使用 ADCS 给 CPPM 签发 RADIUS/EAP 服务器证书

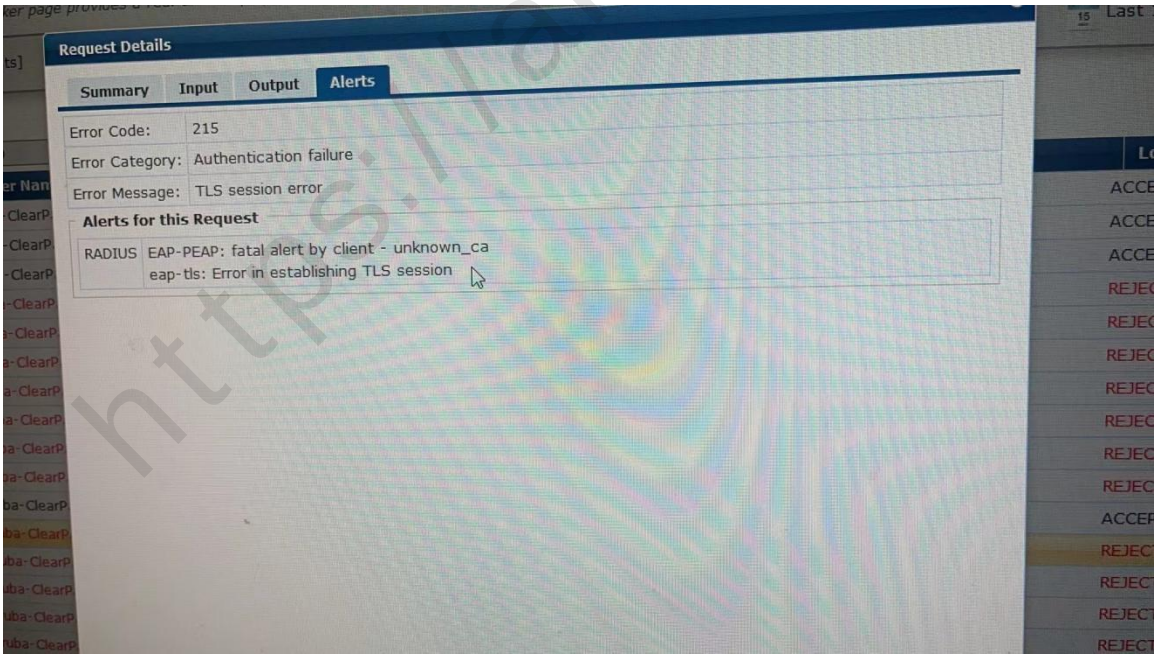
By CCE

现象描述:

CPPM 采用加入 AD 域的方式来实现终端的 802.1x 认证(采用 EAP-PEAP/EAP-TLS/TEAP 认证方法),加域的终端无法完成机器认证或者用户认证..

在 Access Tracker 的 Alerts 选项卡中提示 EAP-PEAP:fatal alert by cient - unknown_ca.

错误信息截图如下:



问题原因:

这里报错的根本原因是在认证过程中,终端是需要验证 RADIUS 服务器证书的,而大多客户场景中的加域电脑上会事先由 ADCS 签发好客户端证书以及在 Trusted Root Certification Authorities-受信任的根证书颁发机构中导入了 ADCS Root CA,所以加域终端会自动信任该 ADCS Root CA 签发的服务器证书. 而 CPPM 系统默认安装好后,采用的是自签的证书,该自签证书是无法被加域终端信任的。

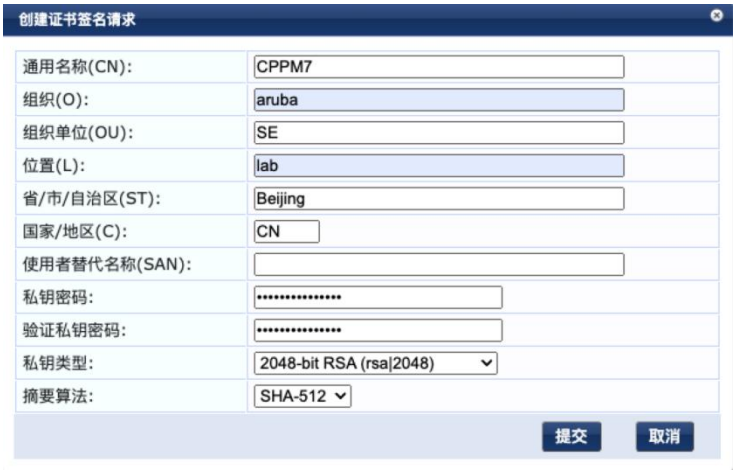
解决办法:

我们需要通过 ADCS 给 CPPM 签发一张 RADIUS/EAP 服务器证书,然后导入到 CPPM 中,这样加域终端就可以自动信任该服务器证书.

以下是配置步骤截图:

1. 打开管理->证书->证书保存, 点击右上角的“创建证书签名请求”

2. 在创建证书签名请求中填写相应信息, 然后点“提交”按钮



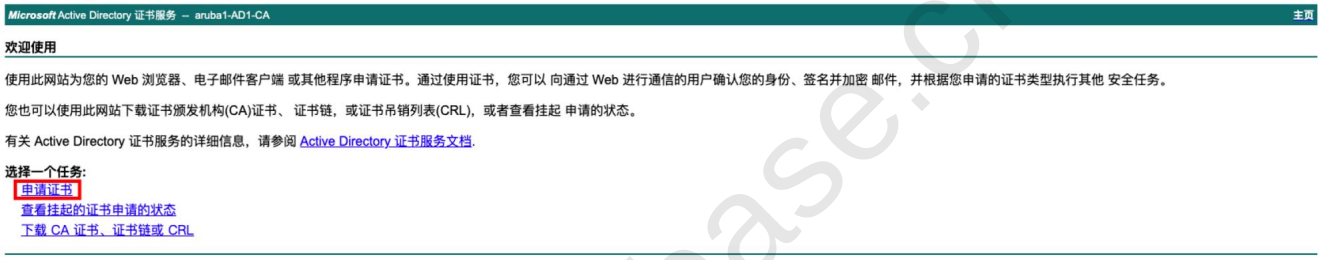
这里的 Private key password 就是后面的导入 cppm 服务器证书时，需要用到的密码

在新的 cppm 6.7 及以后版本，该 private key 是无法导出的，会自动存储在本地，当后面导入证书时，自动会调用本地的 private key。

3. 拷贝自动生成的证书签名请求内容，注意需要包含-----BEGIN…和-----END…内容

4. 通过浏览器打开并登录 ADCS 证书申请页面

5. 点击“申请证书”



6. 点击“高级证书申请”

7. 在打开的证书申请页面中，在 Base-64 编码的证书申请后面的输入框中粘贴第 3 步中拷贝的证书签名请求内容，在证书模板中选择 Web 服务器，点“提交”按钮

8. 在证书已颁发页面勾选 Base 64 编码，点“下载证书”链接下载证书并保存到本地文件夹

9. 点击“主页”返回首页

10. 点击“下载 CA 证书、证书链或 CRL”

11. 在编码方法下勾选 Base 64，然后点击“下载 CA 证书”链接，并保存到本地文件夹

12. 回到 CPPM 管理界面，打开管理->证书->信任列表，点击右上角的“添加”

13. 在添加证书对话框中，点“选择文件”按钮选择第 11 步中保存的 CA 证书文件，在“用法”下面的下拉菜单选择 EAP，然后点“添加证书”按钮

14. 确认 CA 证书已成功添加并启用，用法为 EAP，已启用为 Enabled

15. 打开管理->证书->证书保存，点击右上角的“导入证书”

16. 在导入证书对话框中，证书类型选择“服务器证书”，用法选择“RADIUS/EAP 服务器证书”，上传方法选择“上传证书并使用已保存的私钥”，证书文件后面点“选择文件”选择第 8 步保存的证书文件，然后点“导入”按钮

17. 确认证书已成功导入