StandaardSSH RSA-toetsen aanpassen op Cisco IOS XE SD-WAN randen

Inhoud

Inleiding

Dit document beschrijft hoe u de standaard SSH RSA-toetsen die voor beveiligde protocollen worden gebruikt, kunt verhogen tot een sterkere lengte op Cisco IOS® XE SD-WAN randen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst softwaregedefinieerde Wide Area Network (SD-WAN)
- Basisbediening van SSH-toetsen en -certificaten
- RSA-algoritme

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Secure Shell (SSH) is een netwerkprotocol waarmee gebruikers externe verbindingen met

apparaten kunnen maken, zelfs via een onbeschermd netwerk. Het protocol beveiligt de sessies met behulp van standaard cryptografische mechanismen op basis van een client-serverarchitectuur.

RSA is Rivest, Shamir, Adleman: Encryptiealgoritme (public-key cryptografisch systeem) dat twee toetsen gebruikt: Publieke en privé-sleutel, ook bekend als sleutelpaar. De Public RSA-sleutel is de coderingssleutel en de Private RSA-sleutel is de decryptiesleutel.

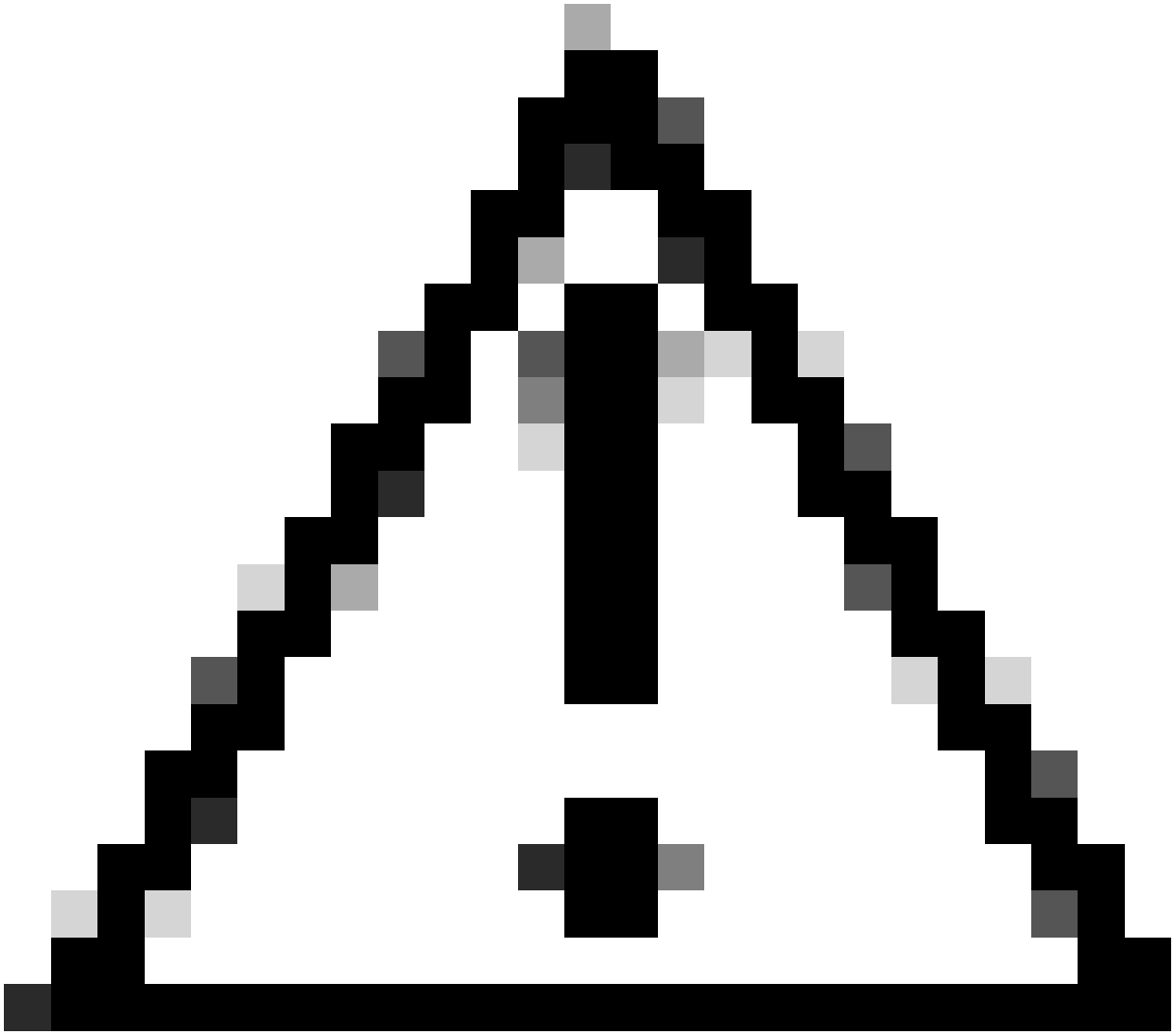
RSA-toetsen hebben een bepaalde lengte, in bits, van de modulus. Als een RSA-toets een lengte heeft van 2048 bits, betekent dat echt dat de modulus-waarde tussen 22047 en 22048 ligt. Omdat de openbare en particuliere sleutels van een gegeven paar dezelfde modulus delen, hebben ze per definitie ook dezelfde lengte.

Een trustpoint certificaat is een zelfondertekend certificaat, vandaar de naam trustpoint, aangezien het zich niet baseert op het vertrouwen van iemand anders of andere partij.

Cisco IOS public key infrastructure (PKI) biedt certificaatbeheer ter ondersteuning van beveiligingsprotocollen zoals IP Security (IPSec), Secure Shell (SSH) en Secure Socket Layer (SSL).

SSH RSA-toetsen zijn belangrijk op Cisco Catalyst SD-WAN omdat ze worden gebruikt door het SSH-protocol om de communicatie tussen SD-WAN Manager en SD-WAN Edge-apparaten tot stand te brengen, aangezien SD-WAN Manager gebruik maakt van NetConf-protocol, dat via SSH werkt om apparaten te beheren, configureren en bewaken.

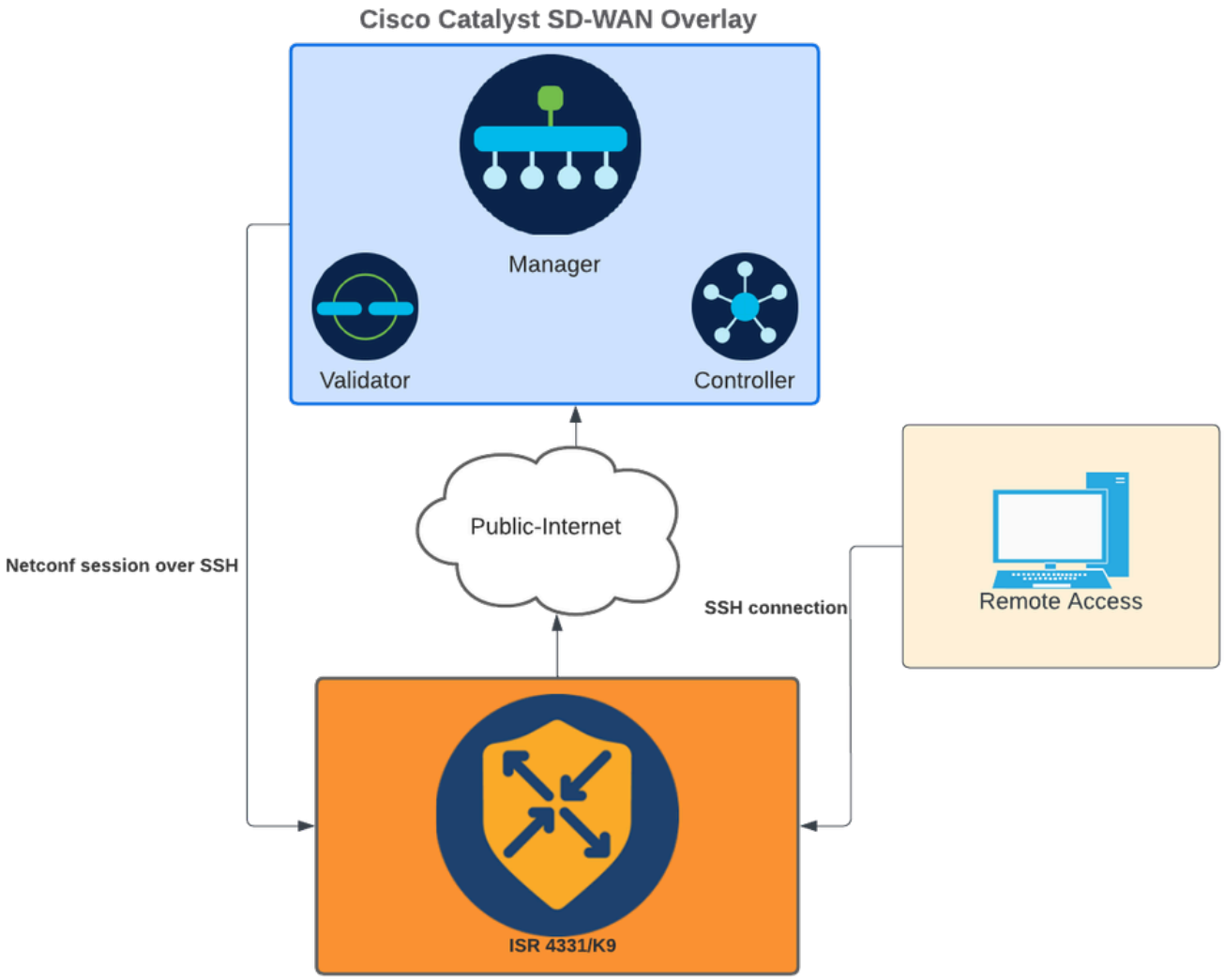
Vanwege dit feit is het noodzakelijk dat de sleutels altijd gesynchroniseerd en bijgewerkt worden. Als het door naleving en controle nodig is om de sleutellengte voor beveiliging te wijzigen, is het noodzakelijk om het proces dat in dit document wordt beschreven te voltooien om de sleutels te verkleinen en ze correct op het certificaat te synchroniseren om loskoppeling tussen de SD-WAN Manager en SD-WAN Edge-apparaten te voorkomen.



Voorzichtig: Voltooi alle stappen in het proces om verlies van toegang tot het apparaat te voorkomen. Als het apparaat in productie is, is het aan te raden om het in een onderhoudsvenster uit te voeren en de console toegang tot het apparaat te hebben.

Configureren

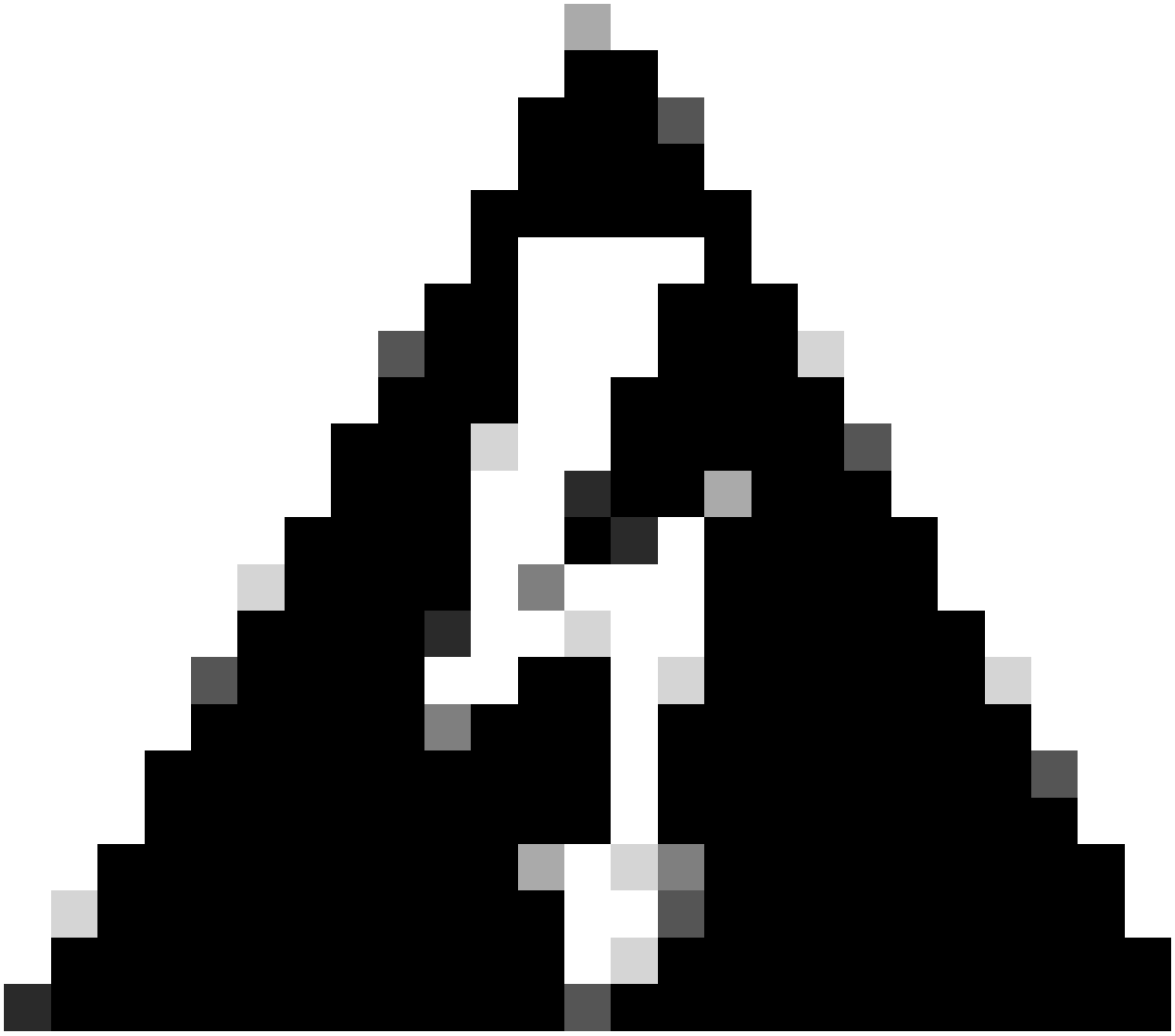
Netwerkdiagram



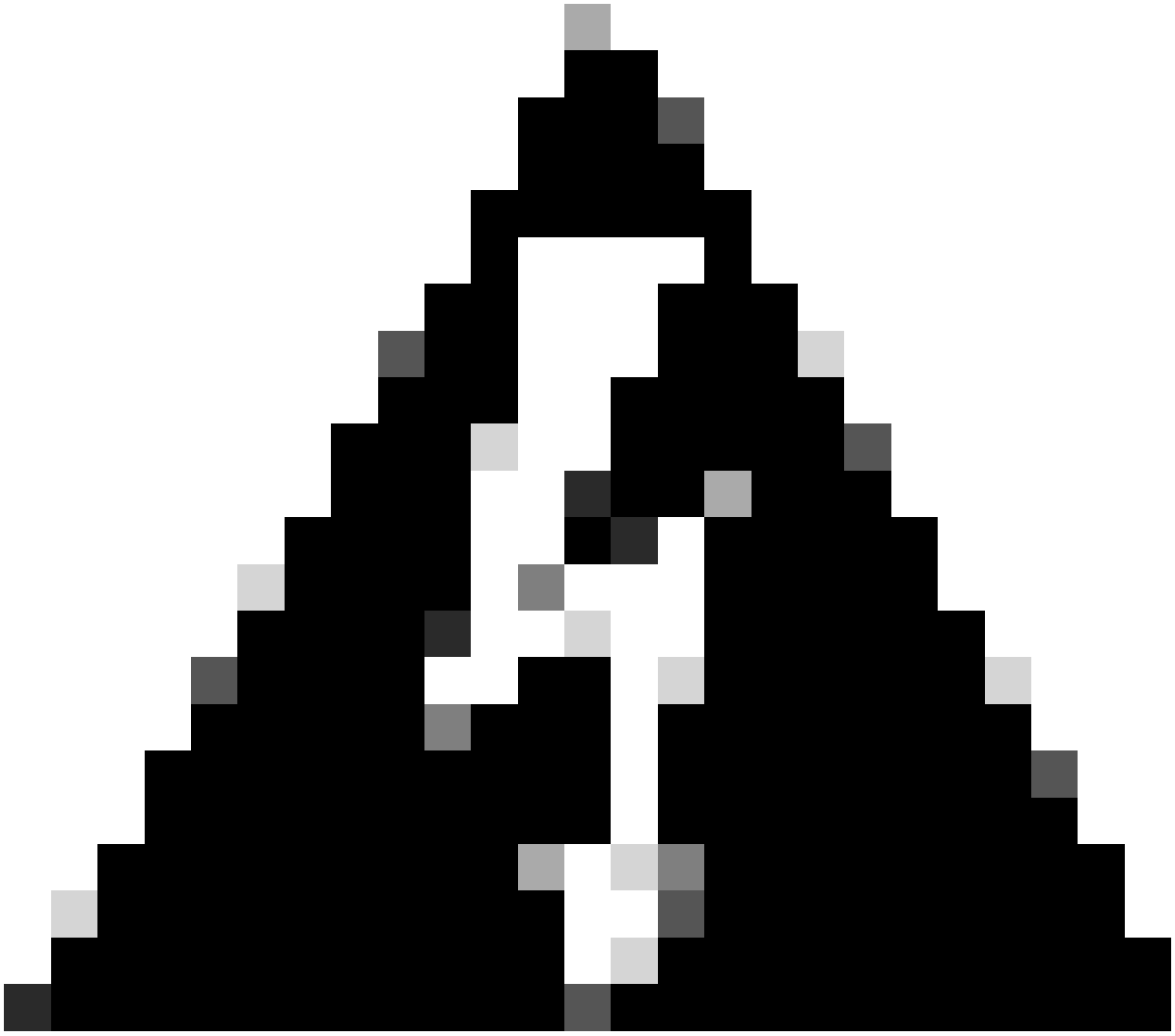
Netwerkdiagram

Configuraties

De RSA-toetsen in de WAN-randapparaten kunnen alleen worden aangepast met behulp van de Command-Line Interface (CLI); De CLI Add-On Feature-sjablonen kunnen niet worden gebruikt om de sleutels bij te werken.



Waarschuwing: Het wordt aanbevolen om het proces te doen met het gebruik van de console als de SD-WAN Manager SSH Tool niet beschikbaar is totdat het proces is voltooid.



Waarschuwing: Voor dit proces moet het apparaat opnieuw worden opgestart. Als het apparaat in productie is, is het aan te raden om het in een onderhoudsvenster uit te voeren en de console toegang tot het apparaat te hebben. Als er geen consoletoegang is, moet u tijdelijk een ander protocol voor externe toegang configureren als telnet.

Dit configuratievoorbeeld laat zien hoe u RSA 2048 verwijdert en RSA 4096-toets gebruikt.

1 - krijg de huidige SSH toetsnaam.

<#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+V0jPR8arK6bLSU7d
iGeSDDwW2MPNck/U5HBry9P/L4nKyZ1oevAhfy7cJVVmoHD41NQW9wb/hLtimuujnRRYkKuIWLmoI7AH
y6YQoetew8XVglVIjva+JzQ5ZX1JGm8AzN6a95RbRNhGRzgz9cTFmD7m6ArIKZPMyYQabXfrY+m/HuQ2
aytbHtJMgmOQk2fLPakO3PnQNYXpiDP3CmOEh3LJg82FZQ1eohmhm+mAInwU4mlLHUouigyBuq1KEBVe
z3vxjB9X8rGF3qzUcx2lpHmhXaNPXWen2QQbyfAIDo8WXVoff24uLYlwCVkv
```

2 - Ontvang het huidige zelfondertekende certificaat van trustpoint.

<#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

Beide waardenamen moeten overeenkomen.

3 - Verwijder de huidige toets.

<#root>

```
Device#
```

crypto key zeroize rsa

4 - Controleer of die oude sleutel is verwijderd.

<#root>

Device#

show ip ssh

5 - Genereert de nieuwe toets.

<#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
```

Dit proces kan 2 tot 5 minuten in beslag nemen.

6 - Bevestig de nieuwe gegenereerde sleutel.

<#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+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eFOOH1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELBO6yYEipPWMRaZYFfTRbNJm8/7SOJGlFkgFVW5nITTIgISoMV8EJv
bLl8cVgATDb1OckeDb7uU6PDXm3zonmZC0yqHtF1OAOJxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0O49UH0y0bMgPuWrJpwtk1iYA3+t6N/QdlC5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKyvkcqXi6nDfAKb8o+Z8/43xbvWlDIKAuj1rbdyqPAJB4llTZJkOHk8zRP5gZ8u4jTjNKQHb
vNa3ieg4RLEDOx4lqCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOul4YDJYr
D+jnyoZr4PnfWAgk4M9U89deWSlIRPMIXYd35YmLvD6OeQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

Er wordt nu een nieuwe sleutel gegenereerd. Echter, op het moment dat die oude sleutel werd verwijderd, zelfondertekende certificaat dat in gebruik is bij Netconf sessies wordt ook verwijderd uit het 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
```

Zodra de nieuwe 4096-toets is gegenereerd, worden de toetsen niet automatisch bijgewerkt op het zelfondertekende certificaat, en is het noodzakelijk volledige extra stappen om het bij te werken.

Opmerking: Als alleen de sleutel wordt gegenereerd, maar niet wordt bijgewerkt in het certificaat, verliest de SD-WAN Manager de NetConf-sessies, en dat zou kunnen breken alle beheeractiviteiten aan het apparaat (sjablonen, configuratie, enzovoort).

Er zijn twee manieren om het certificaat te genereren/de sleutel toe te wijzen:

1 - Laad het apparaat opnieuw.

<#root>

```
Device#
```

reload

2 - Start HTTP Secure-server opnieuw. Deze optie is alleen beschikbaar indien het apparaat in de CLI-modus staat.

<#root>

```
Device (config)#
```

no ip http secure-server

```
Device (config)#
```

commit

```
Device (config)#
```

ip http secure-server

```
Device (config)#
```

commit

Verifiëren

Na het opnieuw laden, valideren dat nieuwe sleutel wordt gegenereerd en het certificaat is onder trustpoint met dezelfde naam.

<#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

Bevestig dat SD-WAN Manager configuratiewijzigingen kan toepassen op de apparaatrouter.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.