证书和权限高级观点CUCM的

目录

简介

本文目的将了解证书和证书权限基础。本文恭维参考所有加密或认证功能在Cisco Unified Communications Manager的其他Cisco文档(CUCM)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

证书目的

证书用于在端点之间建立信任/数据的验证和加密。这确认终端与打算的设备联络并且有选项加密在两个终端之间的数据。

定义托拉斯从证书的观点

证书的多数重要部分是端点可以由您的端点委托的定义。本文帮助您懂得和定义您的数据如何加密并且共享与打算的网站，电话， FTP服务器，等等。

当您的系统委托证书时，这意味着有在陈述的您的系统的一被事先装配的证书它是确信100的百分比共享信息用正确端点。否则，它终止这些端点之间的通信。

此的一非技术性的示例是您的驾驶执照。您使用此许可证(服务器/服务证书)证明，您是谁您说您是;您从由机动车给权限的机动车分组获取您的许可证(中间证书)您的本地分部(DMV)分部您的状态(认证机关)。当您需要显示您的许可证(服务器/服务证书)时对官员，官员知道他们能委托DMV分组(中间证书)和机动车分部(认证机关)，并且他们能验证此许可证由他们发出(认证机关)。您的标识验证给官员，并且他们当前相信，您是谁您说您是。否则，如果给未由DMV的一个错误许可证(服务器/服务证书) (中间证书)签字，然后他们不会委托谁您说您是。本文档的剩余部分提供证书层级的一详细，技术说明。

浏览器如何使用证书

1. 当您访问一个网站时，请输入URL，例如http://www.cisco.com。
2. 主机该站点的DNS查找服务器的IP地址。
3. 浏览器导航到该站点。

没有证书，知道是不可能的是否使用了一个恶意DNS服务器，或者是否路由到另一个服务器。证书保证您适当地和安全地路由到打算的网站，例如您的内存段网站，个人或敏感信息您输入安全。

他们使用的所有浏览器有不同的图标，但是通常，您看到在地址栏的挂锁象这样：

1. 点击挂锁，并且窗口显示：**图 1：网站识别**
2. 如此示例所显示，点击**视图证书**发现站点的证书：**图 2：证书信息，常规选项卡**选中项目信息是重要。**发出由**已经公司或Certificate Authority (CA)该您的系统信任。**有效从/至**是日期范围此证书是可用的。(您有时看到您认识您信任CA，但是的证书您看到证书无效。总是请检查日期，因此您知道它是否超时。)**提示**：在超时前，最佳实践是创建在您的日历的一提醒更新证书。这防止将来问题。

PEM之间的差异与DER证书

PEM是ASCII;DER二进制。图3显示PEM证书格式。

图 3：PEM证书示例

图4显示DER证书。

图 4：DER证书示例

多数CA公司类似Verisign或Thawt使用发送证书的PEM格式对客户，因为是电子邮件友好。客户应该复制整个字符串和包括**-----开始证书-----**并且**-----END证书-----**请粘贴它到文本文件，并且保存它与分机.PEM或.CER。

Windows能读DER如图5.所显示，并且CER格式化与其自己的证书管理Applet并且显示证书。

图 5：证书信息

有时，设备要求一个特定格式(ASCII或二进制)。为了更改此，请下载从CA的证书在需要的格式或请使用一个SSL转换器工具，例如https://www.sslshopper.com/ssl-converter.html。

证书层级

为了委托从端点的一证书，必须有信任已经设立与第三方例如CA.，图6显示那里是三证书层级。

图 6：证书层级

- **Verisign**是CA。
- **Verisign等级3扩展的验证SSL CA**是中间或签署的服务器证书(CA授权的服务器发行在其名称的证书)。
- **www.website.com**是服务器或服务证书。

您的端点需要知道能首先委托CA和半成品证书，在知道前能委托SSL握手(见下)提交的服务器证书。要改善请知道此信任如何工作，参考在本文的部分：**定义"托拉斯"从证书的观点**。

自签名证书与第三方证书

自已签署的和第三方证书之间的主要区别是谁签字证书，您是否委托他们。

自签名证书是提交它的服务器签字的证书;因此，服务器/服务证书和CA证书是相同的。

第三方CA是公共CA (类似Verisign、Entrust， Digicert)或服务器提供的服务(类似Windows 2003年，Linux， Unix， IOS)该控制服务器/服务证书的正确性。

每一个可以是CA.您的系统是否委托该CA，是什么最要紧。

公用名称和附属的代替名称

公用名称(CN)和附属的代替名称(SAN)是对是请求的地址的IP地址或完全合格的域名(FQDN)的参考。例如，如果输入https://www.cisco.com，然后CN或SAN必须有在报头的www.cisco.com。

在Figure7显示的示例中，证书有CN作为www.cisco.com。www.cisco.com的URL请求从浏览器根据证书引见的信息检查URL FQDN。在这种情况下，他们配比，并且它显示SSL握手是成功的。此网站验证是正确网站，并且通信当前加密在桌面和网站之间。

图 7：网站验证

在同一证书，有三个FQDN/DNS地址的一个SAN报头：

图 8：SAN报头

此证书能验证/验证www.cisco.com (也定义在CN)， cisco.com和cisco-images.cisco.com。这意味着您能也键入cisco.com，并且此同样证书可以用于验证和加密此网站。

CUCM能创建SAN报头。参考的贾森预烧硬件的文档，上传Ccmadmin Web在支持公共的CUCM GUI证书关于SAN报头的更多信息。

通配符证书

通配符证书是使用星号(*)代表在URL的部分的所有字符串的证书。例如，为了有www.cisco.com的一证书， ftp.cisco.com， ssh.cisco.com，等等，管理员只将需要创建*.cisco.com的一证书。为了存金钱，仅管理员需要采购单个证书，并且不需要采购多份证书。

Cisco Unified Communications Manager当前不支持此功能(CUCM)。然而，您能记录此增强：CSCta14114 ：要求通配符证书支持在CUCM和专用密钥导入的。

识别证书

当证书有同一信息在他们时，您能看到它是否是同一证书。所有证书有一唯一序列号。您能使用此比较，如果证书是同一证书，重新生成或者假劣。图9提供一示例：

图 9：证书序号

CSR和他们的目的

CSR代表证书签名请求。如果要创建CUCM服务器的一第三方证书，您需要CSR出席到CA。此CSR看起来很多PEM (ASCII)证书。

注意： 这不是证书，并且不可能使用作为一个。

CUCM通过Web GUI自动地创建CSR ：**Cisco Unified操作系统的管理>** Security > Certificate Management **>生成CSR** >选择您要创建证书>然后**生成CSR的**服务。在使用时候此选项，一新的专用密钥和CSR生成。

注意： 专用密钥是对此服务器和服务是唯一的文件。不应该给这到任何人!如果提供一专用密钥给某人，危及该的安全证书提供。并且，如果使用旧有CSR创建证书，请勿重新生成同一服务的新的CSR。CUCM删除旧有CSR和专用密钥并且替换他们两个，使旧有CSR无用。

在支持公共的参考的贾森预烧硬件的文档：上传Ccmadmin Web GUI证书的CUCM关于如何创建CSR的信息。

使用在端点和SSL/TLS握手进程之间的证书

握手协议是协商数据传输会话的安全参数的一系列的程序化的消息。参考详细SSL/TLS ，描述在握手协议的消息序列。这些在数据包捕获(PCAP)能被看到。详细信息包括初始，随后和最终消息传送和接收在客户端和服务器之间。

CUCM如何使用证书

在Tomcat和Tomcat托拉斯之间的区别

当证书上传对CUCM时，有每服务的两个选项通过**Cisco Unified操作系统的管理>** Security > Certificate Management **>查找**。

允许您**管理**在CUCM的证书的五服务是：

- tomcat
- ipsec
- CallManager
- capf
- 电视(在CUCM版本8.0及以后)

这是允许您**上传**证书到CUCM的服务：

- tomcat
- Tomcat托拉斯
- ipsec
- ipsec托拉斯
- CallManager
- CallManager托拉斯
- capf
- CAPF托拉斯

这些是服务可用在CUCM版本8.0及以后：

- 电视
- 电视托拉斯
- 电话托拉斯
- 电话VPN托拉斯
- 电话sast托拉斯
- 电话CTL托拉斯

由版本欲了解更详细的信息参考CUCM安全指南在证书的这些类型。此部分只说明在服务证书和信任认证之间的区别。

例如，与**Tomcat**， Tomcat**信任**上传CA，并且半成品证书，以便此CUCM节点认识它能委托CA和半成品服务器签字的所有证书。Tomcat证书是由在此服务器的Tomcat服务提交的证书，如果端点做一个HTTP请求到此服务器。为了由Tomcat允许第三方证书的演示， CUCM节点需要知道能委托CA和半成品服务器。所以，它是需求上传CA和半成品证书，在Tomcat (服务)前证书上传。

上传Ccmadmin Web在支持公共的参考的贾森预烧硬件的CUCM GUI证书对于将帮助您知道如何上传证书到CUCM的信息。

每服务有其自己的服务证书和信任认证。他们不工作彼此。换句话说，作为Tomcat托拉斯服务和中间证书上传的CA不可能由CallManager服务使用。

注意： 在CUCM的证书是a每个节点基本类型。所以，如果需要证书上传对发行商和您请需要用户有同一证书，您需要上传他们到每个单个服务器和节点在CUCM版本8.5之前。在CUCM版本8.5中及以后，有复制上传的证书对节点其余在集群的服务。

注意： 每个节点有不同的CN。所以，必须由每个节点创建CSR为了服务能提交他们自己的证书。

如果有在的另外的特定问题任何CUCM安全功能，参考安全文档。

结论

本文协助解决并且构件高层次在证书的知识。此主题能要紧能变得更加详细，但是本文熟悉足够您与证书一起使用。如果有在任何CUCM安全功能的问题，由版本参考CUCM安全指南欲知更多信息。

相关信息

- Cisco Unified Communications Manager (CallManager)维护和安全指南
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco支持社区：上传Ccmadmin Web GUI证书的CUCM
- Bug CSCta14114 ：要求通配符证书支持在CUCM和专用密钥导入的
- (CER)解释的Cisco Emergency Responder
- 技术支持和文档 - Cisco Systems