EAP的子类型（EAP-MSCHAPv2，EAP-MD5，EAP-GTC）和两个非EAP的子类型（MSCHAPv2，PAP）。UAM在配置接入策略指定首选EAP类型为EAP-TTLS时，也必须首选一种EAP的子类型。在实际认证过程中，如果终端采用非EAP的子类型，如PAP，则终端可以忽略UAM的配置，使用终端配置的子类型进行认证。
  - EAP-PEAP：是一种基于证书的身份认证，利用TLS认证在客户端和AAA服务器之间建立起一个安全通道，在安全通道上再发起EAP认证。它具有保护用户标识，保护EAP认证的协商过程的作用。目前UAM仅支持EAP-MSCHAPv2、EAP-MD5和EAP-GTC认证类型。
- EAP自协商：当客户端配置的EAP类型与UAM中配置的首选EAP类型不同时的处理方式。配置为“启用”时，UAM完全适应由客户端中配置的EAP认证方式，即无论客户端中配置什么类型的EAP认证，UAM都允许客户端继续认证。配置为“禁用”时，如果客户端配置的EAP类型与UAM中配置的首选EAP类型不同，则UAM拒绝其认证。

在EAP-TLS类型中，需要分别在客户端和服务器端安装根证书（即CA证书），还需要在客户端和服务器上安装相应证书完成校验，具体校验过程如下：服务器使用客户端上安装的客户端证书与自身根证书结合来校验客户端的合法性，同样客户端使用服务器上安装的服务器证书与自身根证书结合来校验服务器的合法性。



在接入服务中引用配置好的接入策略，增加接入用户，注意：账号名与客户端证书的名称有关，其他部分与802.1x认证的配置相同，用户在进行证书认证时，不需要密码，在接入用户处设置密码是用于登录自助服务平台。至此imc侧配置完成。

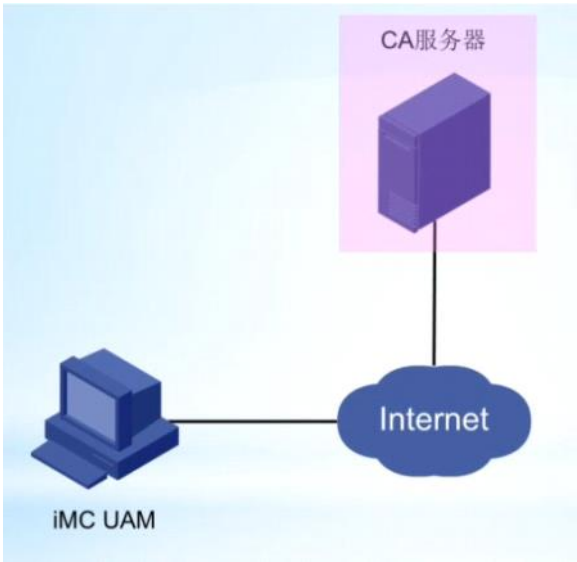
配置接入设备：

接入设备侧只需要更改802.1x的认证方式为eap，其他与802.1x认证的配置相同。

```
[big-sw]dot
[big-sw]dot1x au
[big-sw]dot1x authentication-method e
[big-sw]dot1x authentication-method eap
```

配置服务器证书

在配置服务器证书前需要先配置CA服务器，用来颁发相关证书，

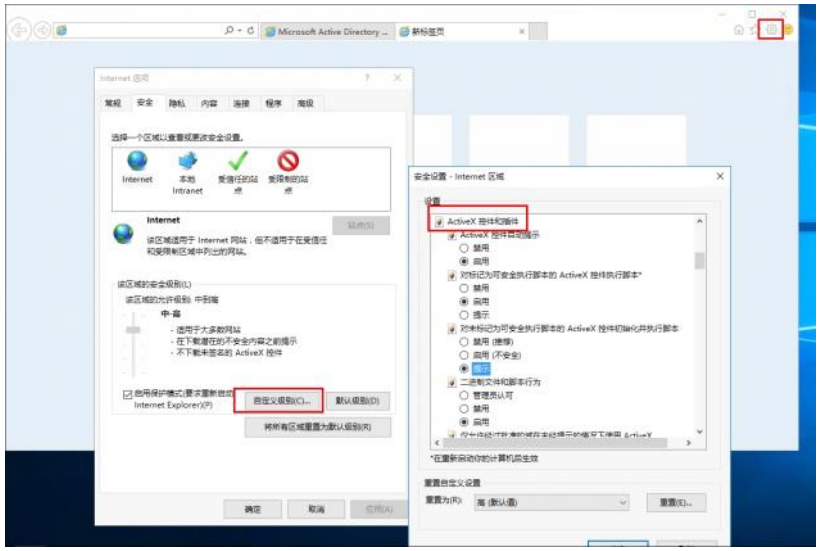


架设CA证书服务器流程及可能遇见问题的解决方法如下：

windows-证书服务...

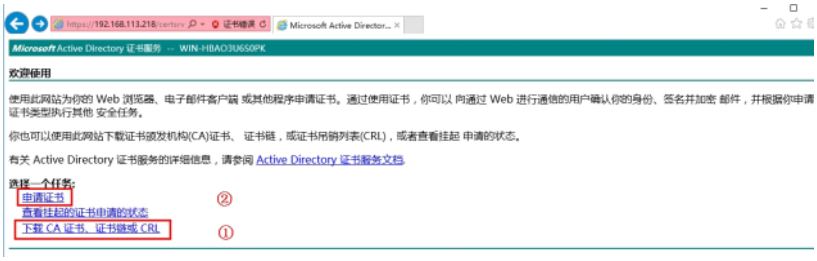
通过web页面申请证书时，有时候会遇到IE浏览器安全控制方面的限制导致你进入到申请证书页面也无法成功申请证书或某些选项无法操作（发生此现象通常在windows server的操作系统）。请参照下面的图示解决此类问题：

点击IE右上角的设置按钮------>Internet选项，对页面中的所有禁用“ActiveX控件”的选项都设置为启用/提示：

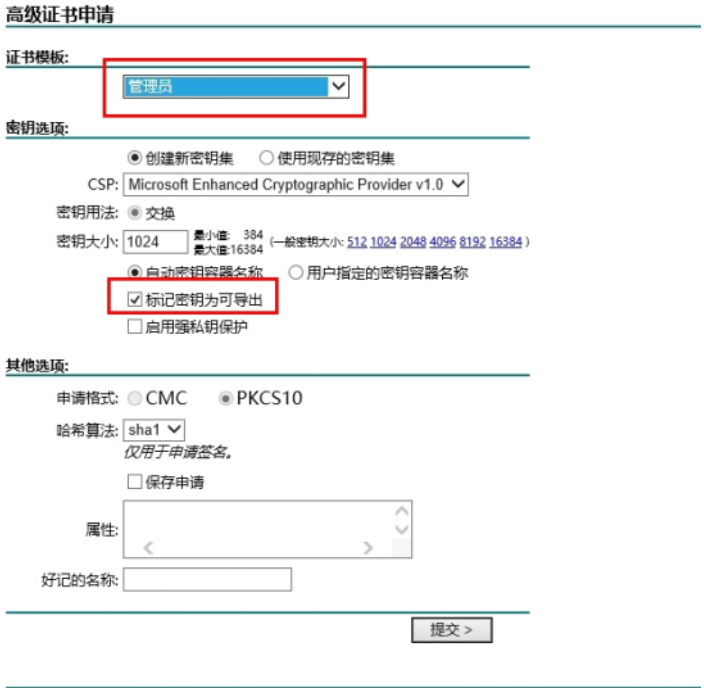


证书服务器架设完成后，在web页面输入https://*证书服务器地址*/certsrv/进入证书申请流程：

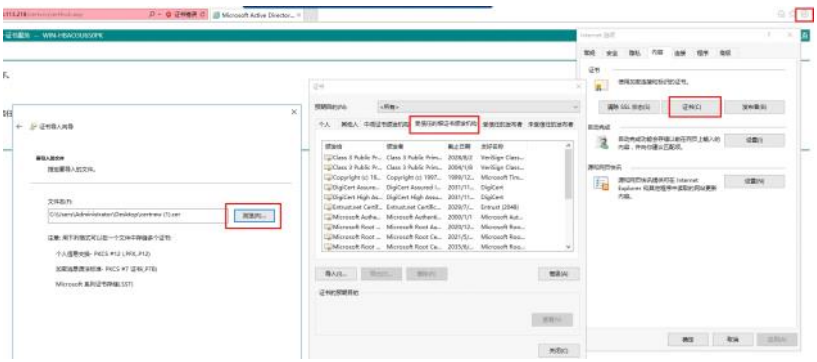
首先下载CA证书（即根证书），将其保存在证书服务器上，



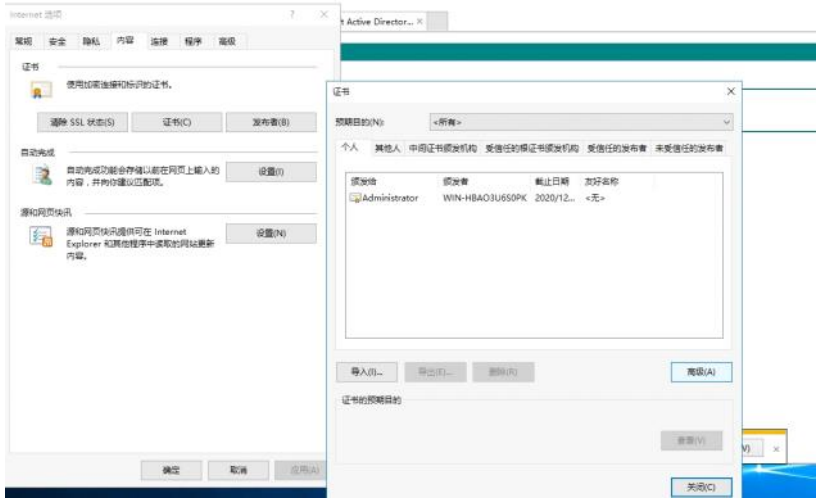
CA证书下载完成后，返回首页，“申请证书”，在服务器证书申请中，证书模板选择“管理员”“标记密钥为可导出”，其他保持缺省设置。

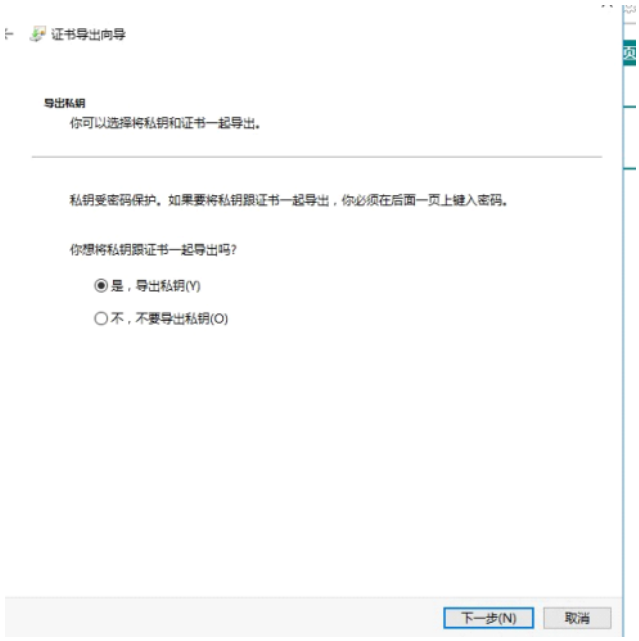


证书申请完成后，点击“安装此证书”时，弹出如下提示，此时需要将CA证书加入到“受信任的根证书颁发机构”中，此后再次安装可安装证书成功，这是因为自己架设的CA服务器不是受信任服务器，需要手动添加到受信任根证书颁发机构中，才可以成功安装，手动添加过程如下：

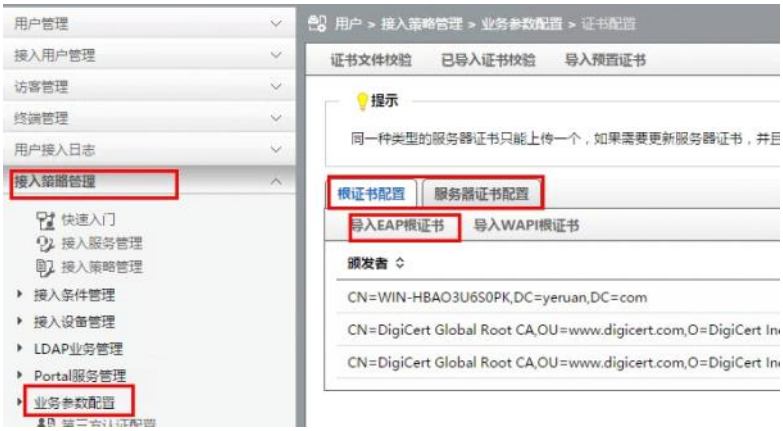


证书安装完成后，可在Internet的证书选项中看到，保存了根证书，且成功安装服务器证书，导出服务器证书，用于配置接入服务中的证书相关配置，在导出证书时必须将私钥与证书一起导出，而且设置密码。

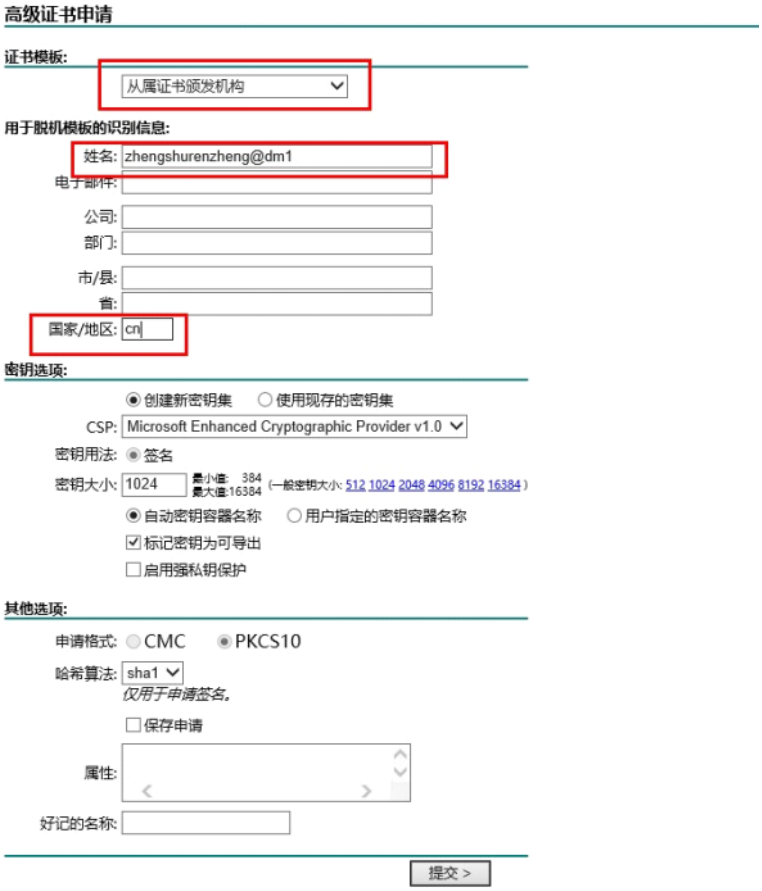




在iMC的接入策略--业务参数配置--证书配置中导入根证书及服务器证书，并进行校验，至此服务器端配置完成。

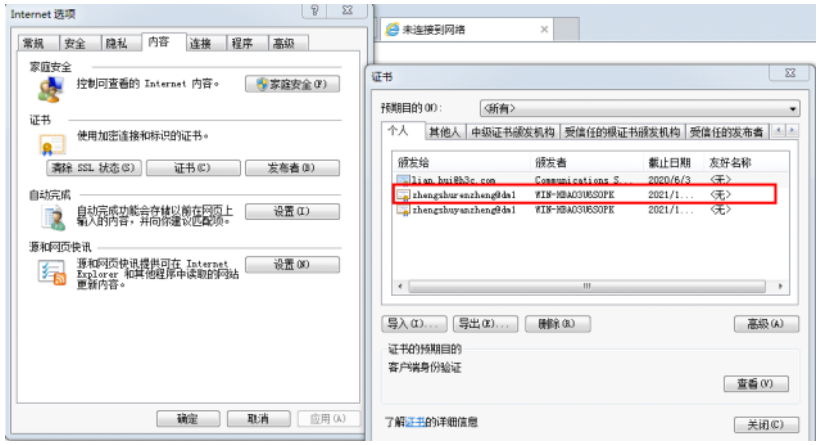


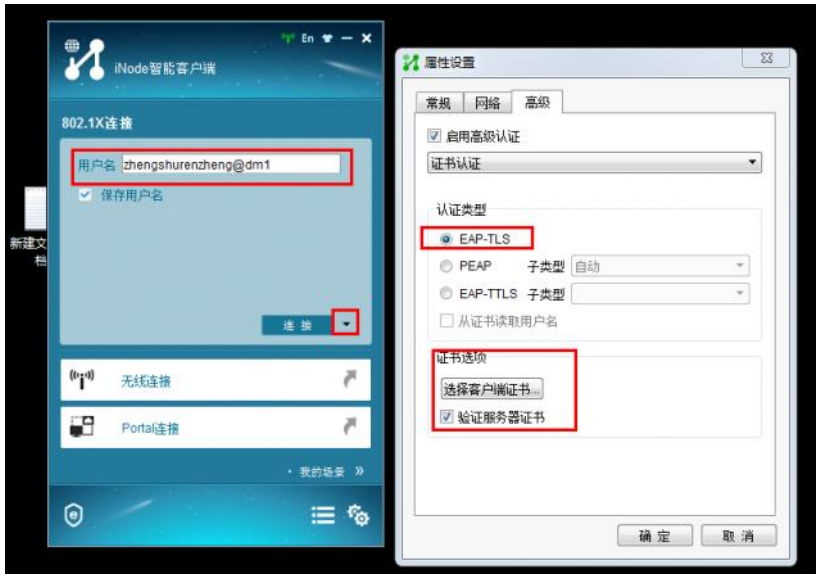
通过上面的方法，申请CA证书和客户端证书，申请客户端证书时的证书模板选择“从属证书颁发机构”，而且姓名必须填写iMC的接入用户的账号，即zhengshurenzheng@dm1，其他与服务器证书一致。证书申请完成后，将CA证书和客户端证书拷贝到客户端安装，然后修改iNode相关配置。



iNode配置

将申请的CA证书及客户端证书安装在客户端后，可在Internet项中检测到，然后将按照图示设置iNode客户端。





认证过程的抓包过程如下：