

使用 ADACS 给 CPPM 签发 RADIUS/EAP 服务器证书

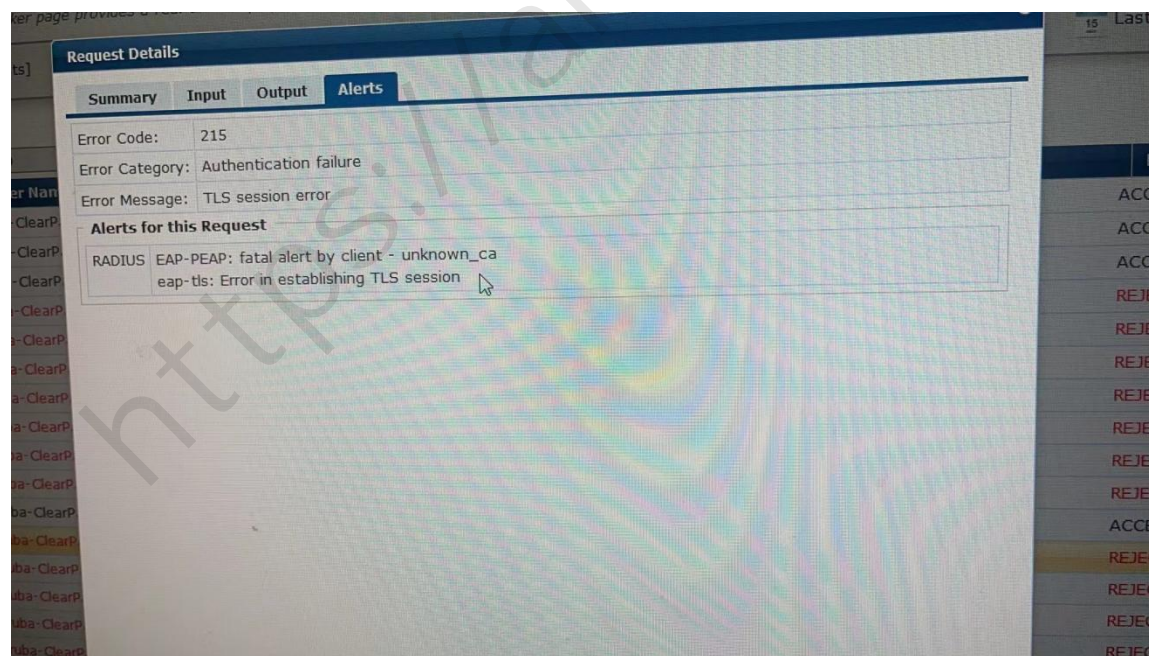
By CCE

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 client - 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

通用名称(CN):	CPPM7
组织(O):	aruba
组织单位(OU):	SE
位置(L):	lab
省/市/自治区(ST):	Beijing
国家/地区(C):	CN
使用者替代名称(SAN):	
私钥密码:	*****
验证私钥密码:	*****
私钥类型:	2048-bit RSA (rsa 2048)
摘要算法:	SHA-512

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，会自动调用本地的 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

创建证书签名请求

在登记过程中将以下内容复制并粘贴到 Web 表单中

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC+DCCAcAQAwwjEOMAwGA1UEAwFQ1BQTTcxCzAJBgNVBAsMA1NFMQ4wDAYD
VQKDAVhcnViYTEQMA4GA1UECAWHQmVpamluZzELMAkGA1UEBhMCQ04xDDAKBgNV
BAcMA2xhYjccASwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOP2F+DduIVN
E/Wc385bqzoR35Ur+dzhcDPKjK24j8bB02J8F/LQBx/Q5UnrqN0kavUhPySuv/5
4Uvc1K8MbkFhkEq6rybnzt3R+IRZze1o2PLf0FLjFj7v6EuEanoV2T+FJxbow21n
RrtMI0uB05uiTNMYpqfMYZD/u6+40Tbi/zeCo9nKEMYjbsxPTgF6BCTcJZwvSC9e
PgWsOG1BFkHrjux7ClR47v2voyv9kVKQKF3DXigTlyHAOUUV53F4FdCvdDTuXQBe
ChxJmYQnRCxizyuv2Ju8x6oNsdBjNKyB6U3AOJswOQSDLZI+Gfznubw4S1Yb1+S1
kyle/3ndGrUCAwEAAaBZMfcGCSqGSIB3DQEJDjFKMEgwJwYDVR01BCAwHgYIKwYB
BQUHAWEGCCsGAQUFBwMDBggrBgEFBQcDDjAdBgNVHQ4EFgQUgJcqaIPwZebAkIeI
G0wnxJz7nOMwDQYJKoZIhvcNAQENBQADggEBAAwfp7gvMmgrWQ1rSJIHuTFl/riO
STmySjbj8t00uFR9hps6V8X3KbHQIU3IiPSCMj5BuB21OMHTJnmXU8ySFOUcttrC
2dETHA0dNTnQnJwPptUAS4Nm/vg3tPCiIhejUnq7SOZKxQRx4SRTbCipsj6kj2KK
Pt2rQGbbEaOdaZQlzpI/Gg+DVGj+czj4eKE7Vz48JpjMmoXGI9ELfWzkFC55UoL
XEjUYF2Rv5QVgSUp0/3TNhH0sOV7HCqxIHh6Dquvxse/DLDtCsotvkh2nvU+eqp
edSKmJNIEfALvJXefLPgzYugbzP/JpkehE8yUTtys91WJe+Tq8fUko3EwCQ=
-----END CERTIFICATE REQUEST-----

```

4. 通过浏览器打开并登录 ADCS 证书申请页面

登录

http://10.254.5.23
您与此网站的连接不是私密连接

用户名

密码

5. 点击“申请证书”

Microsoft Active Directory 证书服务 -- aruba1-AD1-CA 主页

欢迎使用

使用此网站为您的 Web 浏览器、电子邮件客户端 或其他程序申请证书。通过使用证书，您可以 向通过 Web 进行通信的用户确认您的身份、签名并加密 邮件，并根据您申请的证书类型执行其他 安全任务。您也可以使用此网站下载证书颁发机构(CA)证书、证书链，或证书吊销列表(CRL)，或者查看挂起 申请的状态。

有关 Active Directory 证书服务的详细信息，请参阅 [Active Directory 证书服务文档](#)。

选择一个任务:

- [申请证书](#)
- [查看挂起的证书申请的状态](#)
- [下载 CA 证书、证书链或 CRL](#)

6. 点击“高级证书申请”

Microsoft Active Directory 证书服务 -- aruba1-AD1-CA 主页

申请一个证书

选择一个证书类型:

- [用户证书](#)
- [高级证书申请](#)

- 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

提交一个证书申请或续订申请

要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部 源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。

保存的申请:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC+DCCAcAAQAwIjEOMAwGA1UEAwYFQ1B0TTcxZzA3BqNVBAcMAINF
V00KDAVhcnVjYTEwMA4GA1UECAwHQmVpamLuZzELMAkGA1UEBhMC004x
BACMA2hhYjYjCCAS1d0YjKozIhvcNAQEBBQADggEPADCCAOoCggEBAOP2I
E/Wc385bqzrR35U++dzhcDPKjJk24j8bB02J8F/LOBX/05UnrqN0kavUI
4Uvc lK8MbkFHKEq6rybnzt3R+IRZze1o2PLf0FLJfJ7v6EuEanoV2T+F.
RrtMI0B05u1TNMypqfMYZD/u6+40TB1/zeCo9nKEMYjbsxPTqF6BCTC.
PgWs0G18FkHrjux7CIR47v2vovv9kVKQKF3DXigT LyHAOUUV53F4FdCvc
ChxJmY0nRCxlyzuV2Ju8x6oNsd8jNkyB6U3A0Jsw00SDLZI+GfznuBw4:
ky le/3ndGrUCAwEAAbZMfcGCSg6S1b3DQEJDjFKMEgwJwTDVR0LBCAwf
BQUHwECCsGAOUFBwMDgg r9gEFBQDDJ AdBqNVH04EFa0UqJcqaIPwI
G0wnxJz7n0MwDQYJKoZIhvcNAQENBQADggEBAAwf7gVMSgrW01rSJIH
STmySjbj8t00uFR9hps6V8X3KbHQIUI3IIP5CMj5BuB210MHTJnmXU8ySI
2dETH0dNTnQnjWPptUAS4Nm/vg3tPCiIhejUnq750ZKxQRx45RTbCip:
Pt2rQG8BbEa0BaZLzpI/Gg+DVGj+cj4eKE7Vz48JpJmMoXG19ELfWZI
XEjUYF2Rv50VgSUp0/3TNhH0s0V7HCqx1Hh6Dquvxse/DLdtCsotvkH2I
ed5KmjNIEfALvJXefLPgzYuqbzP/JpkehE8vUTtys91Wje+Tq8fUko3Ev
-----END CERTIFICATE REQUEST-----
```

Base-64 编码的
证书申请
(CMC 或
PKCS #10 或
PKCS #7):

证书模板:
Web 服务器

附加属性:
属性:

提交 >

- 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

证书已颁发

您申请的证书已颁发给您。

DER 编码 或 Base 64 编码


 [下载证书](#)
[下载证书链](#)

- 点击“主页”返回首页

证书已颁发

您申请的证书已颁发给您。

DER 编码 或 Base 64 编码

 [下载证书](#)
[下载证书链](#)

- 点击“下载 CA 证书、证书链或 CRL”

欢迎使用

使用此网站为您的 Web 浏览器、电子邮件客户端 或其他程序申请证书。通过使用证书，您可以向通过 Web 进行通信的用户确认您的身份、签名并加密 邮件，并根据您申请的证书类型执行其他 安全任务。

您也可以使用此网站下载证书颁发机构(CA)证书、证书链，或证书吊销列表(CRL)，或者查看挂起 申请的状态。

有关 Active Directory 证书服务的详细信息，请参阅 [Active Directory 证书服务文档](#)。

选择一个任务:

[申请证书](#)

[查看挂起的证书申请的状态](#)

[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

下载 CA 证书、证书链或 CRL

若要信任从此证书颁发机构颁发的证书，[请安装此 CA 证书](#)。

要下载一个 CA 证书、证书链或 CRL，选择证书和编码方法。

CA 证书:

当前 [aruba1-AD1-CA]

编码方法:

DER

Base 64

[安装 CA 证书](#)

[下载 CA 证书](#)

[下载 CA 证书链](#)

[下载最新的基 CRL](#)

[下载最新的增量 CRL](#)

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”

ClearPass Policy Manager

管理 > 证书 > 信任列表

证书信任列表

此页面显示受信任证书颁发机构(CA)的列表。您可以添加、查看或删除证书。

筛选器: 主题 包含 执行 清除筛选器 显示 20 记录

#	主题	用法	有效性	已启用
1.	<input type="checkbox"/> CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR	其他	Valid	Disabled
2.	<input type="checkbox"/> CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR	其他	Valid	Disabled
3.	<input type="checkbox"/> CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR	其他	Valid	Disabled
4.	<input type="checkbox"/> CN=Aruba Networks Trusted Computing Issuing CA 1,DC=deviceign,DC=arubanetworks,DC=com	其他	Valid	Disabled
5.	<input type="checkbox"/> CN=Aruba Networks Trusted Computing Issuing CA 2,DC=deviceign,DC=arubanetworks,DC=com	其他	Valid	Disabled
6.	<input type="checkbox"/> CN=Aruba Networks Trusted Computing Issuing CA 3,DC=deviceign,DC=arubanetworks,DC=com	其他	Valid	Disabled
7.	<input type="checkbox"/> CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	其他	Valid	Disabled

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

导入证书

证书类型:	服务器证书
服务器:	CPPM7 (10.254.5.107)
用法:	RADIUS/EAP 服务器证书
上传方法:	上传证书并使用已保存的私钥
证书文件:	<input type="button" value="选择文件"/> certnew (47).cer

Note: 不建议将使用通配符作为常用名(例如: *.arubanetworks.com)的证书和扩展验证证书(EV, "Green Bar")用作 RADIUS/EAP 服务器证书。使用这些类型的证书时, 部分客户端可能无法进行身份验证。

17. 确认证书已成功导入

aruba
ClearPass Policy Manager
Menu

- 仪表盘
- 监视
- 配置
- 管理
- ClearPass Portal
- 用户和特权
- 服务器管理器
- 外部服务器
- 外部帐户
- 证书
 - 证书保存
 - 信任列表
 - 吊销列表
- 字典
- 代理和软件更新
- 支持

管理 > 证书 > 证书保存
Menu

证书保存

服务器证书更新成功。

可用于创建多个服务证书, 其中的每个证书都与特定 ClearPass 服务关联。

服务器证书
服务与客户证书

选择服务器: CPPM7 (10.254.5.107)
选择使用情况: RADIUS/EAP 服务器证书

Subject:	CN=CPPM7, OU=SE, O=aruba, L=lab, ST=Beijing, C=CN
Issued by:	CN=aruba1-AD1-CA, DC=aruba1, DC=local
Issue Date:	Nov 16, 2023 19:02:36 CST
Expiry Date:	Nov 15, 2025 19:02:36 CST
Public Key Algorithm:	RSA
Certificate Enabled:	是
Validity Status:	Valid
Details:	<input type="button" value="View Details"/>