使用IOS XE PKI配置CA签名证书

目录

简介

本文档可作为配置由第三方证书颁发机构(CA)签名的IOS XE证书的一般指南。

本文档将详细介绍如何导入多级CA签名链以便设备用作身份(ID)证书，以及如何导入其他第三方证书以进行证书验证。

先决条件

要求

使用IOS PKI功能时，必须配置NTP和时钟时间。

如果管理员不配置NTP，则生成证书时可能会遇到将来日期/过去日期/时间的问题。日期或时间的这种偏差可能导致导入问题和其他问题。

NTP配置示例：

```
ntp server 192.168.1.1
clock timezone EST -5
clock summer-time EDT recurring
```

使用的组件

— 运行Cisco IOS® XE17.11.1a的Cisco路由器

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

请注意，本文档中详细介绍的某些功能在较旧的IOS XE版本中可能不可用。尽可能注意记录何时引入或修改了命令或功能。

请务必参考给定版本的IOS XE PKI功能的官方文档，以了解可能与您的特定版本相关的任何限制或更改：

示例：

- IOS 15 M/T:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-pki-overview.html
- IOS XE 16.12.x:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-12/sec-pki-xe-16-12-book/sec-est-client-supp-pki.html
- IOS XE 17.x:https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-pki-overview-0.html

IOS XE PKI配置

在高级级别，管理员在使用IOS XE PKI证书时必须执行以下操作：

1. 创建用于功能或服务的密钥(加密密钥生成)
2. 使用各种参数配置信任点并链接密钥。(crypto pki trustpoint)
3. 生成证书签名请求(CSR)(crypto pki enroll)
4. 将CSR提供给CA进行签名(本文档未涉及)
5. 对根和/或中间CA证书进行身份验证(crypto pki authenticate)
6. 导入设备证书(crypto pki import)
7. 可选：验证对等CA证书(crypto pki authenticate)

这些步骤将在后续章节中详细介绍，这些章节将按照给定操作所需的命令进行分组。

crypto key generate

许多管理员输入此命令以在路由器上启用安全套接字外壳(SSH)，或作为功能的一些配置指南的一部分。但是，很少有人没有分析该命令的实际功能。

以以下命令为例：

```
crypto key generate rsa general-keys modulus 2048 label rsaKey exportable
crypto key generate ec keysize 521 exportable label ecKey
```

将这些命令细分为特定部分会详细描述其用法：

- black(crypto key generate)命令的第一部分指示路由器我们将创建新密钥。还有其他选项，例如加密密钥导出、加密密钥导入或加密密钥零大小，这些选项将在后面详细介绍。
- 绿色(rsa general-keys， ec)命令的下一部分指示路由器正在创建哪种类型的密钥。在大多数情况下，将使用由公钥/私钥组成的Rivest-Shamir-Adleman(RSA)密钥对，但管理员还可以配置椭圆曲线(EC)，以便使用需要ECDSA证书的功能或用于ECDHE握手的功能。
- 橙色命令定义了密钥的大小。
  - 对于RSA，模数是术语和值，例如512-4096之间的可用选项。默认模数大小因版本而异，但建议遵循思科下一代加密的最佳实践，并使用大于2048的密钥。
  - 对于EC，需要key-size命令来指定密钥中的位数。选项为256、384或512。
- 紫色命令定义此键的标签。这一点很重要，因为管理员可能需要在同一IOS XE设备上为各种目的定义多个密钥。标签用于指定与给定功能一起使用的确切密钥。如果可能，请始终使用标签来区分正在使用的密钥，并更轻松地为功能分配密钥。例如：标签SSH、标签CUBE、标签HTTPS将创建两个用于不同服务或功能的密钥。
  - 密钥的默认标签是设备hostname.domain。某些设备可能会在首次启动时生成RSA密钥。如果不输入标签后修复，管理员可能会面临无意中覆盖/重新生成错误密钥的风险
- 最后一条蓝色命令是可导出后缀。此命令详细说明了密钥可以与crypto pki export命令一起使用，以便导出并与其他系统一起使用。例如，可以导入到对等高可用性设备中，以便一个高可用性对的两个成员都使用单个密钥，或者在故障排除工具（如Wireshark）中使用单个密钥解密基于RSA的TLS会话。无论出于何种原因必须说明RSA密钥只能从一开始就作为可导出项创建。如果管理员创建了不可导出的RSA密钥，则此密钥不能设置为可导出密钥而不重新生成密钥，这可能会对其他功能产生涟漪效应，例如使使用该密钥创建的所有证书失效。也就是说，通过使用命令crypto key move rsaKeyLabel non-exportable，可以将可导出密钥降级为不可导出，而无需重新生成密钥

配置示例:

<#root>

```
Router(config)#
```

crypto key generate rsa general-keys modulus 2048 label rsaKey exportable

```
The name for the keys will be: rsaKey

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)

Router(config)#

crypto key generate ec keysize 521 exportable label ecKey

The name for the keys will be: ecKey
```

验证示例：

<#root>

```
Router#

show crypto key mypubkey rsa rsaKey

% Key pair was generated at: 10:21:42 EDT Apr 14 2023
Key name: rsaKey
Key type: RSA KEYS      2048 bits
 Storage Device: not specified
 Usage: General Purpose Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  [..truncated..]
  9F020301 0001

Router#

show crypto key mypubkey ec ecKey

% Key pair was generated at: 10:03:05 EDT Apr 14 2023
Key name: ecKey
Key type: EC KEYS      p521 curve
 Storage Device: private-config
 Usage: Signature Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30819B30 1006072A 8648CE3D 02010605 2B810400 23038186 000401A2 A77FCD34
  [..truncated..]
  93FAC967 96ADA79E 4A245881 B2AD2F4A 279A362D F390A20F C06D5845 06DA
```

crypto pki trustpoint

信任点是“类似文件夹”的概念，用于在IOS XE中存储和管理PKI证书。(命令语法)

在较高层面上：

1. 每个IOS XE信任点可以包含通过crypto pki authenticate命令加载的单个根或中间CA证书。将经过身份验证的信任点视为添加设备现在信任的证书。
2. 每个IOS XE信任点还可以通过crypto pki import命令导入加载的单个身份(ID)证书。ID证书是

通常绑定到某些服务或功能的设备证书。

3. 管理员可以在同一信任点上使用authenticate和import命令（这是导入ID证书所必需的，将在稍后讨论。）使用身份验证/导入工作流程时，信任点将包含两个证书（根/中间+身份证书）。
4. 当信任点用于仅存储受信任的对等根/中间CA证书时 crypto pki authenticate 命令是必需的。在这种情况下，信任点将仅包含由管理员进行身份验证的单个证书。

注意：即将出现的有关crypto pki authenticate和crypto pki import的部分以及后面详细介绍多级证书的身份验证/导入示例的部分将提供这四条项目的进一步上下文。

信任点可以配置各种命令。这些命令可能会影响由设备在信任点上使用crypto pki enroll命令创建的证书签名请求(CSR)中的值。

信任点有许多不同的命令可供使用（数量过多，本文档无法详细说明），但下面的信任点示例和表格中详细介绍了一些更常见的示例：

```
crypto pki trustpoint labTrustpoint
 enrollment terminal pem
 serial-number none
 fqdn none
 ip-address none
 subject-name cn=router.example.cisco.com
 subject-alt-name myrouter.example.cisco.com
 revocation-check none
 rsakeypair rsaKey
 hash sha256
```

命令	描述
crypto pki trustpoint labTrustpoint	此信任点的可读配置标签。用于链接到后来的命令中的功能或服务。
注册终端PEM	确定crypto pki enroll命令将执行的操作。 在本示例中，enrollment terminal pem指示证书签名请求(CSR)将以Base64 PEM格式文本输出到终端。 其他选项(例如enrollment selfsigned)可用于创建自签名证书，或者enrollment url可配置为定义HTTP URL并利用简单证书注册协议(SCEP)协议。这两种方法都不在本文档的讨论范围之内。
serial-number none	确定是否将IOS XE设备串行添加到

	CSR。这也会在crypto pki enroll命令期间禁用提示。
fqdn none	确定是否将完全限定域名(FQDN)添加到CSR。这也会在crypto pki enroll命令期间禁用提示。
ip-address none	确定是否将IOS XE设备IP地址添加到CSR。这也会在crypto pki enroll命令期间禁用提示。
subject-name cn=router.example.cisco.com	指示将添加到CSR的X500格式化。
subject-alt-name myrouter.example.cisco.com	从IOS XE 17.9.1开始，主题备用名称(SAN)值的逗号分隔列表可以添加到CSR。
revocation-check none	指示IOS XE设备应如何检查证书的有效性。如果选择的证书颁发机构支持证书撤销列表(CRL)、在线证书状态协议(OCSP)，则可以使用这些选项。这主要用于信任点被其他已配置的IOS XE功能或服务使用时。使用信任点对证书进行身份验证时，也会检查吊销状态。
rsakeypair rsaKey	指示命令使用此特定标签的RSA密钥对。 对于ECDSA证书，使用引用EC密钥标签的命令“eckeypair ecKey”
hash sha256	此命令影响要使用的散列算法的类型。选项包括SHA1、SHA256、SHA384、SHA512

crypto pki enroll

crypto pki enroll命令用于在给定信任点上触发enrollment命令。(命令语法)
对于之前显示的示例信任点，命令crypto pki enroll labTrustpoint将以Base64 PEM文本格式向终端显示证书签名请求(CSR)，如下例所示。

现在，此证书签名请求可以保存在文本文件中，也可以从命令行进行复制和粘贴，以便提供给任何第三方CA进行验证和签名。

```
<#root>

Router(config)#

crypto pki enroll labTrustpoint

% Start certificate enrollment ..

% The subject name in the certificate will include: cn=router.example.cisco.com
```

```
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwIzEhMB8GA1UEAxMYcm91dGVyLmV4YW1wbGUuY2lzY28uY29t
[..truncated..]
mGvBGUpn+cDIdFcNVzn8LQk=
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---
```

crypto pki authenticate

crypto pki authenticate命令用于向给定信任点添加受信任CA证书。每个信任点可以进行一次身份验证。也就是说，信任点只能包含一个CA根证书或中间证书。再次运行该命令并添加新证书将覆盖第一个证书。

配置了enrollment terminal pem命令后，crypto pki authenticate命令将提示路由器通过CLI上传Base64 PEM格式的证书。(命令语法)

管理员可以对信任点进行身份验证，以便在证书链中添加根证书和可选的中间证书，以便以后导入设备的ID证书。

管理员还可以验证信任点，以将其他受信任根CA添加到IOS XE设备，以便在与该对等设备进行协议握手期间启用与对等设备的信任关系。

为了进一步说明，对等设备可能使用由“根CA 1”签名的证书链。为了在IOS XE设备和对等设备之间的协议握手期间成功进行证书验证，管理员可以使用crypto pki authenticate命令将CA证书添加到IOS XE设备上的信任点。

需要记住的主要事项：使用crypto pki authenticate对信任点进行身份验证始终用于将CA根或中间证书添加到信任点；不用于添加身份证书。请注意，此概念也适用于对来自其他对等设备的自签名证书进行身份验证。

以下示例展示如何使用crypto pki authenticate命令对来自早期的信任点进行身份验证：

<#root>

```
Router(config)#
```

crypto pki authenticate labTrustpoint

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
       Fingerprint MD5: C955FC74 7AABC184 D8A75DE7 3C9E7218
      Fingerprint SHA1: 3A99FF61 1E9E6C7B D0E567A9 96D882F5 2279C534

% Do you accept this certificate? [yes/no]:

yes

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

crypto pki import

此命令用于将身份(ID)证书导入信任点。单个信任点只能包含一个ID证书，再次发出命令将提示覆盖以前导入的证书。 (命令语法)

以下示例展示如何使用crypto pki import命令将身份证书从之前导入到示例信任点。

```
<#root>

Router(config)#

crypto pki import labTrustpoint certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

如果管理员在信任点验证用于直接签署此证书的CA证书之前尝试导入证书，则会收到错误消息。

```
<#root>

Router(config)#

crypto pki import labTrustpoint certificate

% You must authenticate the Certificate Authority before
 you can import the router's certificate.
```

验证对等CA证书

使用添加任何CA证书的相同方法将对CA证书添加到IOS XE。也就是说，使用crypto pki authenticate命令根据信任点对它们进行身份验证。

以下命令显示如何创建信任点和验证对等第三方CA证书。

1. 首先创建具有描述性名称的信任点，该名称将保存对等CA证书
2. 配置enrollment terminal pem，以便crypto pki authenticate命令通过命令行请求证书。
3. 配置revocation-check none以在导入过程中跳过CRL/OCSP检查
4. 验证信任点并提供证书
5. 按照对等CA证书的要求对重复步骤1-4（请记住每个信任点仅有一个CA证书！）

<#root>

```
Router(config)#
crypto pki trustpoint PEER-ROOT
Router(ca-trustpoint)#
enrollment terminal pem
Router(ca-trustpoint)#
revocation-check none


Router(ca-trustpoint)#
crypto pki authenticate PEER-ROOT

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: 62D1381E 3E03D06A 912BAC4D 247EEF17
      Fingerprint SHA1: 3C97CBB4 491FC8D6 3D12B489 0C285481 64198EDB

% Do you accept this certificate? [yes/no]:
yes

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

对一个或多个中间证书进行身份验证

前面的示例详细说明了如何使用crypto pki enroll生成CSR，使用crypto pki authenticate对根CA证书进行身份验证，然后使用crypto pki import导入身份证书。
但是，引入中间证书时，过程略有不同。别害怕，相同的概念和命令仍然适用！区别在于持有证书的信任点的分配方式。

请记住，每个信任点只能包含单个根或中间CA证书。因此，在如下所示的CA链下方的示例中，无法使用crypto pki authenticate命令添加多个CA证书：

<#root>

- Root CA

 - Intermediate CA 1

   - Identity Certificate

解决方案：

1. 创建一个信任点，用于保存经过身份验证的根CA。
2. 然后，使用用于创建CSR的信任点验证中间证书
3. 最后，将身份证书导入到最终信任点。

使用下表，您可以用与前一个链对应的颜色说明证书到命令到信任点的映射，从而帮助实现可视化。

证书名称	要使用的信任点	应使用的命令
根 CA	crypto pki trustpoint ROOT-CA	crypto pki authenticate ROOT-CA
中间CA 1	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份证书	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

相同的逻辑可以应用于具有两个中间CA证书的证书链。同样，提供颜色以帮助直观显示新中间CA应用到IOS XE配置的位置。

<#root>

- Root CA

 - Intermediate CA 1

 - Intermediate CA 2

 - Identity Certificate

证书名称	要使用的信任点	应使用的命令
根 CA	crypto pki trustpoint ROOT-	crypto pki authenticate ROOT-CA

	CA	
中间CA 1	crypto pki trustpoint INTER-CA	crypto pki authenticate INTER-CA
中间CA 2	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份证书	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

仔细观察就会发现两种模式：

1. 所有根或中间证书使用crypto pki authenticate加载到信任点（无论有多少根或中间证书）。
2. 您还可以注意到，设备身份证书（读取直接签署身份证书的证书）之前的最终证书始终在要导入身份证书的同一信任点上进行身份验证。
    - 与前面显示的错误类似，IOS XE不会允许管理员在未经验证用于直接签署此证书的CA证书之前导入证书。

以上两种模式可用于两个以上的任意数量的中间证书，尽管在大多数部署中，管理员在证书链中可能看到两个以上的中间CA。

为完整起见，还提供以下根/身份证书表：

<#root>

```
- Root CA
```

<#root>

```
 - Identity Certificate
```

证书名称	要使用的信任点	应使用的命令
根 CA	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份证书	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

确认

- 在身份验证或导入过程中，IOS XE会执行各种健全性检查，以确保证书有效且格式正确。这些错误将打印到屏幕上，或日志(show logging)查找以“CRYPTO_PKI”开头的行

下面详细介绍一些常见示例：

根据配置的时间与证书中找到的时间执行有效之前/之后检查

<#root>

```
004458:
Aug  9
 21:05:34.403: CRYPTO_PKI: trustpoint labTrustpoint authentication status = 0
%CRYPTO_PKI: Cert not yet valid or is expired -
    start date: 05:54:04 EDT
Aug 29
 2019
    end   date: 05:54:04 EDT Aug 28 2022
```

如果未禁用revocation-check，IOS XE将在导入证书之前通过配置的方法执行撤销检查

```
<#root>
003375: Aug  9 20:24:14:
%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint ROOT failed
003376: Aug  9 20:24:14.121:
CRYPTO_PKI: enrollment url not configured
```

要查看有关经过身份验证或导入的信任点配置的详细信息，请使用以下命令：

```
show crypto pki trustpoints trustpoint_name
show crypto pki certificates trustpoint_name
show crypto pki certificates verbose trustpoint_name
```

故障排除

当调试导入问题或其他PKI问题时，使用以下调试。

```
debug crypto pki messages
debug crypto pki transactions
debug crypto pki validation
debug crypto pki api
debug crypto pki callback
!
debug ssl openssl error
debug ssl openssl msg
debug ssl openssl states
debug ssl openssl ext
```

高级IOS PKI概念

导入PKCS12格式的证书

某些CA提供程序可能会以PKCS#12格式(.pfx、.p12)提供回文件。

PKCS#12是一种特殊类型的证书格式，其中从根证书到身份证书的整个证书链与rsa密钥对一起捆绑。

此格式非常便于使用IOS XE进行导入，并且可以使用以下命令轻松导入：

<#root>

```
Router(config)#
```

crypto pki import PKCS12-TP pkcs12 terminal password Cisco123

or

```
Router(config)#
```

crypto pki import PKCS12-TP pkcs12 ftp://cisco:cisco@192.168.1.1/certificate.pfx password Cisco123

```
% Importing pkcs12...
Address or name of remote host [192.168.1.1]?
Source filename [certificate.pfx]?
Reading file from ftp://cisco@192.168.1.1/certificate.pfx!
[OK - 2389/4096 bytes]
% You already have RSA keys named PKCS12.
% If you replace them, all router certs issued using these keys
% will be removed.
% Do you really want to replace them? [yes/no]:
```

yes

```
CRYPTO_PKI: Imported PKCS12 file successfully.
```

导出PKCS12或PEM证书

管理员可以将证书以Base64纯文本PEM、Base64加密纯文本或PKCS12格式导出到终端，以导入到其他对等设备。

这在启动新的对等设备时非常方便，并且管理员需要共享签署设备身份证书的根CA证书。

以下是一些示例语法：

<#root>

```
Router(config)#
```

crypto pki export labTrustpoint pem terminal

```
Router(config)#
crypto pki export labTrustpoint pem terminal 3des password Cisco!123
Router(config)#
crypto pki export labTrustpoint pkcs12 terminal password cisco!123
```

导出RSA密钥

可能需要导出RSA密钥，以便导入到其他设备或用于故障排除工作。假设密钥对创建为可导出的，可以使用crypto key export命令以及加密方法(DES、3DES、AES)和密码导出密钥。

示例用法：

<#root>

```
Router(config)#
crypto key export rsa rsaKey pem terminal aes Cisco!123
% Key name: IOS-VG
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

base64 len 1664-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,40E087AFF0886DA7C468D2084A0DECFB

[..truncated..]
-----END RSA PRIVATE KEY-----
```

如果密钥无法导出，则会显示错误。

<#root>

```
Router(config)#
crypto key export rsa kydavis.cisco.com pem terminal 3des mySecretPassword

% RSA keypair kydavis.cisco.com' is not exportable.
```

Import RSA Keys generated off-box

某些管理员可能会在出厂时执行RSA和证书创建，因此可以使用crypto key import命令导入RSA密钥，如下所示，请使用密码进行导入。

<#root>

```
Router(config)#
```

crypto key import rsa rsaKey general-purpose exportable terminal mySecretPassword

```
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9E31AAD9B7463502
[..truncated..]
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

删除RSA密钥

使用命令crypto key zeroize rsa rsaKey删除名为rsaKey的RSA密钥对。

通过Trustpool导入思科受信任CA捆绑包

信任池与信任点略有不同，但核心使用相同。信任点通常包含单个CA证书时，信任池将包含多个受信任CA。

思科发布CA捆绑包，网址为https://www.cisco.com/security/pki/

一个常见用法是使用以下命令下载ios_core.p7b文件：

<#root>

```
Router(config)#
```

crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b

```
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
Router(config)#
```

常见问题解答

删除信任点是否会使CSR或从给定CSR授予的证书链失效？

否，生成并保存CSR后，可以在不使CSR无效的情况下删除并重新添加信任点。

当验证/导入证书出错时，思科技术支持经常使用此选项重新开始验证。

只要管理员或支持工程师不重新生成RSA密钥，即可导入CSR或签名证书链进行身份验证/导入。

重要！删除信任点将删除任何经过验证/导入的证书，如果这些证书当前正由某些服务或功能使用，则可能会产生更大的问题。

在信任点上生成CSR是否会使现有证书失效？

否，当证书即将到期时，这种情况很常见。管理员可以执行crypto pki enroll命令以创建新的CSR并使用CA开始证书签名过程，同时已验证/导入的现有证书仍在使用中。管理员使用crypto pki authenticate/crypto pki import替换证书的时间就是替换旧证书的时刻。

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）。