调整Cisco IOS XE SD-WAN边缘上的默认SSH RSA密钥的大小

目录

简介

本文档介绍如何在Cisco IOS® XE SD-WAN边缘上将用于安全协议的默认SSH RSA密钥长度增加至更长的长度。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- SSH密钥和证书基本操作
- RSA算法

使用的组件

- 思科IOS® XE Catalyst SD-WAN边缘17.9.4a

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

Secure Shell(SSH)是一种网络协议，它允许用户即使在未受保护的网络中也能建立到设备的远程连接。该协议使用基于客户端 — 服务器架构的标准加密机制来保护会话。

RSA是Rivest 、 Shamir 、 Adleman :使用两个密钥的加密算法（公钥加密系统）：公钥和私钥，也称为密钥对。公共RSA密钥是加密密钥，专用RSA密钥是解密密钥。

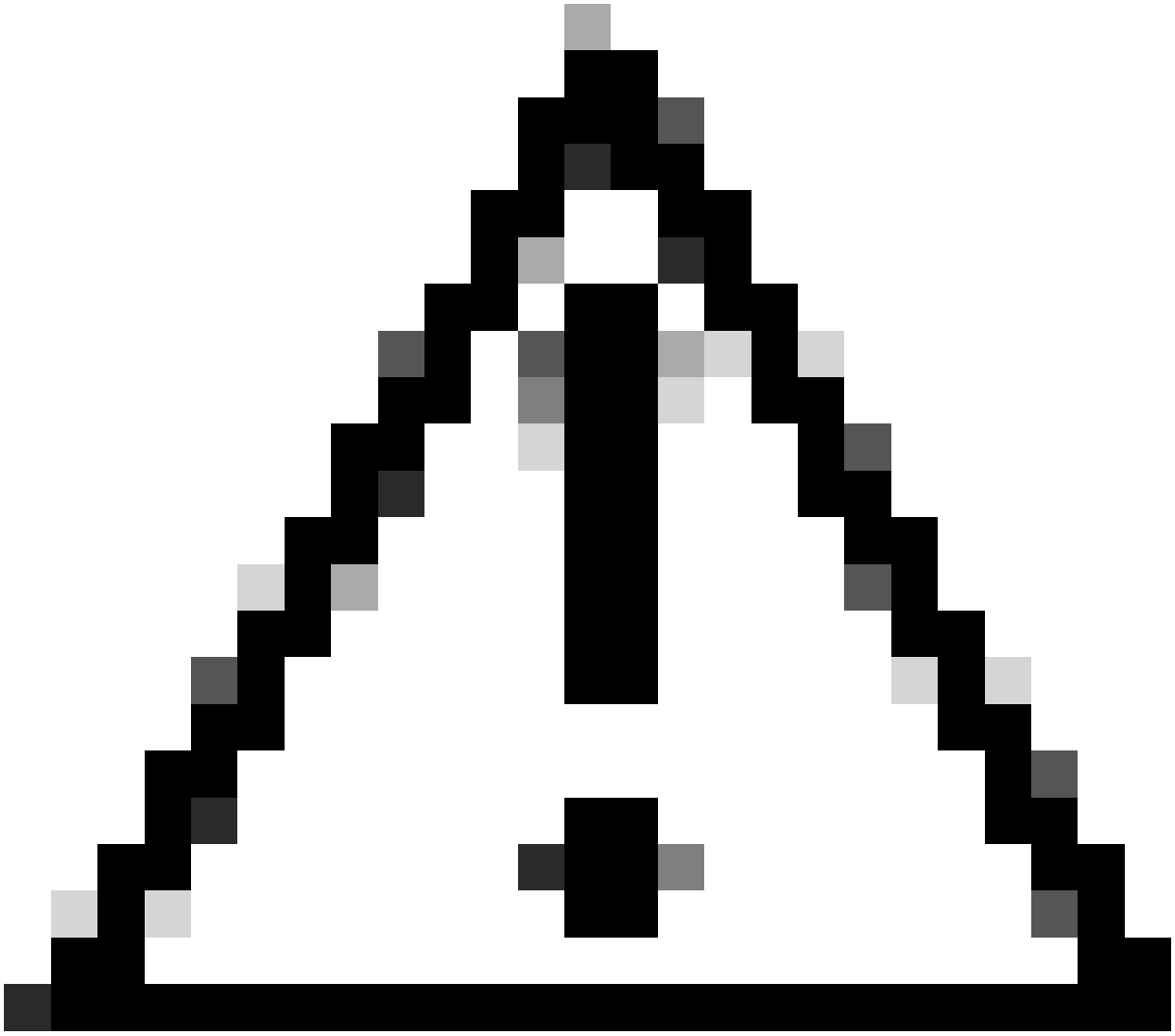
RSA密钥具有定义的模数长度（以位为单位）。当RSA密钥的长度为2048位时，实际上意味着模数值介于22047和22048之间。由于给定对的公钥和私钥共享相同的模数，因此根据定义，它们的长度也相同。

信任点证书是自签名证书，因此称为信任点，因为它不依赖于任何其他方或其他方的信任。

Cisco IOS公共密钥基础设施(PKI)提供证书管理以支持安全协议，例如IP安全(IPSec)、安全外壳(SSH)和安全套接字层(SSL)。

SSH RSA密钥在Cisco Catalyst SD-WAN上非常重要，因为SSH协议使用它们来建立SD-WAN Manager和SD-WAN Edge设备之间的通信，因为SD-WAN Manager使用Netconf协议，通过SSH来管理、配置和监控设备。

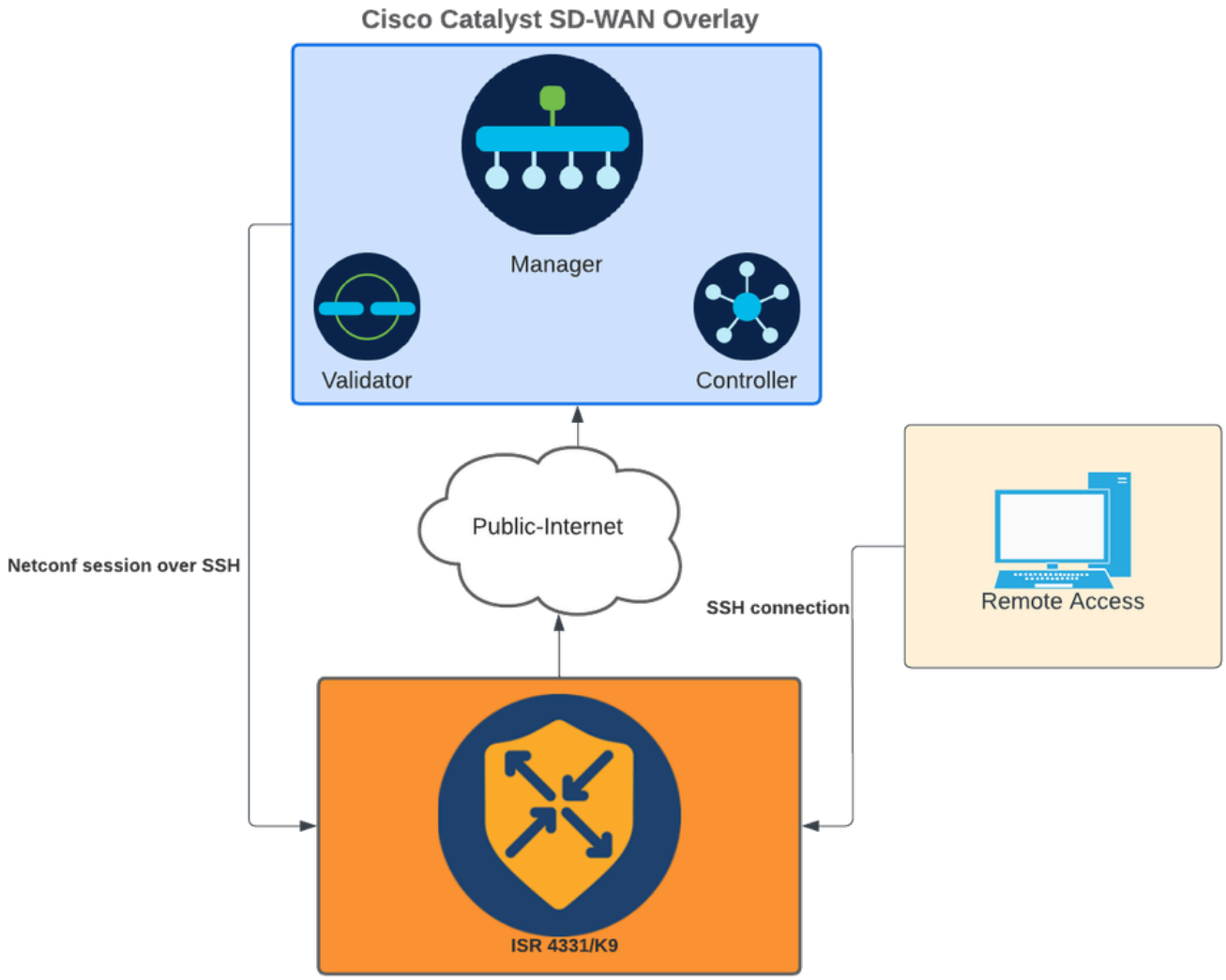
因此，有必要始终同步和更新密钥。如果通过合规性和审核，需要修改密钥长度以实现安全性，则需要完成本文档中介绍的过程，调整密钥大小并在证书上正确同步密钥，以避免SD-WAN Manager和SD-WAN Edge设备之间断开连接。



警告：请完成此过程的所有步骤，以避免丢失对设备的访问权限。如果设备处于生产状态，则建议在维护窗口中执行，并允许通过控制台访问设备。

配置

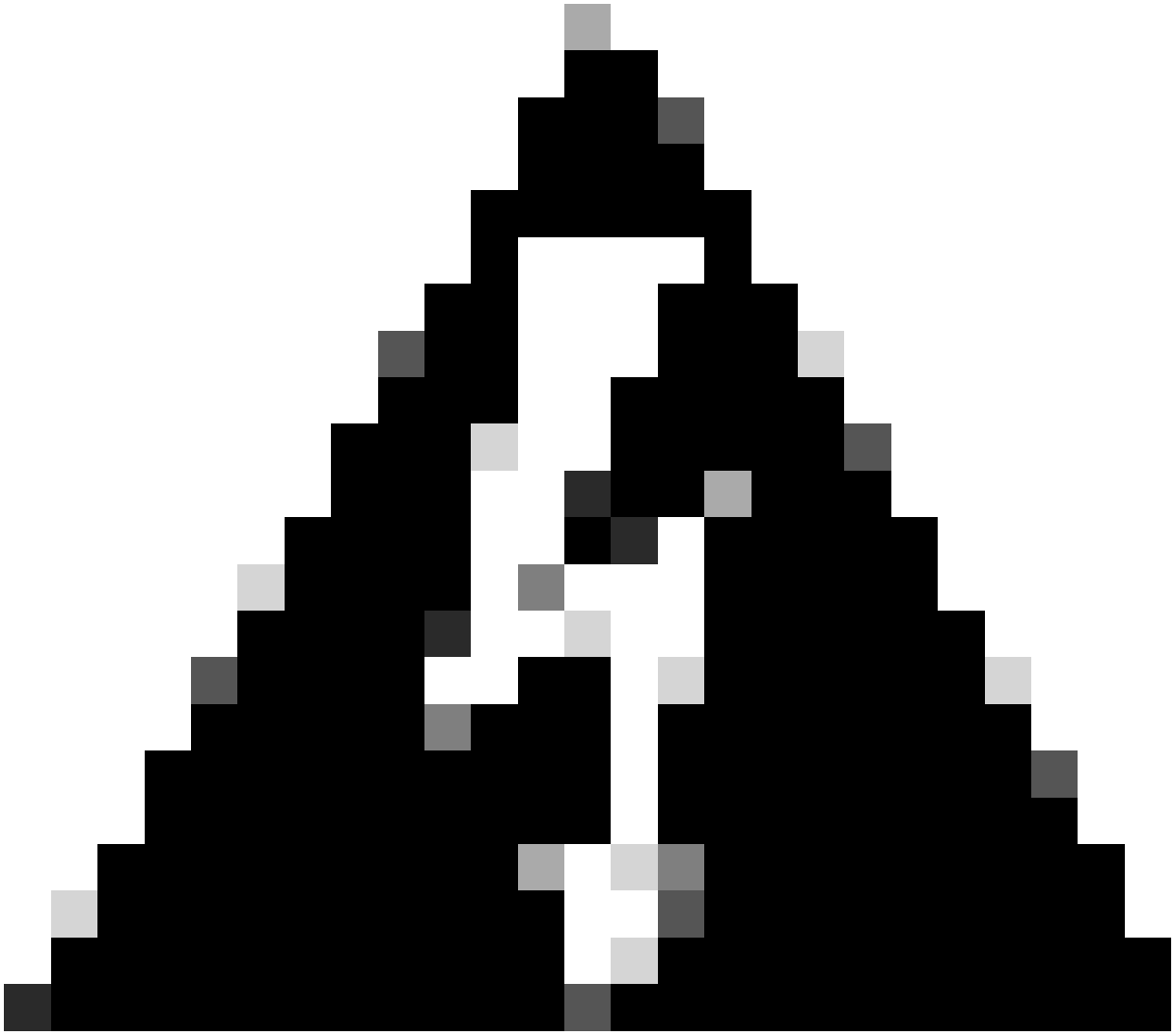
网络图



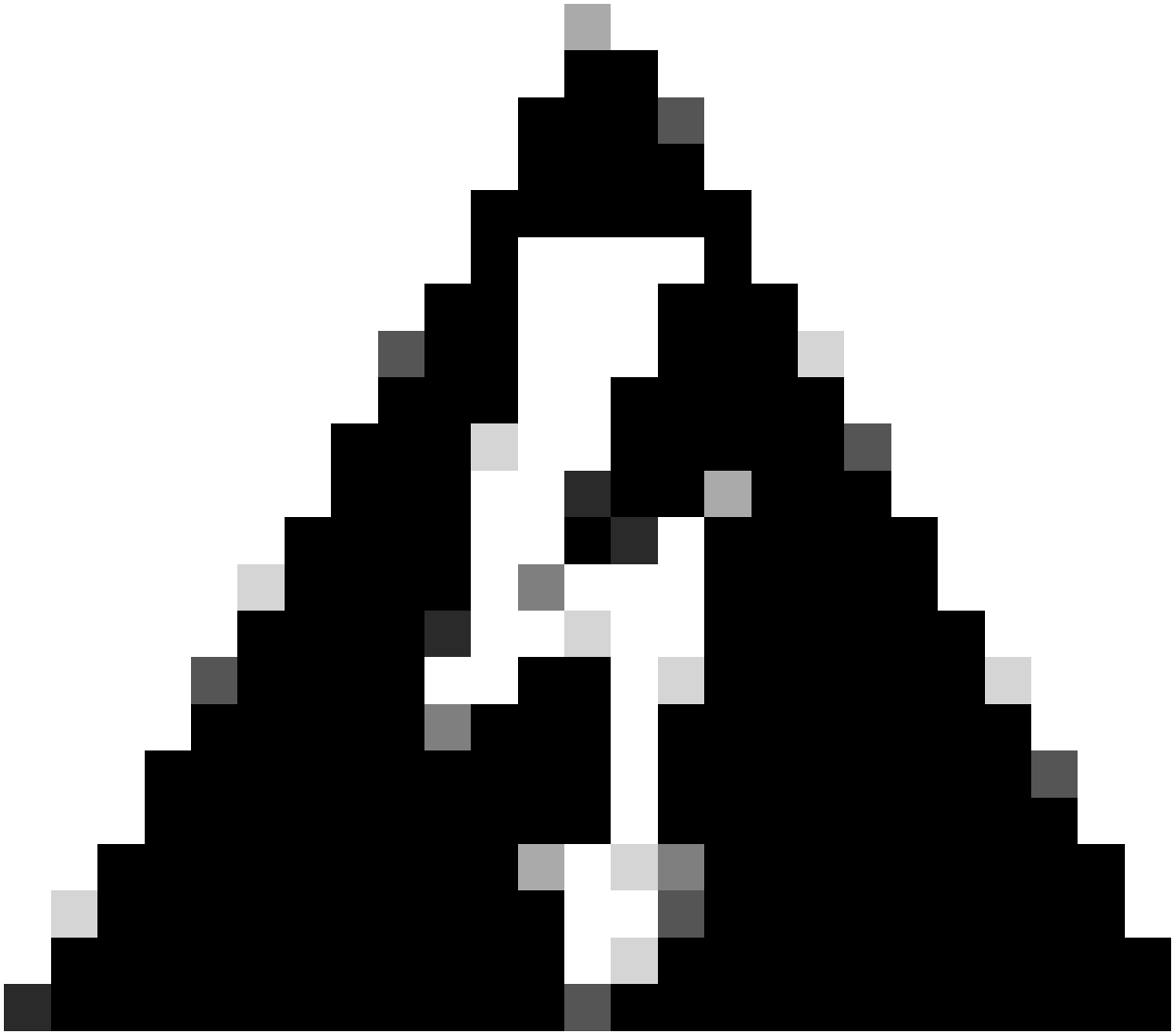
网络图

配置

广域网边缘设备中的RSA密钥只能使用命令行界面(CLI)进行修改；CLI附加功能模板不能用于更新密钥。



警告：建议使用控制台完成此过程，因为SD-WAN Manager SSH工具在该过程完成之前不可用。



警告：此过程需要重新启动设备。如果设备处于生产状态，则建议在维护窗口中执行，并允许通过控制台访问设备。如果没有控制台访问，将另一个远程访问协议临时配置为telnet。

此配置示例显示如何删除RSA 2048和使用RSA 4096密钥。

1 — 获取当前的SSH密钥名称。

<#root>

Device#

show ip ssh

```
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecds
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
```

```
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
```

TP-self-signed-1072201169 <<<< RSA Key Name

Modulus Size : 2048 bits

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDZ5urq7f/X+AZJjUnMOdF9pLX+VOjPR8arK6bLSU7d
iGeSDDwW2MPNck/U5HBry9P/L4nKyZ1oevAhfy7cJVVmoHD41NQW9wb/hLtimuujnRRYkKuIWLmoI7AH
y6YQoetew8XVglVIjva+JzQ5ZX1JGm8AzN6a95RbRNhGRzgz9cTFmD7m6ArIKZPMyYQabXfrY+m/HuQ2
aytbHtJMgmOQk2fLPakO3PnQNYXpiDP3CmOEh3LJg82FZQ1eohmhm+mAInwU4mlLHUouigyBuq1KEBVe
z3vxjB9X8rGF3qzUcx2lpHmhXaNPXWen2QQbyfAIDo8WXVoff24uLYlwCVkv
```

2 — 获取当前信任点自签名证书。

<#root>

```
Device#
```

show crypto pki trustpoint

Trustpoint TP-self-signed-1072201169: <<<< Self-signed Trustpoint name

```
Subject Name:
cn=IOS-Self-Signed-Certificate-1072201169
Serial Number (hex): 01
Persistent self-signed certificate trust point
Using key label
```

TP-self-signed-1072201169

两个值名称必须匹配。

3 — 删除当前密钥。

<#root>

```
Device#
```

crypto key zeroize rsa

4 — 验证旧密钥已成功删除。

<#root>

Device#

show ip ssh

5 — 生成新密钥。

<#root>

Device#

crypto key generate rsa modulus 4096 label

```
The name for the keys will be: TP-self-signed-1072201169
% The key modulus size is 4096 bits
% Generating crypto RSA keys in background ...
*Jun 25 21:35:18.919: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been gen
*Jun 25 21:35:18.924: %SSH-5-ENABLED: SSH 2.0 has been enabled
*Jun 25 21:35:23.205: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been gen
*Jun 25 21:35:29.674: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
```

完成此过程可能需要2到5分钟。

6 — 验证生成的新密钥。

<#root>

Device#

show ip ssh

```
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecds
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
```

IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169

Modulus Size : 4096 bits <<<< Key Size

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDEOt/SX3oQKN6z0WvOaFAkMcaZNzQ6JgP+7xjuX143
YS7YGm0PwIPgs8N2LWvmdLXQ/PqsQ0GGsdxo2+2Y/idAFm8O8mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eFO0H1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELBO6yYEipPWMRaZYFfTRbNJm8/7SOJGlFkgFVW5nITTIgISoMV8EJv
bLl8cVgATDb1OckeDb7uU6PDXm3zonmZC0yqHtF1OAOJxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0O49UH0y0bMgPuWrJpwtk1iYA3+t6N/QdlC5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKyvkcqXi6nDfAKb8o+Z8/43xbvWlDIKAuj1rbdyqPAJB4llTZJkOHk8zRP5gZ8u4jTjNKQHb
vNa3ieg4RLEDOx4lqCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOul4YDJYr
D+jnyoZr4PnfWAgk4M9U89deWSlIRPMIXYd35YmLvD6OeQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

现在，将生成新密钥。但是，在删除旧密钥时，Netconf会话正在使用的自签名证书也会从信任点中删除。

<#root>

Device#

sh crypto pki trustpoint status

```
Trustpoint TP-self-signed-1072201169:
Issuing CA certificate configured::
Issuing CA certificate configured:
Subject Name:
cn=Cisco Licensing Root CA,o=Cisco
Fingerprint MD5: 1468DC18 250BDFCF 769C29DF E1F7E5A8
Fingerprint SHA1: 5CA95FB6 E2980EC1 5AFB681B BB7E62B5 AD3FA8B8
State:
```

Keys generated ..... No <<<< Depending on the version, it can erase the key or even that, delete

```
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
```

生成新的4096密钥后，密钥不会在自签证书上自动更新，并且需要完成额外的步骤来更新密钥。

注意：如果仅生成密钥，但未在证书中更新，则SD-WAN Manager会丢失Netconf会话，这可能会中断设备的所有管理活动（模板、配置等）。

生成证书/分配密钥的方法有两种：

1 — 重新加载设备。

<#root>

```
Device#
reload
```

2 — 重新启动HTTP secure-server。仅当设备处于CLI模式时，此选项才可用。

```
<#root>
Device (config)#
no ip http secure-server

Device (config)#
commit

Device (config)#
ip http secure-server

Device (config)#
commit
```

验证

重新加载后，验证新密钥已生成且证书位于具有相同名称的信任点下。

```
<#root>
Device#
 show ip ssh

SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecds
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169

Modulus Size : 4096 bits

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDEOt/SX3oQKN6z0WvOaFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm8O8mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN
```

```
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796cOB1YLtK3eFOOH1AFmFy5ec8Own7ikO
JjKtwEozImFMjHZfUEUjFuhPJELBO6yYEipPWMRaZYFfTRbNJm8/7SOJGlFkgFVW5nITTIgISoMV8EJv
bLl8cVgATDb1OckeDb7uU6PDXm3zonmZCOyqHtF1OAOJxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5etOO49UHOyObMgPuWrJpwtk1iYA3+t6N/QdlC5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKyvkcqXi6nDfAKb8o+Z8/43xbvWlDIKAuj1rbdyqPAJB4llTZJkOHk8zRP5gZ8u4jTjNKQHb
vNa3ieg4RLEDOx4lqCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOul4YDJYr
D+jnyoZr4PnfWAgk4M9U89deWSlIRPMIXYd35YmLvD6OeQ5EQALNiNPUEkpdPKs4orYysEVOpRoY+HQ
```

<#root>

Device#

show crypto pki trustpoint

Trustpoint TP-self-signed-1072201169: <<<< Trustpoint name

Subject Name:
cn=IOS-Self-Signed-Certificate-1072201169
Serial Number (hex): 01
Persistent self-signed certificate trust point

Using key label TP-self-signed-107220116

<#root>

Device#

show crypto pki certificates

Router Self-Signed Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: General Purpose
Issuer:
cn=IOS-Self-Signed-Certificate-1072201169
Subject:
Name: IOS-Self-Signed-Certificate-1072201169
cn=IOS-Self-Signed-Certificate-1072201169
Validity Date:
start date: 21:07:33 UTC Dec 27 2023
end date: 21:07:33 UTC Dec 26 2033

Associated Trustpoints: TP-self-signed-1072201169

Storage: nvram:IOS-Self-Sig#4.cer

确认SD-WAN Manager可以对设备路由器应用配置更改。

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）。