使用AD证书服务创建Umbrella自定义根证书

目录

简介

本文档介绍使用Microsoft Windows Active Directory(AD)证书服务创建自定义根证书的说明。

先决条件

要求

Cisco 建议您了解以下主题：

- Microsoft当前支持的Microsoft Windows Server版本
- Windows Server上安装的Active Directory证书服务
- 具有Active Directory证书服务和Web服务/Web注册服务角色的帐户
- 配置为使用UTF-8编码(“UTF8STRING”)颁发证书的证书服务

使用的组件

本文档中的信息基于Cisco Umbrella。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

本文包含有关使用Microsoft Windows Active Directory证书服务创建自定义根证书(用于代替标准Cisco Umbrella根CA证书)，然后使用该根证书签署来自Umbrella的客户CA签名的CA证书功能的证书签名请求(CSR)的说明。

证书字符串编码

如果您的证书服务配置为使用默认编码(“PRINTABLESTRING”)，则生成的证书链无法被某些Web客户端（最明显的是Firefox）信任。

Cisco Umbrella安全Web网关代理使用证书链，该证书链使用UTF8STRING编码对字符串进行编码。如果签署CSR以创建Cisco Umbrella客户CA中间证书的颁发证书（例如，根证书）使用PRINTABLESTRING编码，则Cisco Umbrella客户CA证书的Subject字段的编码为PRINTABLESTRING。此编码无法与Cisco Umbrella R1 CA中间证书（证书链中的下一项）中的Issuer字段的UTF8STRING编码匹配。

RFC 5280第4.1.2.6节要求证书链在已颁发证书的Issuer字段与颁发证书的Subject字段之间保持相同的字符串编码：

"如果证书的主题是CA，则主题字段的编码方式必须与主题CA颁发的所有证书中颁发者字段（第4.1.2.4节）的编码方式相同。"

许多浏览器不执行此要求，但某些浏览器（最明显的是Firefox）会执行此要求。因此，当使用具有客户CA签名的CA证书功能的安全Web网关(SWG)时，Firefox等Web客户端可能会生成不受信任的站点错误，并且不会加载网站。

要解决此问题，请使用不执行RFC 5280要求的浏览器（如Chrome）。

步骤 1：准备AD证书服务模板

1.导航到开始>运行> MMC，打开Active Directory证书颁发机构MMC。

2.选择文件>添加/删除管理单元，然后添加证书模板和证书颁发机构管理单元。选择“确定”。

3.展开证书模板，然后右键单击从属证书颁发机构。单击复制模板。

现在您可以创建一个自定义证书模板，以符合Umbrella文档中列出的要求。

以下是本文创建时详细介绍的要求：

- General 选项卡
  - 请为模板指定一个对您有意义的名称。
  - 将有效期设置为35个月（三年减去一个月）。
  - 将续约期间设置为20天。
- Extensions选项卡
  - 双击基本约束。
    - 确保选中Make this extension critical。
  - 在密钥用法下：
    - 确保选中Certificate Signing&CRL Signing。
    - 取消选择数字签名。
    - 确保Make this extension critical也在此处勾选。
- 选择Apply和OK

步骤 2：发布模板

1.返回到在上一个流程的步骤2中设置的MMC中，展开Certificate Authority部分。

2.在新展开的部分中，右键单击Certificate Templates文件夹，然后选择New > Certificate Template to Issue。

3.在新窗口中，选择在上一节中创建的证书模板的名称，然后选择确定。

CA现在已准备好促成请求。

步骤 3：下载并签署CSR

1.登录您的Umbrella Dashboard(https://dashboard.umbrella.com)。

2.导航到部署>配置>根证书。

3.选择角的添加(+)图标，并在新窗口中命名您的CA。

4.下载证书签名请求(CSR)。

5.在新浏览器选项卡中，导航到Active Directory证书服务的Web服务。(如果您使用本地计算机，则为127.0.0.1/certsrv/或类似。)

6.在新页面中，选择请求证书。

7.选择高级证书请求。

8.在已保存请求下，复制并粘贴您在第4步中下载的CSR的内容（必须使用文本编辑器将其打开）。

9.在Certificate Template下，选择您在“Preparing AD Certificate Services Template”部分创建的证书模板的名称，然后选择Submit。

10.请务必选择Base64 Encoded，然后选择Download Certificate，并记录.cer文件的位置。

步骤 4：上传已签名的CSR（和公共根证书）

1.在Umbrella Dashboard上，导航到Deployment > Configuration > Root Certificate。

2.选择您在上一部分步骤3中创建的根证书。

3.选择行右下角的Upload CA*。

4.选择top Browse按钮(证书颁发机构(签名CSR))。

5.浏览到在上一节中创建的.cer文件的位置，然后选择保存。

6.选择Next并选择您希望证书与一起使用的计算机/用户组（而不是Cisco根证书），然后选择Save。

*您也可以选择上传CA证书。可以从证书颁发机构服务器的Web界面(http://127.0.0.1/certsrv/)中检索此证书，然后选择下载CA证书、证书链或CRL。在Base 64中完成屏幕提示以“下载CA证书”。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。