与CA签名的多服务器主题替代名称配置示例的Unified通信团星设置

目录

简介

本文描述如何设置与使用的一Unified通信团星Certificate Authority (CA) -签字的多服务器主题替代名称(SAN)。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)
- CUCM IM和在线状态版本10.5

在您尝试此配置前，请保证这些服务是上和工作：

- Cisco平台管理网站服务
- Cisco Tomcat服务

为了验证在Web接口的这些服务，请导航对**Cisco Unified维护性页Services>网络服务>选择服务器**。为了验证他们在CLI，请输入**使用情况服务列表**命令。

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。

背景信息

在CUCM版本10.5和以上，此托拉斯存储证书签名请求(CSR)请求能包括SAN和备选域。

1. Tomcat
2. Cisco CallManager (CCM)
3. Cisco Unified在线状态可扩展消息传送和在线状态协议(CUP-XMPP)
4. 服务器对服务器的CUP-XMPP (S2S)

更加简单获取在此版本的一个CA签发的证书。仅一个CSR要求由CA签字而不是需求从每个服务器节点获取CSR然后获取每个CSR的一个CA签发的证书和单个管理他们。

配置

1. 登录操作系统(OS)管理并且导航对**安全> Certificate Management >生成CSR**。

2. 选择在分配的**多服务器SAN**。

   它autopopulates SAN域和父域。

   一旦它生成，这显示：

   在证书管理方面， SAN请求生成：

3. 您能使用本地CA或外部CA类似Verisign为了获得它签字。此示例显示Microsoft Windows基于服务器的CA的配置步骤。

   登录https:// <windowsserveripaddress>/certsrv/

   Select请求**证书>Advanced证书请求**。

4. 提交CSR请求如显示此处。

5. 一旦获取证书，您必须上传CA证书作为Tomcat托拉斯然后上传CA签发的证书作为Tomcat。

6. 保证服务重新启动在SAN列表的所有节点，包括节点它上传。您看到在证书管理方面列出的多服务器SAN。

验证

登录http://<fqdnofccm>:8443/ccmadmin为了保证使用新证书。

CallManager多服务器的SAN证书

一种相似的做法可以为CallManager证书被仿效。在这种情况下， autopopulated域是所有CallManager节点。如果它不运行，您能选择从SAN列表保持它或从那里删除它。

在您安装CA后发出的证书，您必须重新启动在所有节点的CallManager服务。

在您获得CUCM的前CA签名的SAN证书，请保证那：

- IP电话能委托托拉斯验证服务(TV)。如果访问从电话的任何HTTPS服务这可以验证。例如，如果公司目录访问工作，然后意味着电话委托TV服务。
- 如果它是一安全集群，请保证证书信任列表(CTL)客户端被重新运行，以便一个新的CTL文件创建，并且集群重新启动。

故障排除

这些日志应该帮助Cisco技术支持中心识别与多服务器SAN CSR CA签名的Certficate生成和加载涉及的所有问题。

- Cisco Unified OS平台API
- Cisco Tomcat
- IPT平台CertMgr日志

在一现有多服务器的Certifcate CUCM，如果服务器的主机名更改，推荐生成一多服务器的SAN CSR请求如以前解释为了获得证书签字由CA。