生成Cisco UCCE网站服务的SHA-256自署名的认证

Contents

[Introduction](#)
[问题](#)
[解决方案](#)
[WebSetup和CCE管理的解决方案](#)
[诊断的框架门廊的解决方案](#)
[验证](#)
[相关条款](#)

Introduction

本文描述生成自署名的认证的进程使用SHA-256认证Cisco Unified Contact Center Enterprise (UCCE)网站服务的签名算法类似Web设置或CCE管理。

问题

Cisco UCCE有Microsoft互联网信息服务(IIS)服务器主机的几个网站服务。在UCCE配置的默认情况下Microsoft IIS以SHA-1认证签名算法使用自署名的认证。

SHA-1算法由大多浏览器认为不安全的，因此重要工具类似Supervisor的CCE管理用于代理程序reskilling可能变得未提供。

解决方案

对该问题的解决方案将生成IIS服务器的SHA-256证书能使用。

> **警告：**推荐使用认证机关签名的证书。因此应该考虑生成被描述的自署名的认证这里作为临时应急方案迅速恢复服务。

> **Note**:万一ICM Internet脚本编辑器应用程序使用远程脚本管理有需要使用Ssl encryption工具生成它的认证。

WebSetup和CCE管理的解决方案

1. 启动在UCCE服务器的Windows PowerShell工具。

2. 在PowerShell请键入命令

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
```

```
"cert:\LocalMachine\My"
```
那里在**DnsName以后的**参数将指定认证共同名称(CN)。在DnsName以后替换参数到正确一个服务器的。认证将生成与一年正确性。

Note:在认证的普通的名字必须匹配服务器的完全合格的域名(FQDN)。

3. 打开微软管理控制台(MMC)工具。选择**文件**- >Add/**去除卡扣式…**- >请选择**证书**，选择**计算机帐户**并且**添加**它到所选的SNAP INS。按ok，然后连接对**Console Root > Certificates (Local Computer) > Personal > Certificates**。

保证新建立的认证存在这里。认证不会有被配置的友好名称，因此可以根据其CN和有效期被认可。

友好名称可以分配到认证通过选择认证**属性**和填装**友好名称**文本框用适当的名称。

4. 开始互联网信息服务(IIS)管理器。选择IIS默认网站，并且在右窗格请选择**捆绑**。选择**HTTPS** - > Edit和从SSL认证列表挑选自已签署的SHA-256生成的证书。

5. 重新启动“Web发布服务”服务。

诊断的框架门廊的解决方案

1. 重复步骤1-3。

一新的自签证书将生成。对于门廊工具有捆绑认证另一个方式。

2. 去除门廊工具的当前认证捆绑。

```
cd c:\icm\serviceability\diagnostics\bin

DiagFwCertMgr /task:UnbindCert
```
3. 捆绑为门廊生成的自签证书。

打开为门廊工具生成的自签证书并且选择**Details选项**。复制Thumbprint值到文本编辑。

Note:在一些文本编辑thumbprint以问号自动地前缀。去除它。

从thumbprint删除所有空格符并且请使用它在以下命令。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<thumbprint-value>
```
4. 保证认证捆绑使用此命令是成功的。

```
DiagFwCertMgr /task:ValidateCertBinding
```
在输出中应该显示相似的消息。
“认证捆绑是有效的”

5. 重新启动诊断的框架服务。

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

验证

清除浏览器高速缓存和历史记录。访问CCE管理服务网页，并且您应该获得自签证书警告。

查看证书详细信息并且保证认证有SHA-256认证签名算法。

相关条款

生成UCCE诊断的门廓工具的CA签名的证书

生成UCCE Web设置的CA签名的证书

使用CLI，生成VOS基于服务器的CA签名的证书

生成CVP OAMP服务器的CA签名的证书