

# 为CallManager实施多SAN Tomcat证书的重复使用

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[重用CallManager的Tomcat证书](#)

[验证](#)

---

## 简介

本文档介绍在CUCM上如何为CallManager重复使用Multi-SAN Tomcat证书的分步过程。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器 (CUCM)
- CUCM证书
- 身份信任列表(ITL)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM版本15 SU1

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。

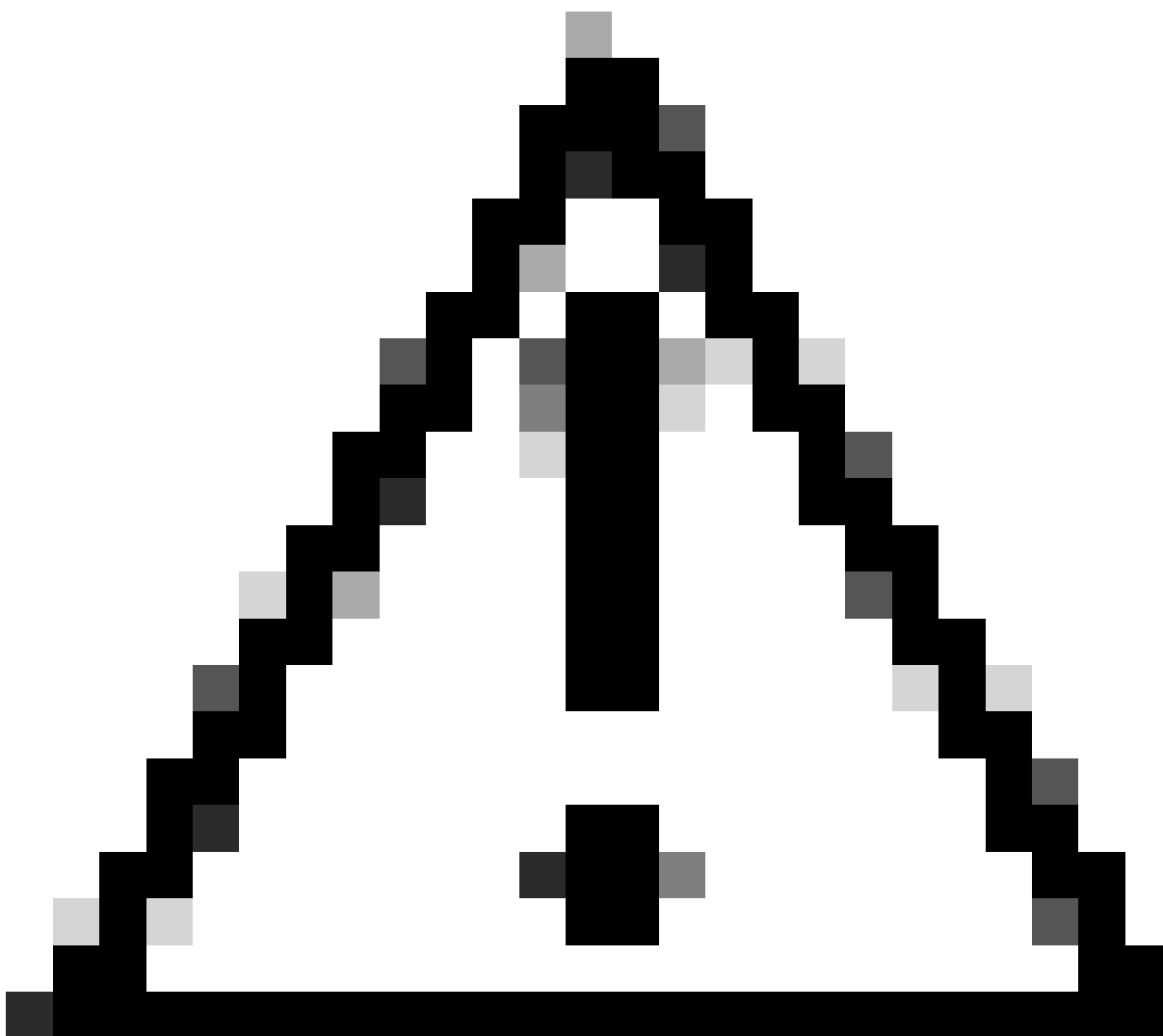
## 背景信息

CUCM的早期版本对完整集群的每个服务使用不同的证书，这增加了证书数量和成本。这包括Cisco Tomcat和Cisco CallManager，它们是在CUCM上运行的重要服务，也具有各自的身份证书。

从CUCM版本14开始，添加了一项新功能，可重用Multi-SAN Tomcat证书用于CallManager服务。

使用此功能的好处是您可以从CA获取一个证书并将其用于多个应用。这确保了成本优化和管理的减少，并减少了ITL文件的大小，从而减少了开销。

---

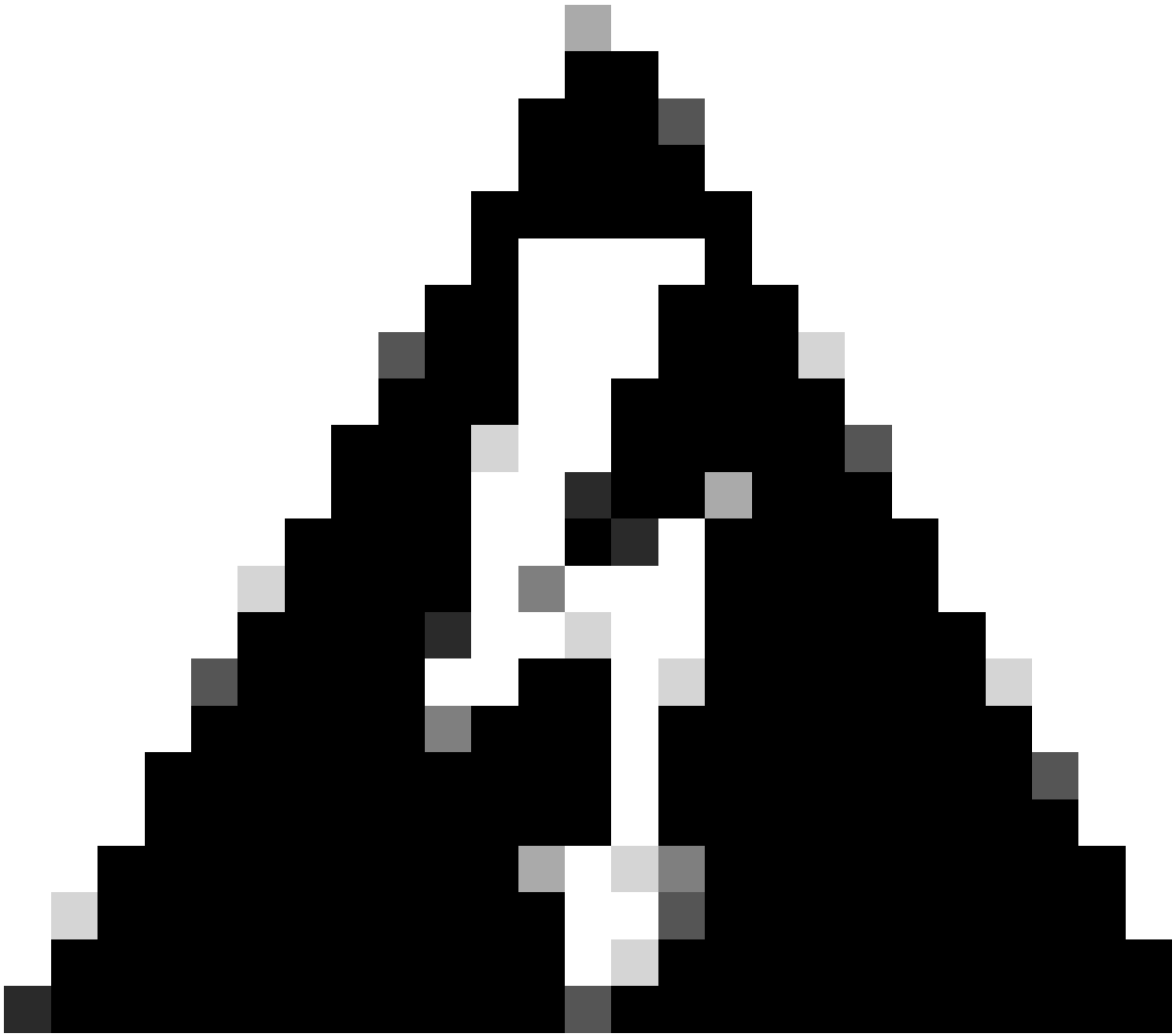


注意：在继续进行重新使用配置之前，请确保Tomcat证书是多服务器SAN证书。Tomcat Multi-SAN证书可以是自签名证书或CA签名证书。

---

## 配置

重用CallManager的Tomcat证书



**警告：**继续之前，请确保已确定集群处于混合模式或非安全模式。

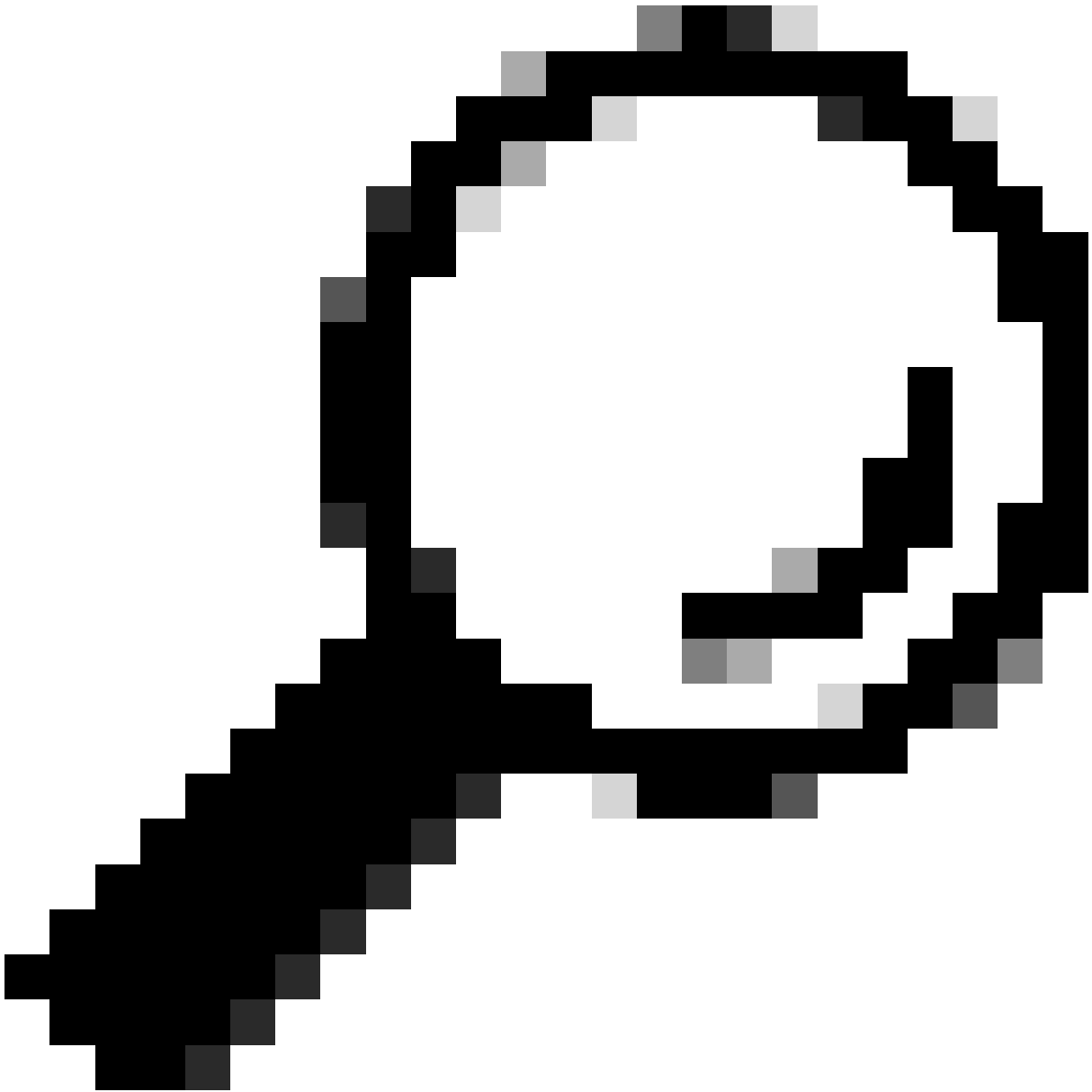
---

**步骤1:**导航到Cisco Unified CM管理>系统>企业参数：

检查Security Parameters部分，并验证Cluster Security Mode设置为0还是1。如果值为0，则集群处于非安全模式。如果值为1，则集群处于混合模式，您需要在重新启动服务之前更新CTL文件。

**第二步：**导航到您的CUCM发布者，然后导航到思科统一操作系统管理>安全>证书管理。

**第三步：**将Multi-SAN Tomcat CA Certificate Chain上传到CallManager Trust存储区。



提示：如果要对Tomcat使用自签名多服务器SAN证书，则可以跳过此步骤。

---

在重新使用证书之前，请确保手动将CA证书链（签署tomcat身份证书）上传到CallManager信任库。

将tomcat证书链上传到CallManager信任时，请重新启动这些服务。

- CallManager：思科HAProxy服务
- CallManager-ECDSA：Cisco CallManager服务和Cisco HAProxy服务

第四步：单击Reuse Certificate。系统将显示Use Tomcat Certificates For Other Services页面。

## Use Tomcat Certificate For Other Services



Finish



Close

### Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

### Source

Choose Tomcat Type\*

tomcat



### Replace Certificate for the following purpose



CallManager



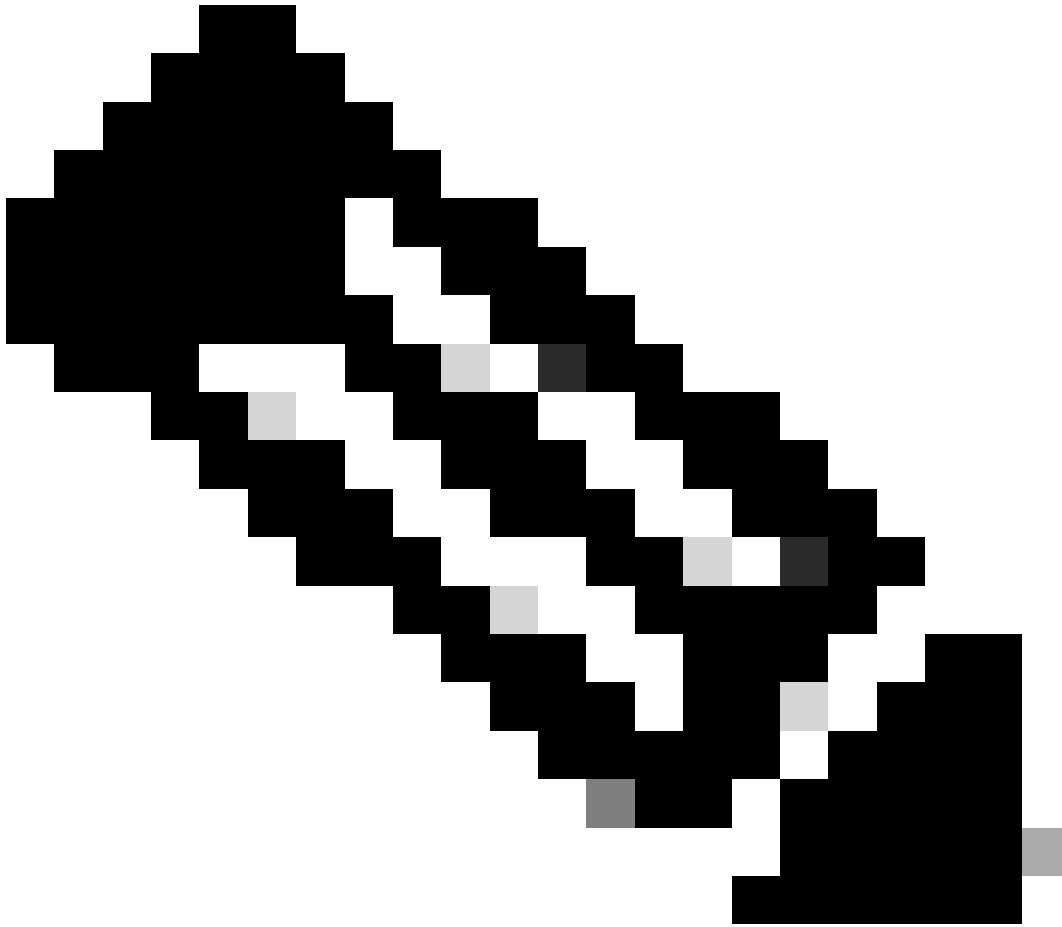
CallManager-ECDSA

Finish

Close

第五步：从Tomcat type下拉列表中选择Tomcat或Tomcat-ECDSA。



第六步：在Replace Certificate for the following purpose窗格中，根据之前步骤中选择的证书选中CallManager或CallManager-ECDSA复选框。



注意：如果选择Tomcat作为证书类型，则会启用CallManager作为替换。如果选择tomcat-ECDSA作为证书类型，则会启用CallManager-ECDSA作为替换。




步骤 7.单击完成将CallManager证书替换为tomcat多服务器SAN证书。

**Use Tomcat Certificate For Other Services**

 Finish  Close

---

**Status**

-  Certificate Successful Provisioned for the nodes cucmpub15. \_\_\_\_\_ ,cucmsub15. \_\_\_\_\_ .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

步骤 8通过CLI执行utils service restart Cisco HAProxy命令，在集群的所有节点上重新启动Cisco HAProxy服务。

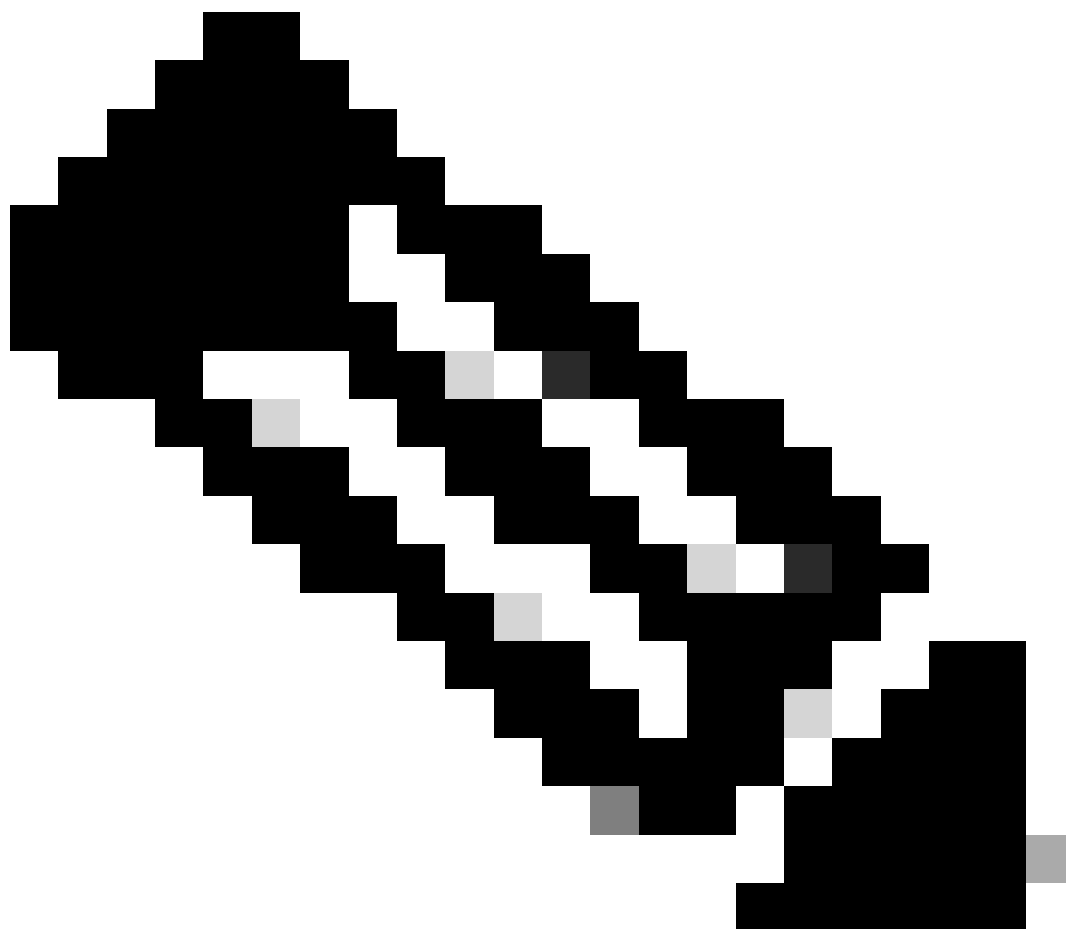
```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin:█
```

步骤 9 如果集群处于混合模式，请通过CUCM发布方的CLI运行命令utils ctl update CTLFile更新CTL文件，然后继续重置电话以获取新的CTL文件。

## 验证

---



---

注意：重复使用证书时，CallManager证书不会显示在GUI上。

---

您可以从CLI运行命令以确认CallManager是否重复使用Tomcat证书。

- show cert list own

```
admin:show cert list own  
  
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA  
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
ITLRecovery/ITLRecovery.pem:  
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager  
TVS/TVS.pem: Self-signed certificate generated by system  
  
admin:█
```



## 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）。