Ejemplos de Configuración de VRF-Aware Management en ASR

Contenido

Introducción

Este documento describe el uso de la administración de Virtual Routing and Forwarding Aware (VRF-Aware) en Cisco Aggregation Services Router serie 1000 (ASR1K) con la interfaz de administración (**GigabitEthernet0**). La información también es aplicable a cualquier otra interfaz en un VRF, a menos que se especifique explícitamente lo contrario. Se describen varios protocolos

de acceso tanto para escenarios de conexión **a medida** como **desde el paquete**.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolos de administración, como SSH, Telnet y HTTP
- Protocolos de transferencia de archivos, como Secure Copy Protocol (SCP), TFTP y FTP
- VRF

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS® XE versión 3.5S (15.2(1)S) o versiones posteriores de Cisco IOS-XE
  Nota: El SCP que reconoce VRF requiere al menos esta versión, mientras que otros protocolos descritos en este documento también funcionan con versiones anteriores.
- 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 su red está activa, asegúrese de comprender el impacto potencial de cualquier comando utilizado.

Antecedentes

Interfaz de administración: El propósito de una interfaz de administración es permitir a los usuarios realizar tareas de administración en el router. Se trata básicamente de una interfaz que no debe reenviar el tráfico del plano de datos, y a menudo no puede hacerlo. De lo contrario, se puede utilizar para el acceso remoto al router, a menudo a través de Telnet y Secure Shell (SSH), y para realizar la mayoría de las tareas de administración en el router. La interfaz es más útil antes de que un router comience el ruteo o en situaciones de solución de problemas cuando las interfaces del adaptador de puerto compartido (SPA) están inactivas. En ASR1K, la interfaz de administración se encuentra en un VRF predeterminado denominado **Mgmt-intf**.

El comando **ip *<protocol>* source-interface** se utiliza ampliamente en este documento (donde la palabra clave *<protocol>* puede ser SSH, FTP, TFTP). Este comando se utiliza para especificar la dirección IP de una interfaz que se utilizará como la dirección de origen cuando ASR sea el dispositivo cliente en una conexión (por ejemplo, la conexión se inicia desde el ASR o desde el tráfico del paquete). Esto también significa que si ASR no es el iniciador de la conexión, el **comando ip *<protocol>* source-interface** no es aplicable, y ASR no utiliza esta dirección IP para el tráfico de respuesta; en su lugar, utiliza la dirección IP de la interfaz más cercana al destino. Este comando le permite generar tráfico (para los protocolos soportados) desde una interfaz que reconoce VRF.

Protocolos de administración

> **Nota:** Utilice la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este artículo.

SCP

Para utilizar el servicio cliente SCP en un ASR desde una interfaz habilitada para VRF, utilice esta configuración.

Configurar

El comando **ip ssh source-interface** se utiliza para señalar la interfaz de administración al VRF **Mgmt-intf** para los servicios de cliente SSH y SCP, ya que SCP utiliza SSH. No hay otra opción en el comando **copy scp** para especificar el VRF. Por lo tanto, debe utilizar este comando **ip ssh source-interface**. La misma lógica se aplica a cualquier otra interfaz habilitada para VRF.

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

> **Nota:** En la plataforma ASR1k, el SCP que reconoce VRF no funciona hasta la versión XE3.5S (15.2(1)S).

Verificación

Utilice estos comandos para verificar la configuración.

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

Para copiar un archivo de ASR a un dispositivo remoto con SCP, ingrese este comando:

```
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#
```

Para copiar un archivo desde un dispositivo remoto a ASR con SCP, ingrese este comando:

```
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

Para utilizar el servicio de cliente TFTP en un ASR1k desde una interfaz habilitada para VRF, utilice esta configuración.

Configurar

La opción **ip tftp source-interface** se utiliza para señalar la interfaz de administración al **VRF Mgmt-intf**. No hay otra opción en el comando **copy tftp** para especificar el VRF. Por lo tanto, debe utilizar este comando **ip tftp source-interface**. La misma lógica se aplica a cualquier otra interfaz habilitada para VRF.

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

Verificación

Utilice estos comandos para verificar la configuración.

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

Para copiar un archivo de ASR al servidor TFTP, ingrese este comando:

```
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#
```

Para copiar un archivo desde el servidor TFTP a la memoria flash de inicialización ASR, ingrese este comando:

```
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

Para utilizar el servicio de cliente FTP en un ASR desde una interfaz habilitada para VRF, utilice

esta configuración.

Configurar

La opción **ip ftp source-interface** se utiliza para señalar la interfaz de administración al **VRF Mgmt-intf**. No hay otra opción en el comando **copy ftp** para especificar el VRF. Por lo tanto, debe utilizar el comando **ip ftp source-interface**. La misma lógica se aplica a cualquier otra interfaz habilitada para VRF.

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

Verificación

Utilice estos comandos para verificar la configuración.

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

Para copiar un archivo de ASR a un servidor FTP, ingrese este comando:

```
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#
```

Para copiar un archivo del servidor FTP en la memoria flash de inicialización ASR, ingrese este comando:

```
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#
```

Protocolos de acceso a la gestión

Acceso regular

SSH

> **Precaución:** Un problema común visto con ASR1ks es que el SSH falla debido a la memoria baja. Para obtener más información con respecto a este problema, consulte el artículo de

Cisco SSH Authentication Failure Debido a condiciones de memoria baja.

Hay dos opciones usadas para ejecutar el servicio de cliente SSH en el ASR (SSH desde el paquete). Una opción es especificar el nombre VRF en el propio comando **ssh**, de modo que pueda originar tráfico SSH de un VRF determinado.

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

La otra opción es utilizar la opción **ip ssh source-interface** para originar tráfico SSH desde una interfaz específica habilitada para VRF.

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

Para utilizar el servicio de servidor SSH (SSH to-the-box), siga el procedimiento para habilitar SSH en cualquier otro router Cisco IOS. Refiérase a la sección Descripción General de Telnet y SSH para Cisco ASR 1000 Series Routers de la **Guía de Configuración de Software de Cisco ASR 1000 Series Aggregation Services Routers** para obtener más información.

TELNET

Hay dos opciones usadas para ejecutar el servicio de cliente Telnet en el ASR (Telnet from-the-box). Una opción es especificar la interfaz de origen o el VRF en el propio comando **telnet** como se muestra aquí:

```
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#
```

La otra opción es utilizar el comando **ip telnet source-interface**. Aún debe especificar el nombre VRF en el siguiente paso con el comando **telnet**, como se muestra aquí:

```
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#
```

Para utilizar el servicio de servidor Telnet (Telnet to-the-box), siga el procedimiento para habilitar Telnet en cualquier otro router. Refiérase a la sección Descripción General de Telnet y SSH para Cisco ASR 1000 Series Routers de la **Guía de Configuración de Software de Cisco ASR 1000 Series Aggregation Services Routers** para obtener más información.

HTTP

La interfaz de usuario web heredada que está disponible para todos los routers también está disponible para ASR1K. Habilite el servicio de cliente o servidor HTTP en el ASR como se muestra en esta sección.

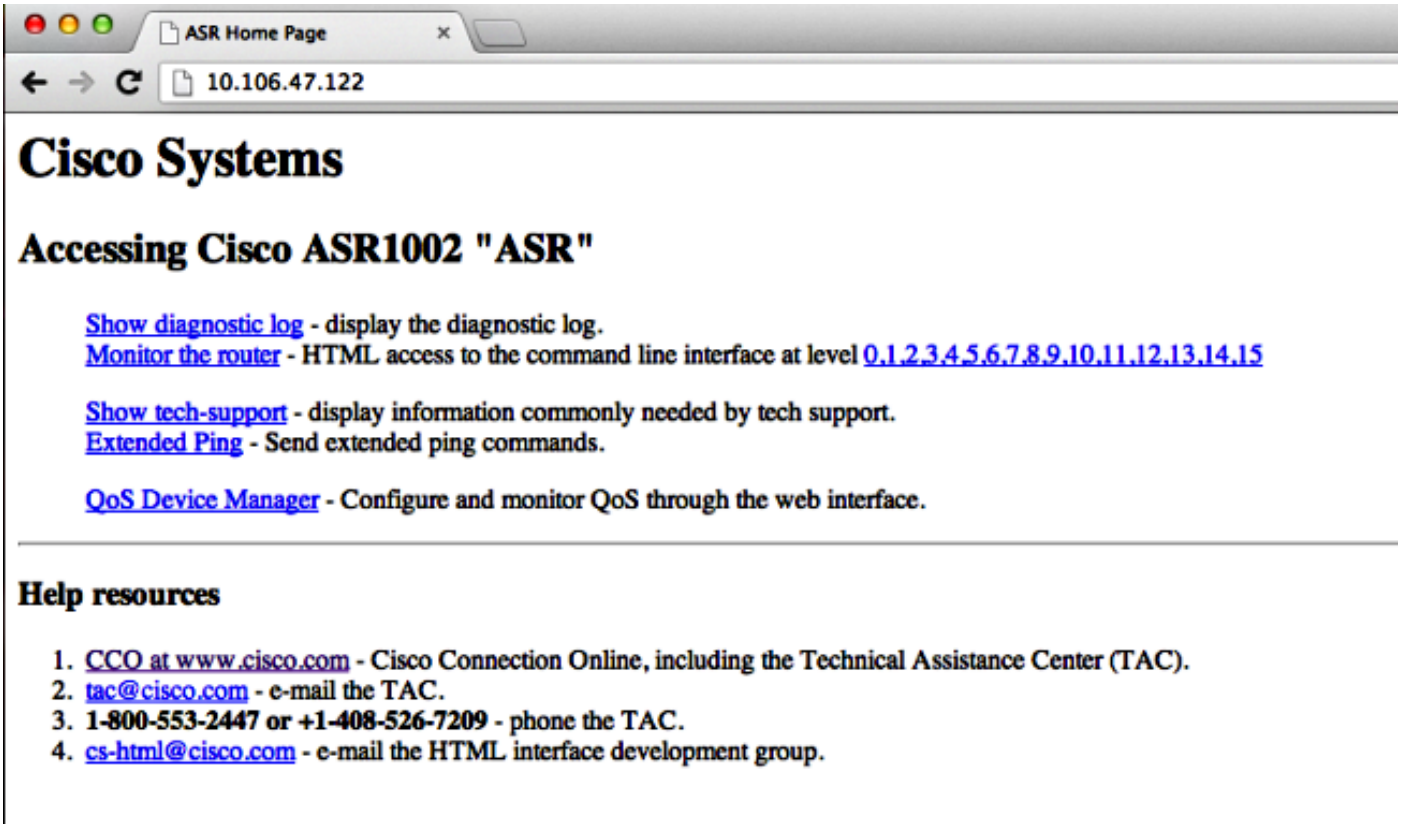
Para habilitar el acceso HTTP antiguo al servicio (servidor) y utilizar el acceso GUI basado en Web, utilice esta configuración que utiliza la autenticación local (también puede utilizar un servidor externo de autenticación, autorización y contabilidad (AAA)).

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

Esta es la configuración para habilitar el servidor seguro HTTP (HTTPS):

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

Busque la dirección IP de una interfaz en el ASR e inicie sesión con la cuenta de usuario que creó. Esta es una captura de pantalla:



Para utilizar el servicio de cliente HTTP, ingrese el **origen de comando ip http client source-interface <interface name>** para el tráfico del cliente HTTP desde una interfaz habilitada para VRF, como se muestra:

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

A continuación se muestra un ejemplo que ilustra el uso del servicio de cliente HTTP para copiar una imagen de un servidor HTTP remoto en la memoria 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#
```

Acceso persistente

Esta sección sólo se aplica a las conexiones Telnet/SSH/HTTP listas para usar.

Con SSH persistente y Telnet persistente, puede configurar un mapa de transporte que defina el tratamiento del tráfico SSH o Telnet entrante en la interfaz Ethernet de administración. Esto crea la capacidad de acceder al router a través del modo de diagnóstico incluso cuando el proceso de Cisco IOS no está activo. Para obtener más información sobre el modo de diagnóstico, refiérase a la sección Introducción al Modo de Diagnóstico de la Guía de Configuración del Software de Routers de Servicios de Agregación de Cisco ASR 1000 Series.

> **Nota:** SSH persistente o Telnet persistente sólo se puede configurar en la interfaz de administración, **GigabitEthernet0.**

Nota: En las versiones que no tienen la corrección para el ID de bug de Cisco CSCuj37515, el método de autenticación para el acceso permanente depende del método que se utiliza bajo la línea **VTY**. El acceso persistente requiere que la autenticación sea local, de modo que el acceso al modo de diagnóstico siga funcionando cuando falla la autenticación externa. Esto significa que cualquier acceso normal de SSH y Telnet también requiere el uso de la autenticación local.

Precaución: En las versiones que no tienen la corrección para el ID de bug Cisco CSCug77654, el uso del método AAA predeterminado restringe la capacidad del usuario para ingresar el mensaje SSH cuando se utiliza SSH persistente. El usuario siempre se ve obligado a ingresar el mensaje de diagnóstico. Para estas versiones, Cisco recomienda que utilice un método de autenticación de nombre o asegúrese de que se habiliten SSH y Telnet normales.

SSH persistente

Cree un mapa de transporte para permitir el SSH persistente como se muestra en la siguiente sección:

Configurar

```
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
```

Ahora debe habilitar la autenticación local para SSH persistente. Esto puede hacerse con el comando **aaa new-model** o sin él. Ambos escenarios se describen aquí. (En cualquier caso, asegúrese de tener una cuenta de nombre de usuario/contraseña local en el router).

Puede elegir qué configuración se basa en si tiene AAA habilitado en el ASR.

1. Con AAA habilitado:

```
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. Sin AAA habilitado:

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

Verificación

SSH al ASR con la dirección IP de la interfaz **Gigabitethernet0** habilitada para VRF. Una vez ingresada la contraseña, debe ingresar la secuencia de interrupción (**Ctrl-C** o **Ctrl-Shift-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)#
```

> **Nota:** Ingrese la secuencia de interrupción (**Ctrl-C** o **Ctrl-Shift-6**) cuando **—Esperando línea vty—** aparezca en el terminal para entrar al modo de diagnóstico.

Telnet persistente

Configurar

Con una lógica similar a la descrita en la sección anterior para SSH, cree un mapa de transporte para Telnet persistente como se muestra aquí:

```
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
```

Como se discute en la última sección para SSH, hay dos maneras de configurar la autenticación local como se muestra aquí:

1. Con AAA habilitado:

```
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. Sin AAA:

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

Verificación

Telnet a la dirección IP de la interfaz **GigabitEthernet0**. Después de ingresar las credenciales, introduzca la secuencia de interrupción y espere unos segundos (a veces puede tardar un tiempo) antes de iniciar sesión en el modo de diagnóstico.

```
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)#
```

> **Nota:** Ingrese la secuencia de interrupción **Ctrl+C** o **Ctrl+Mayús+6**, y espere unos segundos. Cuando **—Esperando el proceso del IOS—** se muestra en el terminal, puede ingresar al modo de diagnóstico.

HTTP persistente

Para habilitar el acceso HTTP continuo al paquete (HTTP desde el paquete o el servicio cliente HTTP no está disponible) y utilizar el nuevo acceso GUI basado en web, utilice esta configuración que utiliza la autenticación local (también puede utilizar un servidor AAA externo).

Configurar

En estas configuraciones, **http-webui** y **https-webui** son los nombres de los mapas de transporte.

```
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
```

Esta es la configuración utilizada para habilitar el servidor seguro 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
```

Verificación

Busque la dirección IP de una interfaz en el ASR. Inicie sesión con el nombre de usuario/contraseña que creó para iniciar la página de inicio. Se muestra información relacionada con el estado y la supervisión, junto con una **interfaz de usuario WebIOS** donde puede aplicar comandos. Esta es una captura de pantalla de la página de inicio:

Troubleshoot

Si WebUI no está disponible a través de HTTPS, verifique que el certificado y la clave Rivest-Shamir-Adleman (RSA) estén presentes y en funcionamiento. Puede utilizar este comando **debug** para determinar la razón por la que la WebUI no se inicia correctamente:

```
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
```

Clave RSA

Para verificar la presencia de la clave RSA, ingrese este comando:

```
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#
```

Tenga en cuenta el nombre de la clave, ya que es necesario para crear el certificado. Si no hay una clave presente, puede crear una con estos comandos:

```
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
```

Certificado

Una vez que la clave está presente, puede ingresar este comando para verificar el certificado:

```
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 el certificado no es válido o no está presente, puede crear el certificado con estos comandos:

```
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
```

Una vez que la clave y el certificado RSA se actualizan y son válidos, el certificado se puede asociar con la configuración HTTPS:

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

A continuación, puede desactivar y volver a habilitar la interfaz de usuario Web para asegurarse de que funciona:

```
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
```

Información Relacionada

- Gestión de puerto de consola, Telnet y SSH
- Introducción al modo de diagnóstico
- Soporte Técnico y Documentación - Cisco Systems