تغيير حجم مفاتيح SSH RSA الافتراضية على حواف Cisco IOS XE SD-WAN

المحتويات

المقدمة

يوضح هذا المستند كيفية زيادة مفاتيح SSH rsa الافتراضية المستخدمة للبروتوكولات الآمنة إلى طول أقوى على حواف Cisco IOS® XE SD-WAN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة منطقة واسعة معرفة ببرنامج Cisco Catalyst (SD-WAN)
- عملية مفاتيح SSH والشهادة الأساسية
- خوارزمية RSA

المكونات المستخدمة

- Cisco IOS® XE Catalyst SD-WAN Edges 17.9.4a

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

Secure Shell (SSH) هو بروتوكول شبكة يسمح للمستخدمين بإنشاء إتصالات عن بعد بالأجهزة حتى عبر شبكة غير محمية. يؤمن البروتوكول الجلسات باستخدام الآليات

المشفرة القياسية استنادا إلى بنية العميل-الخادم.

إن RSA هو نظام تشفير المفتاح العام) التي ريفشتلا ةيمزراوخ :نامدلأ ،ريماش ،ريست لثمي .حيتافملا جوز مساب اضيأ ةفورعملاو ،ةصاخلاو ةماعلا حيتافملا :نيحاتفم مدختست ريفشتلا كف حاتفم صاخلا RSA حاتفم لثمي امنيب ريفشتلا حاتفم ماعلا RSA حاتفم.

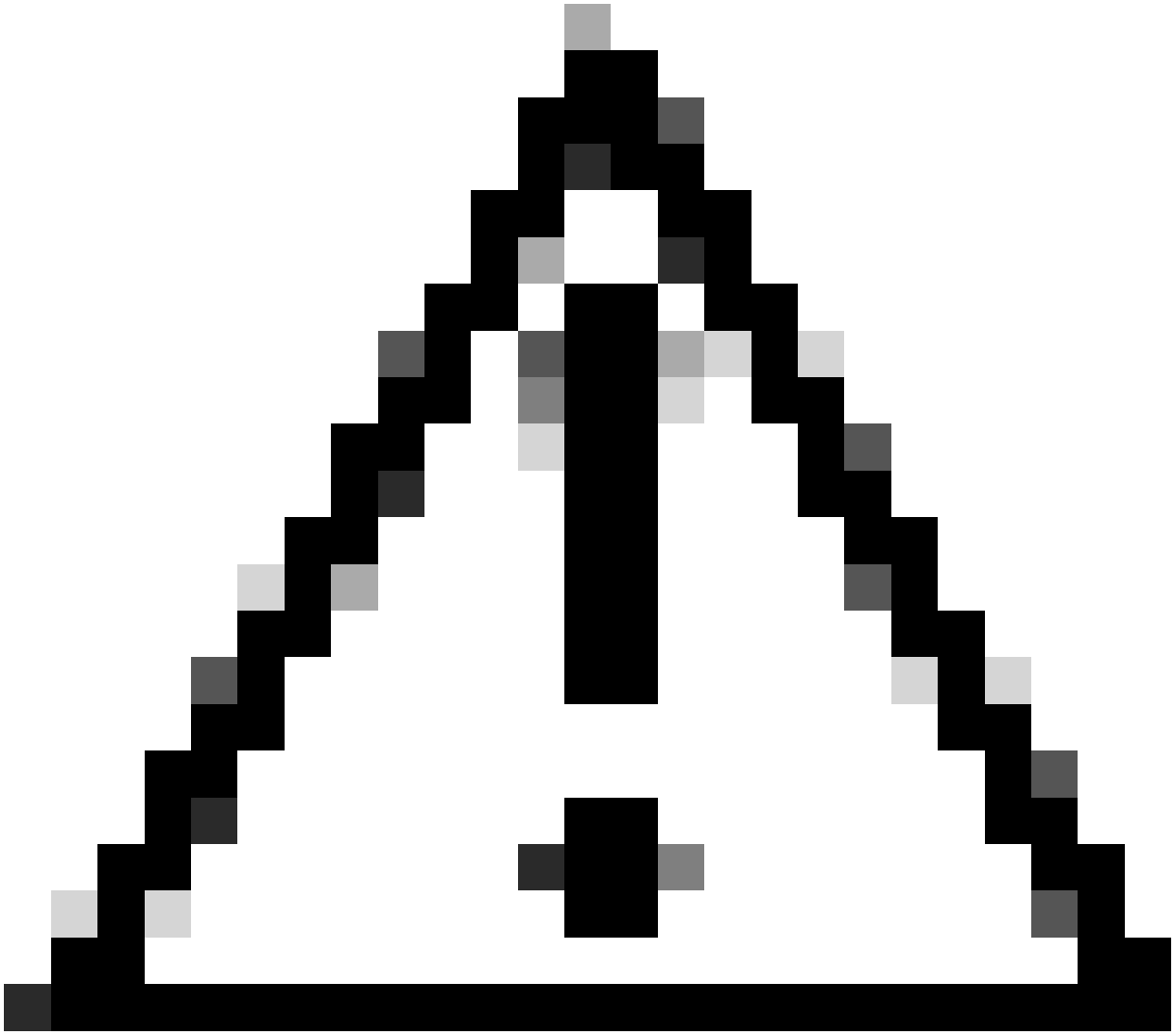
يكون مفاتيح RSA لوط مرعف ،في وحدات ،تب للماعلا. عندما يقال ان مفتاح RSA له لوط 2048 ،تب يعني ذلك حقا ان قيمة المعامل تقع بين 22047 و 22048. وبما ان المفاتيح العامة والخاصة لزوج معين تتشارك في المعامل نفسه، فهي تمتلك أيضا، بحكم التعريف، الطول نفسه.

إن شهادة TrustPoint هي شهادة موقعة ذاتيا، وبالتالي هي TrustPoint، لأنها لا تعتمد على ثقة أي شخص آخر أو طرف آخر.

معدل الشهادة إدارة Cisco من IOS عبر نظام إدارة المفتاح العام (PKI) للمفاتيح الأساسية البنية توفر لبروتوكولات الأمان مثل أمان IP (IPSec) وبروتوكول Secure Shell (SSH) وطبقة مآخذ التوصيل الآمنة (SSL).

تدعم مفاتيح SSH RSA مهمة على بروتوكول Cisco Catalyst SD-WAN لأنها تستخدم بواسطة بروتوكول SSH لإنشاء الاتصال بين برنامج SD-WAN Manager وأجهزة SD-WAN Edge، نظرا لأن برنامج SD-WAN Manager يستخدم بروتوكول NetConf، الذي يعمل عبر SSH لإدارة الأجهزة وتكوينها ومراقبتها.

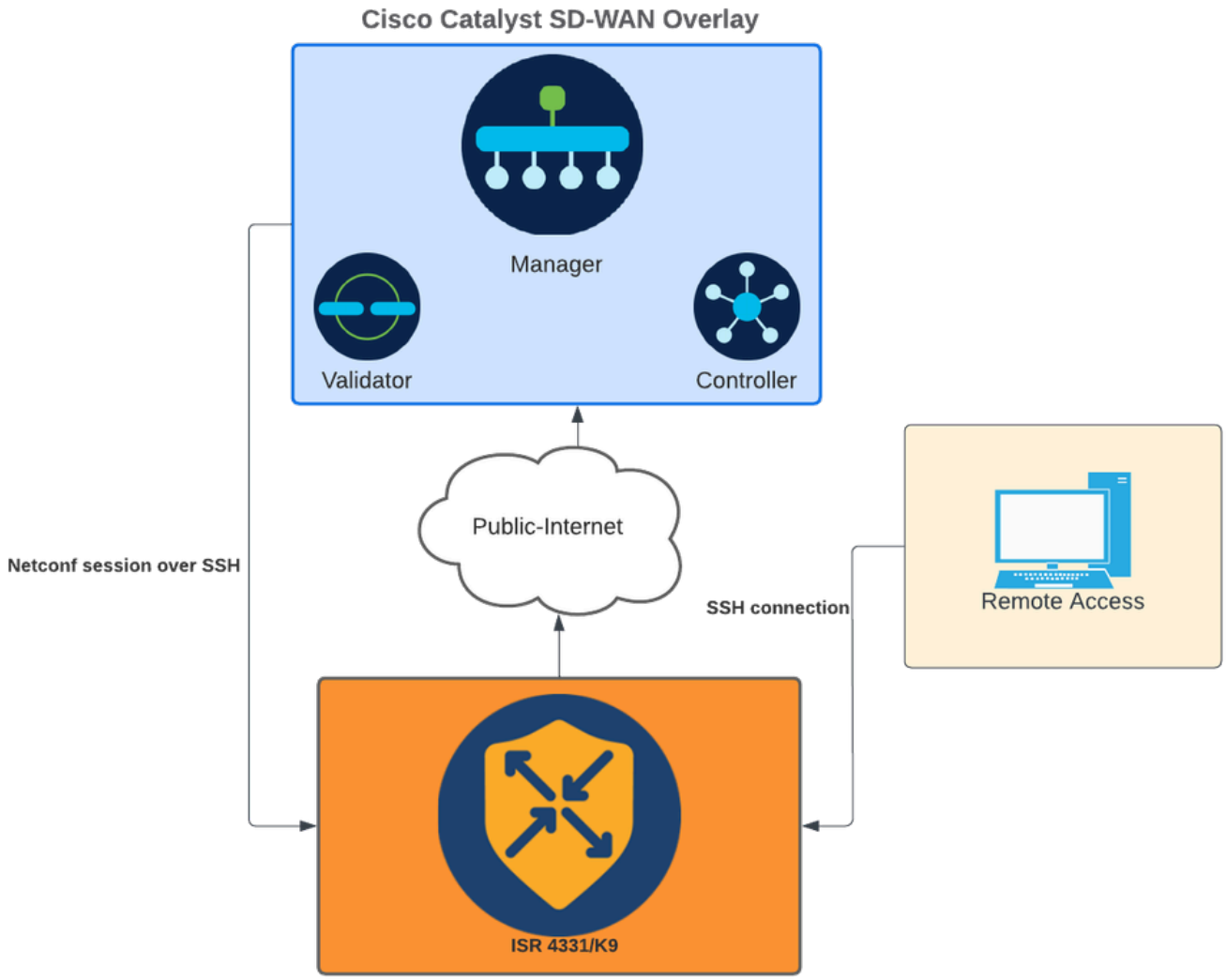
ونظرا لهذه الحقيقة، من الضروري مزامنة المفاتيح وتحديثها طوال الوقت. إذا كانت هناك حاجة إلى تعديل طول المفتاح للأمان عن طريق التوافق والمراجعة، فمن الضروري إكمال العملية على الشهادة بشكل صحيح لتغيير حجم المفاتيح ومزامنتها في هذا المستند الموضح لتجنب قطع الاتصال بين إدارة SD-WAN وأجهزة حافة SD-WAN.



تحذير: الرجاء إكمال كافة الخطوات في العملية لتجنب فقدان الوصول إلى الجهاز. إذا كان الجهاز قيد الإنتاج، فمن المستحسن إجراؤه في نافذة الصيانة والوصول إلى وحدة التحكم إلى الجهاز.

التكوين

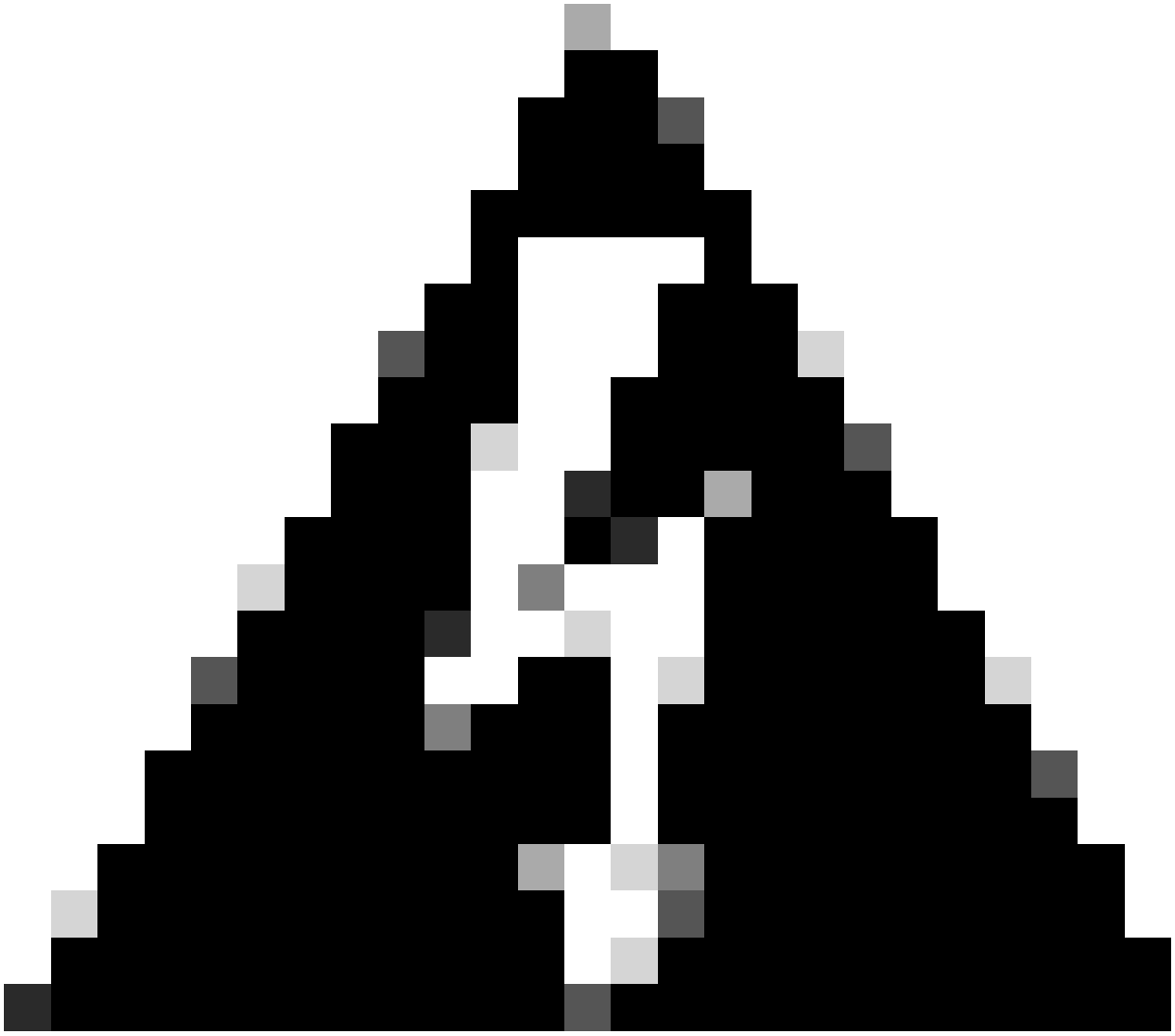
الرسم التخطيطي للشبكة



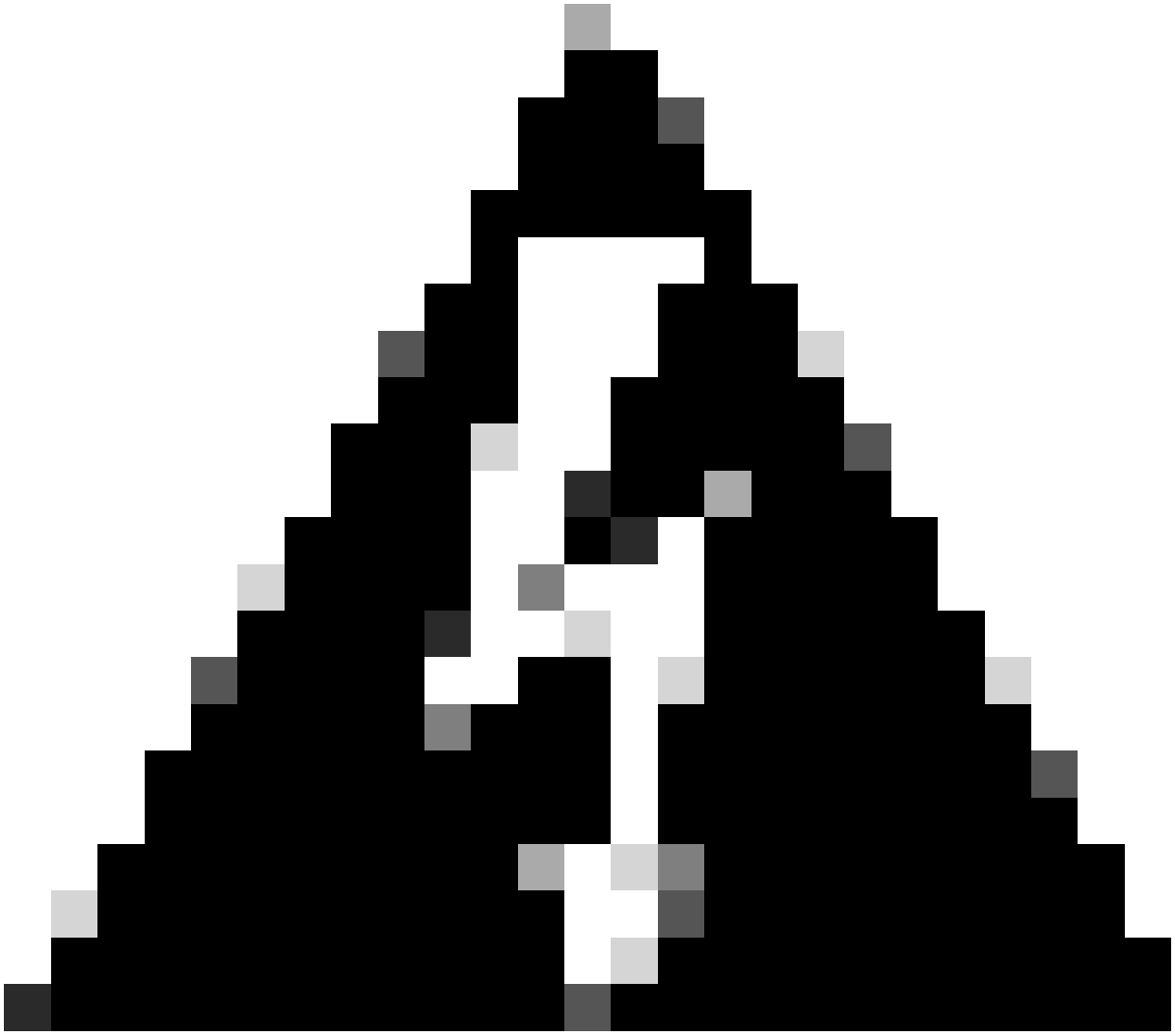
الرسم التخطيطي للشبكة

التكوينات

يمكن تعديل مفاتيح RSA في أجهزة حافة شبكة WAN فقط باستخدام واجهة سطر الأوامر (CLI)؛ لا يمكن إستخدام قوالب ميزة ميزة ميزة ميزة CLI الإضافية لتحديث المفاتيح.



تحذير: يوصى بإجراء العملية باستخدام وحدة التحكم حيث أن أداة SD-WAN Manager SSH غير متوفرة حتى انتهاء العملية.



تحذير: تتطلب هذه العملية إعادة تشغيل الجهاز. إذا كان الجهاز قيد الإنتاج، فمن المستحسن إجراؤه في نافذة الصيانة والوصول إلى وحدة التحكم إلى الجهاز. إذا لم يكن هناك وصول إلى وحدة التحكم، فقم بتكوين بروتوكول وصول عن بعد آخر بشكل مؤقت كبرنامج Telnet.

يوضح مثال التكوين هذا كيفية إزالة RSA 2048 واستخدام مفتاح RSA 4096.

1 - احصل على اسم مفتاح SSH الحالي.

<#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 - الحصول على الشهادة الحالية الموقعة ذاتيا لنقطة الثقة.

<#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

يجب أن يتطابق كل من اسمي القيمة.

3 - حذف المفتاح الحالي.

<#root>

```
Device#
```

crypto key zeroize rsa

4 - التحقق من صحة حذف المفاتيح القديمة بنجاح.

```
<#root>

Device#

show ip ssh
```

5 - إنشاء المفاتيح الجديد.

```
<#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
```

قد تستغرق هذه العملية من دقيقتين إلى 5 دقائق لإكمالها.

6 - التحقق من صحة المفاتيح الجديد الذي تم إنشاؤه.

```
<#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
```

الآن، يتم إنشاء مفتاح جديد. ومع ذلك، في اللحظة التي تم فيها حذف المفتاح القديم، يتم أيضا حذف الشهادة الموقعة ذاتيا والمستخدمة من قبل جلسات عمل NetConf من TrustPoint.

<#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
```

بمجرد إنشاء المفتاح الجديد 4096، الذي تم تحديث المفاتيح تلقائيا على الشهادة الموقعة ذاتيا، ومن الضروري إكمال خطوات إضافية لتحديثه.

ملاحظة: في حالة إنشاء المفاتيح فقط، ولكن لم يتم تحديثه في الشهادة، تفقد إدارة SD-WAN جلسات عمل NetConf، ويمكن أن يؤدي ذلك إلى تقسيم جميع أنشطة الإدارة إلى الجهاز (القوالب والتكوين وما إلى ذلك).

هناك طريقتان لإنشاء الشهادة/تعيين المفاتيح:

1 - إعادة تحميل الجهاز.

```
<#root>

Device#

reload
```

2 - إعادة تشغيل خادم HTTP الآمن. الا يتاح هذه الخيار إلا إذا كان الجهاز في وضع CLI.

```
<#root>

Device (config)#

no ip http secure-server

Device (config)#

commit

Device (config)#

ip http secure-server

Device (config)#

commit
```

التحقق من الصحة

بعد إعادة التحميل، تحقق من إنشاء المفاتيح الجديد ومن أن الشهادة تحت TrustPoint بنفس الاسم.

```
<#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/SX3oQKN6zOWvOaFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm8O8mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eFOOH1AFmFy5ec8Own7ikO
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

تأكد من أنه يمكن لـ SD-WAN Manager تطبيق تغييرات التكوين على موجه الجهاز.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).