生成Cisco UCCE网站服务的SHA-256自签名证书

目录

简介

本文描述生成自签名证书进程使用SHA-256证书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

思科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部署的默认情况下Microsoft IIS以SHA-1证书签名算法使用自签名证书。

SHA-1算法由大多浏览器认为不安全的，因此关键工具类似Supervisor的CCE管理用于代理程序reskilling可能变得不可用。

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证书。因此应该考虑生成描述的自签名证书此处作为临时应急方案迅速恢复服务。

WebSetup和CCE管理的解决方案

1. 启动Windows在UCCE服务器的PowerShell工具。

2. 在PowerShell类型命令

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
"cert:\LocalMachine\My"
```

那里在**DnsName以后的**参数将指定证书共同名称(CN)。在DnsName以后替换参数到正确一个服务器的。证书将生成与一年正确性。

> **注意**：在证书的公用名称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/**删除管理单元...**- >请选择**证书**，选择**计算机帐户**并且**添加**它到选定SNAP INS。按ok，然后导航对**Console Root > Certificates (Local Computer) > Personal > Certificates**。

保证新建立的证书存在这里。证书不会有配置的友好名称，因此可以根据其CN和有效期被认可。

友好名称可以分配到证书通过选择证书**属性**和填装**友好名称**文本框用适当的名称。

4. 启动互联网信息服务(IIS)管理器。挑选IIS默认网站和在右窗格选择**捆绑**。挑选**HTTPS** - > Edit和从SSL证书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。

注意：没有需要解开或绑定在Ssl encryption工具工具的证书。

诊断框架门廊的解决方案

1. 重复步骤1-3。

一新的自签名证书将生成。对于门廊工具有另一个方式绑定证书。

2. 删除为门廊工具绑定的当前证书。

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

DiagFwCertMgr /task:UnbindCert
```

3. 绑定为门廊生成的自签名证书。

打开为门廊工具生成的自签名证书并且选择**详细信息选项卡**。复制Thumbprint值对文本编辑。

注意：在一些文本编辑thumbprint以一个问号自动地前缀。删除它。

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. 保证证书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。
“证书捆绑有效”
5. 重新启动诊断框架服务。

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

验证

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

查看证书详细信息并且保证证书有SHA-256证书签名算法。

相关条款

生成UCCE诊断门廊工具的CA签名证书

生成UCCE Web设置的CA签名证书

使用CLI，生成VOS基于服务器的CA签名证书

生成CVP OAMP服务器的CA签名证书