Exemples de configuration de VRF-Aware Management sur ASR

Contenu

Introduction

Ce document décrit l'utilisation de la gestion VRF (Virtual Routing and Forwarding-Aware) sur le routeur de services d'agrégation Cisco de la gamme 1000 (ASR1K) avec l'interface de gestion (**GigabitEthernet0**). Ces informations sont également applicables à toute autre interface d'un VRF, sauf indication contraire explicite. Différents protocoles d'accès **aux** scénarios **de** connexion **prêts**

à porter et **prêts à l'emploi** sont décrits.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocoles de gestion, tels que SSH, Telnet et HTTP
- Protocoles de transfert de fichiers, tels que le protocole SCP (Secure Copy Protocol), TFTP et FTP
- VRF

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS® XE version 3.5S (15.2(1)S) ou ultérieure Cisco IOS-XE
  Note: La SCP compatible VRF nécessite au moins cette version, alors que les autres protocoles décrits dans ce document fonctionnent également avec les versions précédentes.
- ASR1K

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande utilisée.

Informations générales

Interface de gestion: L'objectif d'une interface de gestion est de permettre aux utilisateurs d'effectuer des tâches de gestion sur le routeur. Il s'agit essentiellement d'une interface qui ne doit pas, et souvent ne peut pas, transférer le trafic du plan de données. Sinon, il peut être utilisé pour un accès distant au routeur, souvent via Telnet et Secure Shell (SSH), et pour effectuer la plupart des tâches de gestion sur le routeur. L'interface est plus utile avant qu'un routeur ne commence le routage, ou dans des scénarios de dépannage lorsque les interfaces SPA (Shared Port Adapter) sont inactives. Sur ASR1K, l'interface de gestion se trouve dans un VRF par défaut nommé **Mgmt-intf**.

La commande **ip *<protocol>* source-interface** est largement utilisée dans ce document (où le mot clé *<protocol>* peut être SSH, FTP, TFTP). Cette commande est utilisée afin de spécifier l'adresse IP d'une interface à utiliser comme adresse source lorsque l'ASR est le périphérique client dans une connexion (par exemple, la connexion est initiée à partir du trafic ASR ou du trafic de la boîte). Cela signifie également que si ASR n'est pas l'initiateur de la connexion, la commande **ip *<protocol>* source-interface** n'est pas applicable et qu'ASR n'utilise pas cette adresse IP pour le trafic de réponse ; il utilise plutôt l'adresse IP de l'interface la plus proche de la destination. Cette commande vous permet d'approvisionner le trafic (pour les protocoles pris en charge) à partir d'une interface VRF-Aware.

Protocoles de gestion

> **Note**: Utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cet article.

SCP

Afin d'utiliser le service client SCP sur un ASR à partir d'une interface compatible VRF, utilisez cette configuration.

Configuration

La commande **ip ssh source-interface** est utilisée afin de pointer l'interface de gestion vers le VRF **Mgmt-intf** pour les services client SSH et SCP, puisque SCP utilise SSH. Il n'existe aucune autre option dans la commande **copy scp** pour spécifier le VRF. Par conséquent, vous devez utiliser cette commande **ip ssh source-interface**. La même logique s'applique à toute autre interface compatible VRF.

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

> **Note**: Sur la plate-forme ASR1k, la SCP compatible VRF ne fonctionne qu'avec la version XE3.5S (15.2(1)S).

Vérification

Utilisez ces commandes afin de vérifier la configuration.

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

Afin de copier un fichier d'ASR vers un périphérique distant avec SCP, entrez cette commande :

```
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#
```

Afin de copier un fichier d'un périphérique distant vers ASR avec SCP, entrez cette commande :

```
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

Afin d'utiliser le service client TFTP sur un ASR1k à partir d'une interface compatible VRF, utilisez cette configuration.

Configuration

L'option **ip tftp source-interface** est utilisée afin de pointer l'interface Management vers le VRF **Mgmt-intf**. Il n'existe aucune autre option dans la commande **copy tftp** pour spécifier le VRF. Par conséquent, vous devez utiliser cette commande **ip tftp source-interface**. La même logique s'applique à toute autre interface compatible VRF.

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

Vérification

Utilisez ces commandes afin de vérifier la configuration.

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

Afin de copier un fichier d'ASR vers le serveur TFTP, entrez cette commande :

```
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#
```

Afin de copier un fichier du serveur TFTP vers le bootflash ASR, entrez cette commande :

```
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

Afin d'utiliser le service client FTP sur un ASR à partir d'une interface compatible VRF, utilisez cette configuration.

Configuration

L'option **ip ftp source-interface** est utilisée afin de pointer l'interface Management vers le VRF **Mgmt-intf**. Il n'existe aucune autre option dans la commande **copy ftp** pour spécifier le VRF. Par conséquent, vous devez utiliser la commande **ip ftp source-interface**. La même logique s'applique à toute autre interface compatible VRF.

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

Vérification

Utilisez ces commandes afin de vérifier la configuration.

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

Afin de copier un fichier d'ASR vers un serveur FTP, entrez cette commande :

```
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#
```

Afin de copier un fichier du serveur FTP vers le bootflash ASR, entrez cette commande :

```
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#
```

Protocoles d'accès à la gestion

Accès régulier

SSH

> **Attention** : Un problème courant observé avec ASR1 est que le SSH échoue en raison d'une mémoire insuffisante. Pour plus d'informations sur ce problème, reportez-vous à l'article

Cisco Échec de l'authentification SSH en raison de conditions de mémoire insuffisante.

Deux options sont utilisées afin d'exécuter le service client SSH sur l'ASR (SSH from the box). Une option consiste à spécifier le nom VRF dans la commande **ssh** elle-même, afin que vous puissiez source du trafic SSH à partir d'un VRF particulier.

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

L'autre option est d'utiliser l'option **ip ssh source-interface** afin de source du trafic SSH à partir d'une interface VRF spécifique.

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

Afin d'utiliser le service de serveur SSH (SSH to the box), suivez la procédure pour activer SSH sur tout autre routeur Cisco IOS. Référez-vous à la section Vue d'ensemble de Telnet et SSH pour les routeurs de la gamme Cisco ASR 1000 du **Guide de configuration du logiciel des routeurs à services d'agrégation de la gamme Cisco ASR 1000** pour plus d'informations.

Telnet

Deux options sont utilisées pour exécuter le service client Telnet sur l'ASR (Telnet from the-box). Une option consiste à spécifier l'interface source ou le VRF dans la commande **telnet** elle-même, comme indiqué ici :

```
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#
```

L'autre option consiste à utiliser la commande **ip telnet source-interface**. Vous devez toujours spécifier le nom VRF à l'étape suivante avec la commande **telnet**, comme indiqué ici :

```
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#
```

Afin d'utiliser le service de serveur Telnet (Telnet to-the-box), suivez la procédure pour activer Telnet sur n'importe quel autre routeur. Référez-vous à la section Vue d'ensemble de Telnet et SSH pour les routeurs de la gamme Cisco ASR 1000 du **Guide de configuration du logiciel des routeurs à services d'agrégation de la gamme Cisco ASR 1000** pour plus d'informations.

HTTP

L'interface utilisateur Web héritée disponible pour tous les routeurs est également disponible pour l'ASR1K. Activez le service client ou serveur HTTP sur l'ASR, comme indiqué dans cette section.

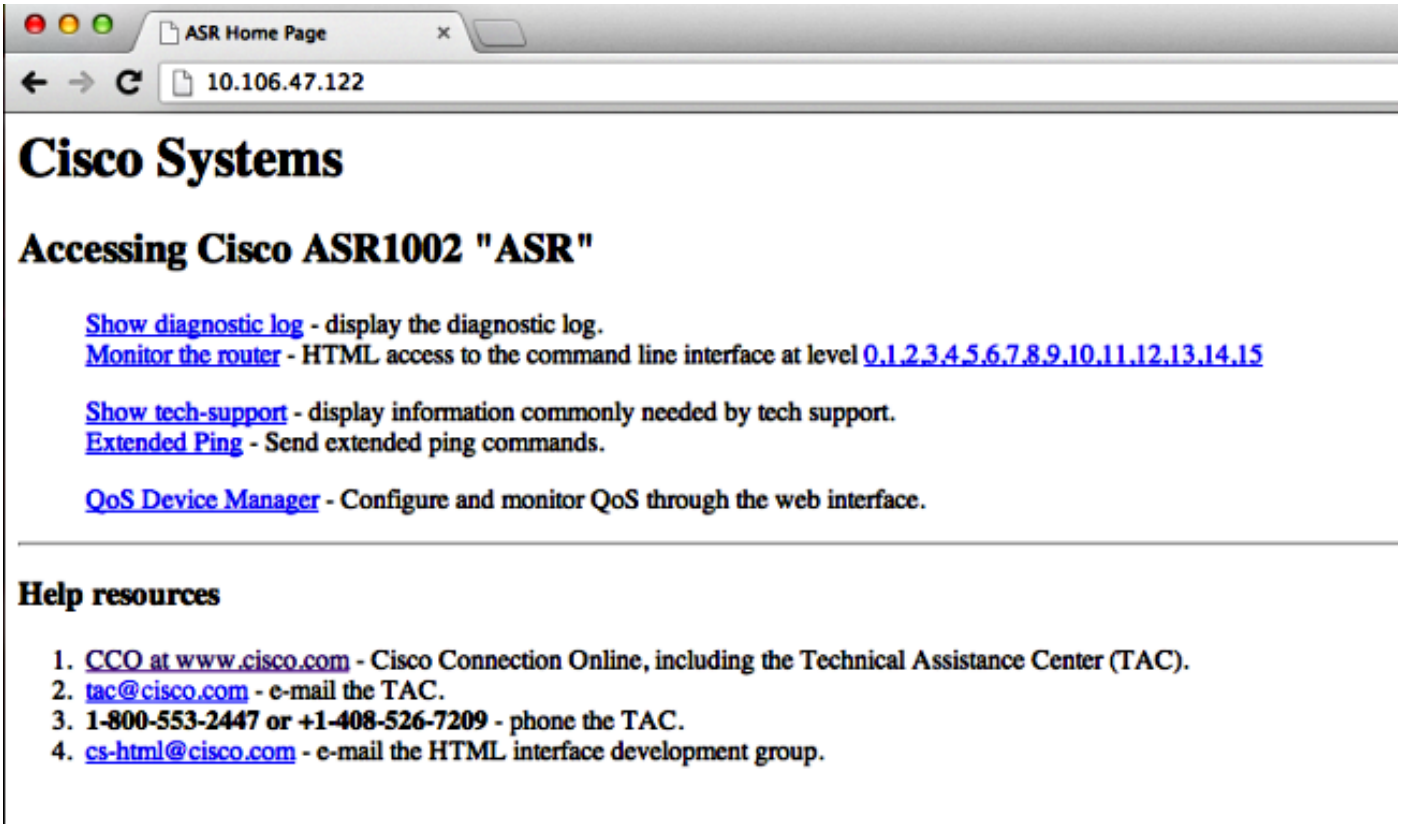
Afin d'activer l'accès HTTP hérité au service (serveur) et l'accès Web à l'interface utilisateur graphique, utilisez cette configuration qui utilise l'authentification locale (vous pouvez également utiliser un serveur AAA (Authentication, Authorization, and Accounting) externe).

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

Voici la configuration pour activer le serveur sécurisé HTTP (HTTPS) :

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

Accédez à l'adresse IP d'une interface sur l'ASR et connectez-vous avec le compte d'utilisateur que vous avez créé. Voici une capture d'écran :



Afin d'utiliser le service client HTTP, entrez la source de commande **ip http client source-interface <nom de l'interface>** pour le trafic client HTTP à partir d'une interface compatible VRF, comme indiqué :

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

Voici un exemple qui illustre l'utilisation du service client HTTP afin de copier une image d'un serveur HTTP distant vers la mémoire flash :

```
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#
```

Accès permanent

Cette section s'applique uniquement aux connexions Telnet/SSH/HTTP prêtes à l'emploi.

Avec SSH et Telnet persistants, vous pouvez configurer une carte de transport qui définit le traitement du trafic SSH ou Telnet entrant sur l'interface Ethernet de gestion. Cela permet donc d'accéder au routeur via le mode de diagnostic même lorsque le processus Cisco IOS n'est pas actif. Pour plus d'informations sur le mode de diagnostic, reportez-vous à la section Comprendre le mode de diagnostic du Guide de configuration du logiciel des routeurs à services d'agrégation de la gamme Cisco ASR 1000.

> **Note**: SSH persistant ou Telnet persistant ne peut être configuré que sur l'interface de gestion, **GigabitEthernet0.**

Note: Dans les versions qui n'ont pas le correctif pour l'ID de bogue Cisco CSCuj37515, la méthode d'authentification pour l'accès permanent dépend de la méthode utilisée sous la ligne **VTY**. L'accès permanent nécessite que l'authentification soit locale, de sorte que l'accès au mode de diagnostic fonctionne toujours en cas d'échec de l'authentification externe. Cela signifie que tout accès SSH et Telnet normal nécessite également l'utilisation de l'authentification locale.

Attention : Dans les versions qui n'ont pas le correctif pour l'ID de bogue Cisco CSCug77654, l'utilisation de la méthode AAA par défaut limite la capacité de l'utilisateur à entrer l'invite SSH lorsque SSH persistant est utilisé. L'utilisateur est toujours forcé d'entrer l'invite de diagnostic. Pour ces versions, Cisco vous recommande d'utiliser une méthode d'authentification de nom ou de vous assurer que SSH et Telnet normaux sont activés.

SSH persistant

Créez une carte de transport afin d'autoriser SSH persistant comme indiqué dans la section suivante :

Configuration

```
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
```

Vous devez maintenant activer l'authentification locale pour SSH persistant. Cela peut être fait soit avec la commande **aaa new-model**, soit sans elle. Les deux scénarios sont décrits ici. (Dans les deux cas, assurez-vous d'avoir un nom d'utilisateur/mot de passe local sur le routeur).

Vous pouvez choisir la configuration en fonction de l'activation ou non d'AAA sur l'ASR.

1. Avec AAA activé :

```
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. Sans AAA activé :

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

Vérification

SSH à l'ASR avec l'adresse IP de l'interface **Gigabitethernet0** compatible VRF. Une fois le mot de passe entré, vous devez entrer la séquence de pause (**Ctrl-C** ou **Ctrl-Maj-6**).

```
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)#
```

> **Note**: Entrez la séquence d'interruption (**Ctrl-C** ou **Ctrl-Maj-6**) lorsque **- En attente de la ligne vty— s'**affiche sur le terminal afin de passer en mode diagnostic.

Telnet persistant

Configuration

Avec la même logique que celle décrite dans la section précédente pour SSH, créez un plan de transport pour Telnet persistant comme indiqué ici :

```
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
```

Comme indiqué dans la dernière section pour SSH, il existe deux façons de configurer l'authentification locale comme indiqué ici :

1. Avec AAA activé :

```
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. Sans AAA :

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

Vérification

Établissez une connexion Telnet avec l'adresse IP de l'interface **GigabitEthernet0**. Après avoir entré les informations d'identification, entrez la séquence d'interruption et attendez quelques secondes (parfois un certain temps) avant de vous connecter au mode de diagnostic.

```
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)#
```

> **Note**: Entrez la séquence de pause **Ctrl+C** ou **Ctrl+Maj+6**, et attendez quelques secondes. Lorsque **—Waiting for IOS Process—** s'affiche sur le terminal, vous pouvez passer en mode diagnostic.

HTTP persistant

Afin d'activer l'accès HTTP persistant à la boîte (le service client HTTP de la boîte ou HTTP n'est pas disponible) et utiliser le nouvel accès Web à l'interface utilisateur graphique, utilisez cette configuration qui utilise l'authentification locale (vous pouvez également utiliser un serveur AAA externe).

Configuration

Dans ces configurations, **http-webui** et **https-webui** sont les noms des transports-maps.

```
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
```

Voici la configuration utilisée pour activer le serveur sécurisé HTTP (HTTPS).

```
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
```

Vérification

Accédez à l'adresse IP d'une interface sur l'ASR. Connectez-vous avec le nom d'utilisateur/mot de passe que vous avez créé afin de lancer la page d'accueil. Les informations relatives à l'état et à la surveillance s'affichent, ainsi qu'une interface **WebUI IOS** où vous pouvez appliquer des commandes. Voici une capture d'écran de la page d'accueil :

Dépannage

Si WebUI n'est pas disponible via HTTPS, vérifiez que le certificat et la clé RSA (Rivest-Shamir-Adleman) sont présents et opérationnels. Vous pouvez utiliser cette commande **debug** afin de déterminer la raison pour laquelle l'interface WebUI ne démarre pas correctement :

```
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
```

Clé RSA

Afin de vérifier la présence de la clé RSA, entrez cette commande :

```
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#
```

Notez le nom de clé, car il est nécessaire pour créer le certificat. Si aucune clé n'est présente, vous pouvez en créer une à l'aide des commandes suivantes :

```
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
```

Certificat

Une fois la clé présente, vous pouvez entrer cette commande afin de vérifier le certificat :

```
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
```

Si le certificat n'est pas valide ou n'est pas présent, vous pouvez créer le certificat avec les commandes suivantes :

```
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
```

Une fois que la clé RSA et le certificat sont mis à jour et valides, le certificat peut être associé à la configuration HTTPS :

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

Vous pouvez ensuite désactiver et réactiver l'interface WebUI afin de vous assurer qu'elle fonctionne :

```
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

Informations connexes

- Port de console, Telnet et gestion SSH
- Présentation du mode de diagnostic
- Support et documentation techniques - Cisco Systems