VRF-bewust beheer op ASR-configuratievoorbeelden

Inhoud

Inleiding

Dit document beschrijft het gebruik van Virtual Routing and Forwarding-Aware (VRF-bewust) beheer op de Cisco Aggregation Services Router 1000 Series (ASR1K) met de beheerinterface (**Gigabit Ethernet0**). De informatie is ook van toepassing op elke andere interface in een VRF, tenzij uitdrukkelijk anders vermeld. Verschillende toegangsprotocollen voor **zowel de-aan-box** als

de verbindingsscenario's **van-de-doos** worden beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beheerprotocollen, zoals SSH, telnet en HTTP
- Bestandsoverdrachtprotocollen, zoals Secure Kopie Protocol (SCP), TFTP en FTP
- VRF's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS: XE versie 3.5S (15.2(1)S) of hoger Cisco IOS-XE versies
  Opmerking: VRF-bewuste SCP vereist deze versie ten minste, terwijl andere protocollen die in dit document worden beschreven ook met vorige versies werken.
- ASR1K

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 levend is, zorg er dan voor dat u de mogelijke impact van elke gebruikte opdracht begrijpt.

Achtergrondinformatie

Management-interface: Het doel van een beheerinterface is om gebruikers toe te staan om beheertaken op de router uit te voeren. Het is in wezen een interface die het dataplaneverkeer niet zou moeten en vaak niet kan doorsturen. Anders kan het worden gebruikt voor externe toegang tot de router, vaak via telnet en Secure Shell (SSH), en om de meeste beheertaken op de router uit te voeren. De interface is het meest nuttig voordat een router begint met het routing, of in scenario's voor probleemoplossing wanneer de gedeelde interfaces van de poortadapter (SPA) inactief zijn. Op ASR1K, is de beheerinterface in een standaard VRF genoemd **Mgmt-intf**.

De opdracht **ip *<protocol>*bron-interface** wordt in dit document uitgebreid gebruikt (waar het *<protocol>*trefwoord SSH, FTP, TFTP kan zijn). Deze opdracht wordt gebruikt om het IP-adres van een interface te specificeren dat als bronadres gebruikt moet worden wanneer ASR het clientapparaat in een verbinding is (de verbinding wordt bijvoorbeeld gestart vanuit de ASR of vanuit het box-verkeer). Dit betekent ook dat als ASR niet de initiator van de verbinding is, de **ip *<protocol>*bron-interface** opdracht niet van toepassing is en ASR dit IP-adres niet gebruikt voor het antwoordverkeer; In plaats daarvan gebruikt het het IP-adres van de dichtstbijzijnde interface naar de bestemming. Met deze opdracht kunt u verkeer bronnen (voor de ondersteunde protocollen) vanaf een VRF-bewuste interface.

Management-protocollen

> Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in dit artikel worden gebruikt.

SCP

Gebruik deze configuratie om de SCP clientservice op een ASR-account van een VRF-enabled-interface te gebruiken.

Configureren

De opdracht **ip SSH-bron-interface** wordt gebruikt om de beheerinterface naar de **MGMT-intf** VRF te richten voor zowel SSH- als SCP-clientservices, aangezien SCP SSH gebruikt. Er is geen andere optie in de opdracht **exemplaar**-scp om de VRF te specificeren. Daarom moet u deze **IP-bron-interface** opdracht gebruiken. Dezelfde logica is van toepassing op elke andere VRF-enabled-interface.

```
ASR(config)#ip ssh source-interface GigabitEthernet0
```

> Opmerking: Op het ASR1k-platform werkt VRF-bewuste SCP niet tot versie XE3.5S (15.2(1)S).

Verifiëren

Gebruik deze opdrachten om de configuratie te controleren.

```
ASR#show vrf
Name Default RD Protocols Interfaces
Mgmt-intf <not set> ipv4,ipv6 Gi0
ASR#
```

Typ deze opdracht om een bestand van ASR naar een extern apparaat met SCP te kopiëren:

```
ASR#copy running-config scp://guest@10.76.76.160/router.cfg
Address or name of remote host [10.76.76.160]?
Destination username [guest]?
Destination filename [router.cfg]?
Writing router.cfg Password:
!
Sink: C0644 2574 router.cfg
2574 bytes copied in 20.852 secs (123 bytes/sec)
ASR#
```

U kunt een bestand van een extern apparaat naar ASR met SCP kopiëren door deze opdracht in te voeren:

```
ASR#copy scp://guest@10.76.76.160/router.cfg bootflash:
Destination filename [router.cfg]?
Password:
Sending file modes: C0644 2574 router.cfg
!
2574 bytes copied in 17.975 secs (143 bytes/sec)
```

TFTP

Gebruik deze configuratie om de TFTP-clientservice op een ASR1k te gebruiken vanuit een VRF-enabled-interface.

Configureren

De **ip bron-interface** optie wordt gebruikt om de interface van het beheer naar de **Mgmt-intf** VRF te richten. Er is geen andere optie in de opdracht van het **kopieer** tftp om de VRF te specificeren. Daarom moet u deze **ip bron-interface** opdracht gebruiken. Dezelfde logica is van toepassing op elke andere VRF-enabled-interface.

```
ASR(config)#ip tftp source-interface GigabitEthernet0
```

Verifiëren

Gebruik deze opdrachten om de configuratie te controleren.

```
ASR#show vrf
Name Default RD Protocols Interfaces
Mgmt-intf <not set> ipv4,ipv6 Gi0
ASR#
```

U kunt een bestand van ASR naar de TFTP-server kopiëren door deze opdracht in te voeren:

```
ASR#copy running-config tftp
Address or name of remote host [10.76.76.160]?
Destination filename [ASRconfig.cfg]?
!!
2658 bytes copied in 0.335 secs (7934 bytes/sec)
ASR#
```

Om een bestand van de TFTP-server naar de ASR-flitser te kopiëren, voert u deze opdracht in:

```
ASR#copy tftp://10.76.76.160/ASRconfig.cfg bootflash:
Destination filename [ASRconfig.cfg]?
Accessing tftp://10.76.76.160/ASRconfig.cfg...
Loading ASRconfig.cfg from 10.76.76.160 (via GigabitEthernet0): !
[OK - 2658 bytes]

2658 bytes copied in 0.064 secs (41531 bytes/sec)
ASR#
```

FTP

Om de FTP client service op een ASR te gebruiken vanuit een VRF-enabled interface, gebruikt u deze configuratie.

Configureren

De **ip ftp bron-interface** optie wordt gebruikt om de beheersinterface naar de **Mgmt-intf** VRF te richten. Er is geen andere optie in de opdracht van **kopieer ftp** om de VRF te specificeren. Daarom moet u de **ip ftp bron-interface** opdracht gebruiken. Dezelfde logica is van toepassing op elke andere VRF-enabled-interface.

```
ASR(config)#ip ftp source-interface GigabitEthernet0
```

Verifiëren

Gebruik deze opdrachten om de configuratie te controleren.

```
ASR#show vrf
Name Default RD Protocols Interfaces
Mgmt-intf <not set> ipv4,ipv6 Gi0
```

Als u een bestand van ASR naar een FTP-server wilt kopiëren, voert u deze opdracht in:

```
ASR#copy running-config ftp://username:password@10.76.76.160/ASRconfig.cfg
Address or name of remote host [10.76.76.160]?
Destination filename [ASRconfig.cfg]?
Writing ASRconfig.cfg !
2616 bytes copied in 0.576 secs (4542 bytes/sec)
ASR#
```

Als u een bestand van de FTP-server naar de ASR-flitser wilt kopiëren, voert u deze opdracht in:

```
ASR#copy ftp://username:password@10.76.76.160/ASRconfig.cfg bootflash:
Destination filename [ASRconfig.cfg]?
Accessing ftp://*****:*****@10.76.76.160/ASRconfig.cfg...
Loading ASRconfig.cfg !
[OK - 2616/4096 bytes]

2616 bytes copied in 0.069 secs (37913 bytes/sec)
ASR#
```

Toegangsprotocollen voor beheer

Normale toegang

SSH

> **Voorzichtig:** Een veelvoorkomend probleem dat bij ASR1ks wordt gezien, is dat de SSH faalt als gevolg van geheugenverlies. Raadpleeg het Cisco-artikel voor meer informatie over dit

probleem de SSH-verificatiefout vanwege lage geheugencondities.

Er zijn twee opties gebruikt om de SSH-clientservice via de ASR (SSH vanaf de doos) te starten. Eén optie is de naam VRF in de opdracht **ssh** zelf op te geven, zodat u SSH-verkeer uit een bepaalde VRF kunt bron.

```
ASR#ssh -vrf Mgmt-intf -l cisco 10.76.76.161
Password:
Router>en
Password:
Router#
```

De andere optie is om de **IP bron-interface** optie te gebruiken om SSH-verkeer te bronnen vanuit een bepaalde VRF-enabled-interface.

```
ASR(config)#ip ssh source-interface GigabitEthernet0
ASR#
ASR#ssh -l cisco 10.76.76.161
Password:
Router>en
Password:
Router#
```

Om de SSH-serverservice (SSH to-the-box) te gebruiken, volgt u de procedure om SSH op een andere Cisco IOS-router in te schakelen. Raadpleeg het telnet en het SSH-Overzicht voor de Cisco ASR 1000 Series routers in het **gedeelte Cisco ASR 1000 Series aggregation services routers** voor meer informatie.

Telnet

Er zijn twee opties die gebruikt worden om de Telnet-clientservice op de ASR (telnet uit de-box) uit te voeren. Eén optie is de broninterface of VRF in het **telnet**-commando zelf te specificeren zoals hier wordt getoond:

```
ASR#telnet 10.76.76.160 /source-interface GigabitEthernet 0 /vrf Mgmt-intf
Trying 10.76.76.160 ... Open

User Access Verification

Username: cisco
Password:

Router>en
Password:
Router#
```

De andere optie is de **ip telnet bron-interface** opdracht te gebruiken. U moet in de volgende stap met de opdracht **telnet** nog de naam VRF specificeren, zoals hier wordt getoond:

```
ASR(config)#ip telnet source-interface GigabitEthernet0
ASR#
ASR#telnet 10.76.76.160 /vrf Mgmt-intf
Trying 50.50.50.3 ... Open

User Access Verification
```

```
Username: cisco
Password:

Router>en
password:
Router#
```

Als u de Telnet-serverservice (Telnet aan-the-box) wilt gebruiken, volgt u de procedure om telnet op een andere router in te schakelen. Raadpleeg het telnet en het SSH-Overzicht voor de Cisco ASR 1000 Series routers in het **gedeelte Cisco ASR 1000 Series aggregation services routers** voor meer informatie.

HTTP

De legacy web user interface die beschikbaar is voor alle routers is ook beschikbaar voor de ASR1K. Schakel HTTP-server of client-service in op de ASR zoals in deze sectie wordt getoond.

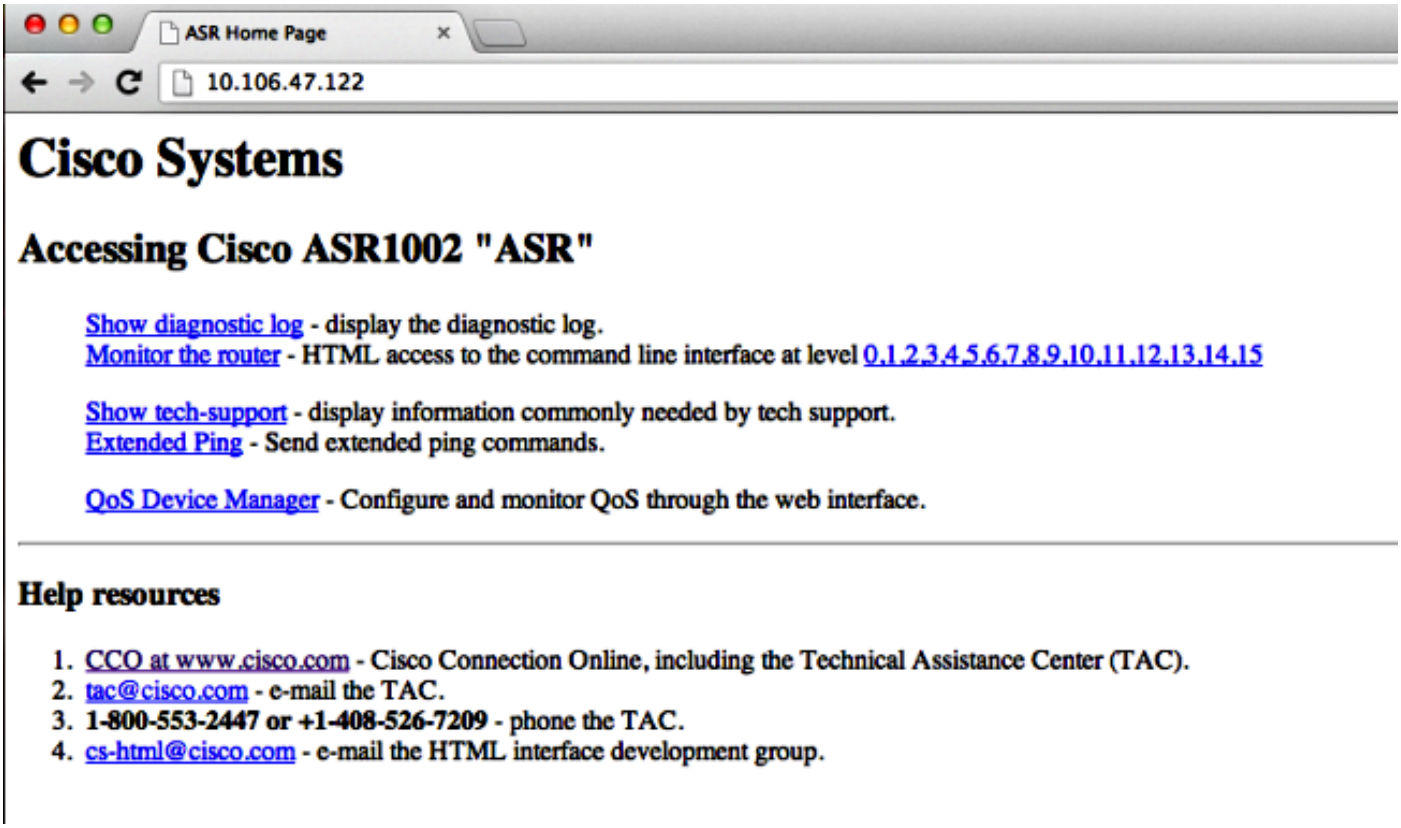
Gebruik deze configuratie die lokale verificatie gebruikt (u kunt ook een externe verificatie-, autorisatie- en accounting-server (AAA) gebruiken) om oudere HTTP-toegang tot de service (server) en de online gebaseerde GUI-toegang mogelijk te maken.

```
ASR(config)#ip http
ASR(config)#ip http authentication local
ASR(config)#username <> password <>
```

Hier is de configuratie om HTTP Secure-server (HTTPS) mogelijk te maken:

```
ASR(config)#ip http secure-server
ASR(config)#ip http authentication local
ASR(config)#username <> password <>
```

Bladeren naar het IP-adres van een interface in de ASR en inloggen met de gebruikersaccount die u hebt gemaakt. Dit is een screenshot:



Als u de HTTP client-service wilt gebruiken, voert u de **ip http client-bron-interface <interface name>**opdrachtbron voor het HTTP client-verkeer in van een VRF-enabled interface, zoals wordt getoond:

```
ASR(config)#ip http client source-interface GigabitEthernet0
```

Hier is een voorbeeld dat het gebruik van HTTP client service illustreert om een afbeelding van een externe HTTP server naar de flitser te kopiëren:

```
ASR#
ASR#copy http://username:password@10.76.76.160/image.bin flash:
Destination filename [image.bin]?
Accessing http://10.106.72.62/image.bin...
Loading http://10.106.72.62/image.bin
1778218 bytes copied in 20.038 secs (465819 bytes/sec)
ASR#
```

Persistente toegang

Deze sectie is alleen van toepassing op de-box telnet/SSH/HTTP-verbindingen.

Met aanhoudende SSH en persisterend telnet, kunt u een transportkaart configureren die de behandeling van inkomend SSH- of telnet-verkeer op de Ethernet-interface van het beheer definieert. Dit creëert de mogelijkheid om toegang te krijgen tot de router via diagnostische modus zelfs wanneer het Cisco IOS-proces niet actief is. Raadpleeg voor meer informatie over de diagnostische modus het gedeelte Understanding van de softwareconfiguratie van de Cisco ASR 1000 Series aggregation services routers.

> Opmerking: Persistente SSH of persistente telnet kunnen alleen worden geconfigureerd op de Management-interface, **Gigabit Ethernet0.**

Opmerking: In versies die de oplossing voor Cisco bug-ID CSCuj37515 niet hebben, is de authenticatiemethode voor permanente toegang afhankelijk van de methode die onder regel VTY wordt gebruikt. Voor blijvende toegang is vereist dat de authenticatie plaatselijk is, zodat toegang tot de diagnostische modus nog steeds werkt als externe verificatie mislukt. Dit betekent dat elke normale toegang tot SSH en telnet ook het gebruik van lokale authenticatie vereist.

Voorzichtig: In versies die de oplossing voor Cisco bug-ID CSC7654 niet hebben, beperkt het gebruik van de standaard AAA-methode de gebruikersmogelijkheid om de SSH-melding in te voeren wanneer er een persistente SSH wordt gebruikt. De gebruiker wordt altijd gedwongen om de diagnostische prompt in te voeren. Voor deze versies raadt Cisco u aan een methode van de naamauthenticatie te gebruiken, of om te verzekeren dat normale SSH en telnet worden geactiveerd.

Persistent SSH

Maak een transportkaart om persistente SSH's mogelijk te maken zoals in de volgende sectie wordt getoond:

Configureren

```
ASR(config)#crypto key generate rsa label ssh-keys modulus 1024
The name for the keys will be: ssh-keys

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

ASR#
ASR(config)#transport-map type persistent ssh
persistent-ssh-map
ASR(config-tmap)#rsa keypair-name ssh-keys
ASR(config-tmap)#transport interface GigabitEthernet0
ASR(config-tmap)#banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for vty line--
X
ASR(config-tmap)#
ASR(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
c
ASR(config-tmap)#connection wait allow interruptible
ASR(config-tmap)#exit
ASR(config)#transport type persistent ssh input persistent-ssh
*Jul 10 15:31:57.102: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd:
Server persistent ssh has been notified to start
```

Nu moet u lokale authenticatie voor persistente SSH mogelijk maken. Dit kan worden gedaan met de opdracht nieuw model of zonder. Beide scenario's worden hier beschreven. (Zorg er in beide gevallen voor dat u een lokale gebruikersnaam/wachtwoordaccount op de router hebt).

U kunt kiezen welke configuratie is gebaseerd op de vraag of u AAA ingeschakeld hebt op de ASR.

1. Met AAA ingeschakeld:

```
ASR(config)#aaa new-model
ASR(config)#aaa authentication login default local
ASR(config)#line vty 0 4
ASR(config-line)#login authentication default
```

2. Zonder AAA ingeschakeld

```
ASR(config)#line vty 0 4
ASR(config-line)#login local
```

Verifiëren

SSH naar de ASR met het IP-adres van de VRF-enabled Gigabit **Ethernet0-**interface. Zodra het wachtwoord is ingevoerd, moet u de break sequentie (**Ctrl-C** of **Ctrl-Shift-6**) invoeren.

```
management-station$ ssh -l cisco 10.106.47.139
cisco@10.106.47.139's password:

--Waiting for vty line--

--Welcome to Diagnostic Mode--
ASR(diag)#
```

> Opmerking: Voer de break sequentie (**Ctrl-C** of **Ctrl-Shift-6**) in —Wachten op **vty lijn—** weergegeven op de terminal om de diagnostische modus in te voeren.

Persistent telnet

Configureren

Met een zelfde logica zoals in de vorige sectie voor SSH wordt beschreven, creëer een vervoerkaart voor persisterend telnet zoals hier getoond:

```
ASR(config)#transport-map type persistent telnet persistent-telnet
ASR(config-tmap)#banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
ASR(config-tmap)#banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
ASR(config-tmap)#connection wait allow interruptible
ASR(config-tmap)#transport interface gigabitEthernet 0
ASR(config-tmap)#exit
ASR(config)#transport type persistent telnet input persistent-telnet
*Jul 10 15:26:56.441: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd:
Server persistent telnet has been notified to start
```

Zoals in de laatste sectie voor SSH is besproken, zijn er twee manieren om lokale authenticatie te configureren zoals hier wordt getoond:

1. Met AAA ingeschakeld:

```
ASR(config)#aaa new-model
```

```
ASR(config)#aaa authentication login default local
ASR(config)#line vty 0 4
ASR(config-line)#login authentication default
```

2. Zonder AAA:

```
ASR(config)#line vty 0 4
ASR(config-line)#login local
```

Verifiëren

Telnet aan het IP adres van **Gigabit Ethernet0** interface. Nadat u de aanmeldingsgegevens hebt ingevoerd, voert u de break sequentie in en wacht u een paar seconden (soms duurt het even) voordat u zich in de diagnostische modus inlogt.

```
Management-station$ telnet 10.106.47.139
Trying 10.106.47.139...
Connected to 10.106.47.139.
Escape character is '^]'.
Username: cisco
Password:

--Waiting for IOS Process--


--Welcome to Diagnostic Mode--
ASR(diag)#
```

> Opmerking: Voer de breukvolgorde in **Ctrl+C** of **Ctrl+Shift+6**, en wacht even. Wanneer **—en wachten op IOS proces—** op de terminal, kunt u diagnostische modus invoeren.

Persistent HTTP

Om de persistente HTTP-toegang tot de-box mogelijk te maken (HTTP van-the-box of HTTP client-service is niet beschikbaar) en de nieuwe web-gebaseerde GUI-toegang te gebruiken, gebruikt u deze configuratie die lokale verificatie gebruikt (u kunt ook een externe AAA-server gebruiken).

Configureren

In deze formaties zijn **http-webui** en **https-webui** de namen van de vervoerskaarten.

```
ASR(config)#ip http serverASR(config)#ip http authentication local
ASR(config)#username <> password <>
ASR(config)#transport-map type persistent webui http-webui
ASR(config-tmap)#server
ASR(config-tmap)#exit
ASR(config)#transport type persistent webui input http-webui
```

Hier wordt de configuratie gebruikt om HTTP security server (HTTPS) mogelijk te maken.

```
ASR(config)#ip http secure-serverASR(config)#ip http authentication local
ASR(config)#username <> password <>
ASR(config)#transport-map type persistent webui https-webui
ASR(config-tmap)#secure-server
ASR(config-tmap)#exit
```

```
ASR(config)#transport type persistent webui input https-webui
```

Verifiëren

Bladeren naar het IP-adres van een interface in de ASR. Meld u aan met de gebruikersnaam/het wachtwoord dat u hebt ingesteld om de startpagina te starten. Beveiliging en controle gerelateerde informatiedisplays, samen met een **IOS WebUI** waar u opdrachten kunt toepassen. Dit is een screenshot van de startpagina:

Problemen oplossen

Als WebUI niet via HTTPS beschikbaar is, controleer dan of de certificaat en Rivest-Shamir-Adleman (RSA) toets aanwezig en operationeel zijn. U kunt deze **debug** opdracht gebruiken om de reden te bepalen dat WebUI niet goed start:

```
ASR#debug platform software configuration notify webui
ASR#config t
ASR(config)#no transport type persistent webui input https-webui
%UICFGEXP-6-SERVER_NOTIFIED_STOP: SIP0: psd: Server wui has been notified to stop
ASR(config)#transport type persistent webui input https-webui

CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map https-webui input being processed
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: server cache: false, tm: false
CNOTIFY-UI: secure-server cache: true, tm: true
CNOTIFY-UI: Validating server config
CNOTIFY-UI: Validating secure server config
CNOTIFY-UI: Checking if secure server config is ok
CNOTIFY-UI: Secure server is enabled in map
CNOTIFY-UI: Getting trust point
CNOTIFY-UI: Getting self-signed trust point
CNOTIFY-UI: Could not get self-signed trustpoint
CNOTIFY-UI: A certificate for does not exist
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Failed to get rsa key pair name
CNOTIFY-UI: Key needed to generate the pem file
CNOTIFY-UI: Secure-server config invalid
CNOTIFY-UI: Config analysis indicates no change
CNOTIFY-UI: Failed to prepare config
```

RSA-toets

Om de aanwezigheid van de RSA-toets te controleren voert u deze opdracht in:

```
ASR#show crypto key mypubkey rsa
% Key pair was generated at: XX:XX:XX XXX XXX XX XXXX
Key name: ASR.ASR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data&colon;
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXX
% Key pair was generated at: XX:XX:XX XXX XXX XX XXXX
Key name: ASR.ASR.server
```

```
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable. Redundancy enabled.
Key Data&colon;
 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXX
ASR#
```

Let op de naam van de toets, omdat deze vereist is om het certificaat te maken. Als er geen toets aanwezig is, kunt u een met deze opdrachten maken:

```
ASR(config)#ip domain-name Router
ASR(config)#crypto key generate rsa
The name for the keys will be: Router.Router
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

ASR(config)#
*Dec 22 10:57:11.453: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Certificaat

Zodra de toets aanwezig is, kunt u deze opdracht invoeren om het certificaat te controleren:

```
ASR#show crypto pki certificates
ASR Self-Signed Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: General Purpose
Issuer:
serialNumber=XXXXXXXXXXX+ipaddress=XXX.XXX.XXX.XXX+hostname=ASR
cn=XXX.XXX.XXX.XXX
c=US
st=NC
l=Raleigh
Subject:
Name: Router
IP Address: XXX.XXX.XXX.XXX
Serial Number: XXXXXXXXXXX
serialNumber=XXXXXXXXXXX+ipaddress=XXX.XXX.XXX.XXX+hostname=aSR
cn=XXX.XXX.XXX.XXX
c=US
st=NC
l=Raleigh
Validity Date:
start date: XX:XX:XX XXX XXX XX XXXX
end date: XX:XX:XX XXX XXX XX XXXX
Associated Trustpoints: local
```

Als het certificaat ongeldig is of niet aanwezig is, kunt u het certificaat met deze opdrachten maken:

```
ASR(config)#crypto pki trustpoint local
ASR(ca-trustpoint)#enrollment selfsigned
```

```
ASR(ca-trustpoint)#subject-name CN=XXX.XXX.XXX.XXX; C=US; ST=NC; L=Raleigh
ASR(ca-trustpoint)#rsakeypair ASR.ASR 2048
ASR(ca-trustpoint)#crypto pki enroll local
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: XXX.XXX.XXX.XXX
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

Zodra de RSA-toets en het certificaat worden bijgewerkt en geldig zijn, kan het certificaat worden gekoppeld aan de HTTPS-configuratie:

```
ASR(config)#ip http secure-trustpoint local
```

U kunt vervolgens de WebexUI uitschakelen om er zeker van te zijn dat deze functioneel is:

```
ASR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ASR(config)#no transport type persistent webui input https-webui
ASR(config)#
CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map usage being disabled
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: Persistent webui will be shutdown if running
CNOTIFY-UI: Creating config message
CNOTIFY-UI: Secure-server state actually being set to: disabled
CNOTIFY-UI: Webui server information: changed: true, status: disabled, port: 80
CNOTIFY-UI: Webui secure server information: changed: true, status: disabled, port: 443
CNOTIFY-UI: Webui service (re)start: false. Sending all config
ASR(config)#
ASR(config)#transport type persistent webui input https-webui
ASR(config)#
CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map https-webui input being processed
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: server cache: false, tm: false
CNOTIFY-UI: secure-server cache: true, tm: true
CNOTIFY-UI: Validating server config
CNOTIFY-UI: Validating secure server config
CNOTIFY-UI: Checking if secure server config is ok
CNOTIFY-UI: Secure server is enabled in map
CNOTIFY-UI: Getting trust point
CNOTIFY-UI: Using issued certificate for identification
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Getting private key
CNOTIFY-UI: Getting certificate
CNOTIFY-UI: Secure server config is ok
CNOTIFY-UI: Secure-server config is valid
CNOTIFY-UI: Creating config message
CNOTIFY-UI: Secure-server state actually being set to: enabled
CNOTIFY-UI: Adding rsa key pair
CNOTIFY-UI: Getting base64 encoded rsa key
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Getting private key
CNOTIFY-UI: Added rsa key
CNOTIFY-UI: Adding certificate
CNOTIFY-UI: Getting base64 encoded certificate
```

```
CNOTIFY-UI: Getting certificate
CNOTIFY-UI: Getting certificate for local
CNOTIFY-UI: Certificate added
CNOTIFY-UI: Webui server information: changed: false, status: disabled, port: 80
CNOTIFY-UI: Webui secure server information: changed: true, status: enabled, port: 443
CNOTIFY-UI: Webui service (re)start: true. Sending all config

%UICFGEXP-6-SERVER_NOTIFIED_START: SIP0: psd:  Server wui has been notified to start
```

Gerelateerde informatie

- Console-poort, telnet en SSH-verwerking
- De diagnostische modus begrijpen
- Technische ondersteuning en documentatie – Cisco Systems