Gerenciamento com reconhecimento de VRF em exemplos de configuração de ASR

Contents

Introduction

Este documento descreve o uso do gerenciamento do Virtual Routing and Forwarding-Aware (VRF-Aware) no Cisco Aggregation Services Router 1000 Series (ASR1K) com a interface de gerenciamento (**GigabitEthernet0**). As informações também se aplicam a qualquer outra interface em um VRF, a menos que explicitamente especificado de outra forma. Vários protocolos de

acesso para cenários **de** conexão **imediata** e **imediata** são descritos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolos de gerenciamento, como SSH, Telnet e HTTP
- Protocolos de transferência de arquivos, como protocolo de cópia segura (SCP), TFTP e FTP
- VRFs

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS® XE Versão 3.5S (15.2(1)S) ou versões posteriores do Cisco IOS-XE
  Note: A SCP com VRF requer pelo menos esta versão, enquanto outros protocolos descritos neste documento também funcionam com versões 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. Se sua rede estiver ativa, certifique-se de que você entendeu o impacto potencial de qualquer comando usado.

Informações de Apoio

Interface de gerenciamento: A finalidade de uma interface de gerenciamento é permitir que os usuários executem tarefas de gerenciamento no roteador. É basicamente uma interface que não deve, e muitas vezes não pode, encaminhar o tráfego de dataplane. Caso contrário, ele pode ser usado para acesso remoto ao roteador, geralmente via Telnet e Secure Shell (SSH), e para executar a maioria das tarefas de gerenciamento no roteador. A interface é mais útil antes que um roteador comece o roteamento ou em cenários de solução de problemas quando as interfaces do Adaptador de porta compartilhada (SPA) estão inativas. No ASR1K, a interface de gerenciamento está em um VRF padrão chamado **Mgmt-intf**.

O comando **ip *<protocol>* source-interface** é usado extensivamente neste documento (onde a palavra-chave *<protocol>* pode ser SSH, FTP, TFTP). Esse comando é usado para especificar o endereço IP de uma interface a ser usada como o endereço de origem quando o ASR é o dispositivo cliente em uma conexão (por exemplo, a conexão é iniciada a partir do ASR ou do tráfego de caixa). Isso também significa que, se o ASR não for o iniciador da conexão, o comando **ip *<protocol>* source-interface** não será aplicável e o ASR não usará esse endereço IP para o tráfego de resposta; em vez disso, ele usa o endereço IP da interface mais próxima do destino. Esse comando permite que você origine tráfego (para os protocolos suportados) de uma interface com VRF-Aware.

Protocolos de gerenciamento

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste artigo.

SCP

Para usar o serviço de cliente SCP em um ASR de uma interface habilitada para VRF, use essa configuração.

Configurar

O comando **ip ssh source-interface** é usado para apontar a interface de gerenciamento para o **Mgmt-intf** VRF para os serviços de cliente SSH e SCP, já que o SCP usa SSH. Não há outra opção no comando **copy scp** para especificar o VRF. Portanto, você deve usar este comando **ip ssh source-interface**. A mesma lógica se aplica a qualquer outra interface habilitada para VRF.

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

> **Note**: Na plataforma ASR1k, a SCP com reconhecimento de VRF não funciona até a versão XE3.5S (15.2(1)S).

Verificar

Use estes comandos para verificar a configuração.

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

Para copiar um arquivo do ASR para um dispositivo remoto com SCP, insira 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 um arquivo de um dispositivo remoto para o ASR com SCP, insira 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 usar o serviço de cliente TFTP em um ASR1k de uma interface habilitada para VRF, use essa configuração.

Configurar

A opção **ip tftp source-interface** é usada para apontar a interface de gerenciamento para o VRF **Mgmt-intf**. Não há outra opção no comando **copy tftp** para especificar o VRF. Portanto, você deve usar este comando **ip tftp source-interface**. A mesma lógica se aplica a qualquer outra interface habilitada para VRF.

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

Verificar

Use estes comandos para verificar a configuração.

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

Para copiar um arquivo do ASR para o servidor TFTP, insira 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 um arquivo do servidor TFTP para o flash de inicialização ASR, digite 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 usar o serviço de cliente FTP em um ASR de uma interface habilitada para VRF, use essa configuração.

Configurar

A opção **ip ftp source-interface** é usada para apontar a interface de gerenciamento para o VRF **Mgmt-intf**. Não há outra opção no comando **copy ftp** para especificar o VRF. Portanto, você deve usar o comando **ip ftp source-interface**. A mesma lógica se aplica a qualquer outra interface habilitada para VRF.

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

Verificar

Use estes comandos para verificar a configuração.

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

Para copiar um arquivo do ASR para um servidor FTP, digite 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 um arquivo do servidor FTP para o flash de inicialização ASR, digite 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 acesso de gerenciamento

Acesso regular

SSH

> **Caution**: Um problema comum observado com os ASR1ks é que o SSH falha devido à falta de memória. Para obter mais informações sobre esse problema, consulte o artigo Falha de autenticação SSH devido a condições de memória baixa da Cisco.

Há duas opções usadas Para executar o serviço de cliente SSH no ASR (SSH da caixa). Uma opção é especificar o nome do VRF no próprio comando **ssh**, para que você possa originar o tráfego SSH de um VRF específico.

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

A outra opção é usar a opção **ip ssh source-interface** para originar o tráfego SSH de uma interface 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 usar o SSH server service (SSH para a caixa), siga o procedimento para ativar o SSH em qualquer outro roteador Cisco IOS. Consulte a Visão Geral do Telnet e do SSH para a seção Cisco ASR 1000 Series Routers do **Guia de Configuração de Software Cisco ASR 1000 Series Aggregation Services Routers** para obter mais informações.

Telnet

Há duas opções usadas para executar o serviço de cliente Telnet no ASR (Telnet a partir da caixa). Uma opção é especificar a interface de origem ou o VRF no próprio comando **telnet**, como mostrado aqui:

```
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#
```

A outra opção é usar o comando **ip telnet source-interface**. Você ainda deve especificar o nome do VRF na próxima etapa com o comando **telnet**, como mostrado aqui:

```
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 usar o serviço de servidor Telnet (Telnet para a caixa), siga o procedimento para ativar o Telnet em qualquer outro roteador. Consulte a Visão Geral do Telnet e do SSH para a seção Cisco ASR 1000 Series Routers do **Guia de Configuração de Software Cisco ASR 1000 Series Aggregation Services Routers** para obter mais informações.

HTTP

A interface de usuário da Web legada que está disponível para todos os roteadores também está disponível para o ASR1K. Ative o servidor HTTP ou o serviço cliente no ASR, como mostrado nesta seção.

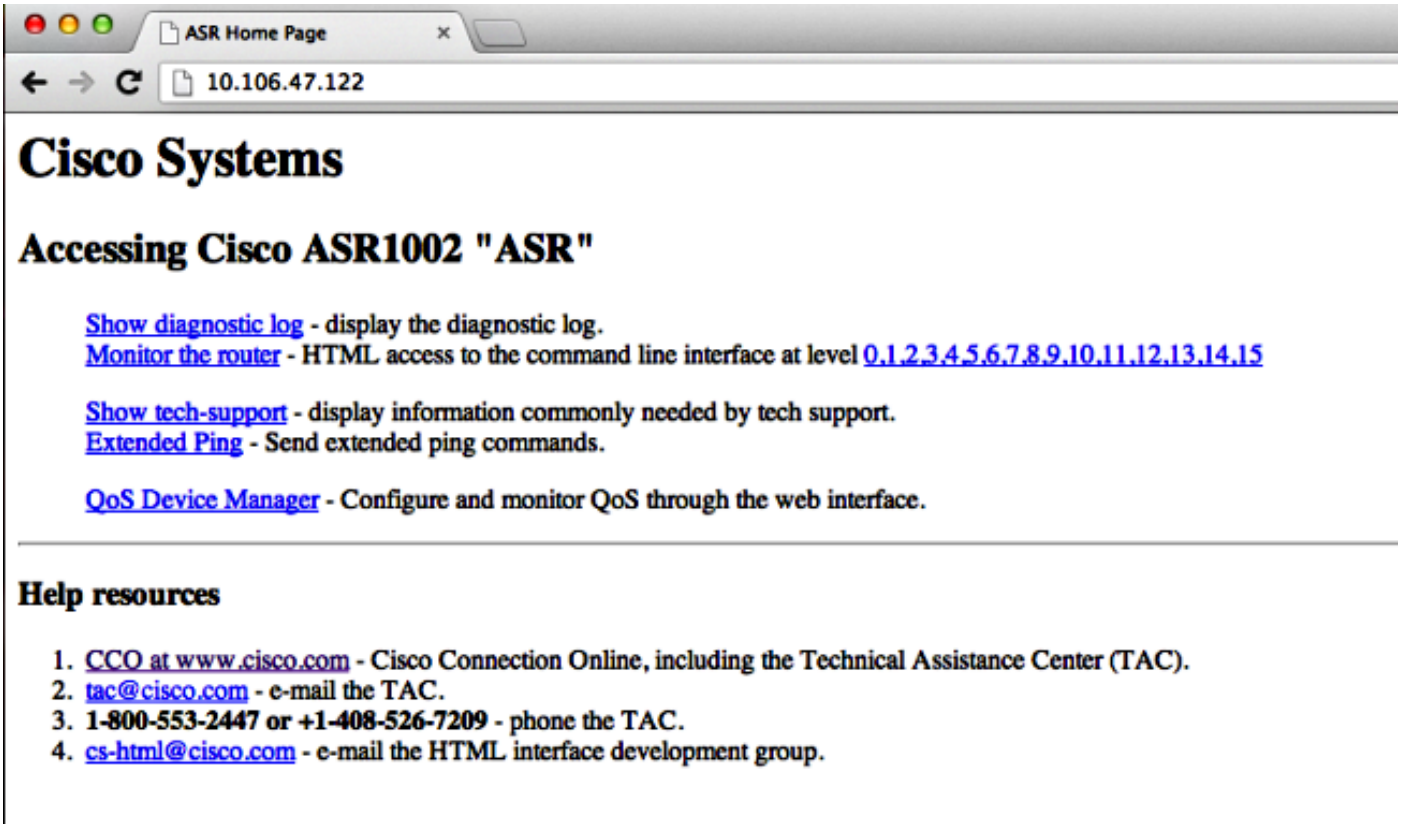
Para habilitar o acesso HTTP legado ao serviço in a box (servidor) e usar o acesso GUI baseado na Web, use esta configuração que usa autenticação local (você também pode usar um servidor AAA (External Authentication, Authorization, and Accounting - Autenticação, Autorização e Contabilidade)).

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

Esta é a configuração para ativar o servidor seguro HTTP (HTTPS):

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

Navegue até o endereço IP de uma interface no ASR e faça login com a conta de usuário que você criou. Aqui está uma imagem:



Para usar o serviço de cliente HTTP, insira a origem do comando **ip http client source-interface <nome da interface>** para o tráfego de cliente HTTP de uma interface habilitada para VRF, como mostrado:

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

Aqui está um exemplo que ilustra o uso do serviço de cliente HTTP para copiar uma imagem de um servidor HTTP remoto para a memória 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#
```

Acesso persistente

Esta seção é aplicável somente para conexões Telnet/SSH/HTTP prontas para uso.

Com SSH persistente e Telnet persistente, você pode configurar um mapa de transporte que define o tratamento do tráfego de entrada SSH ou Telnet na interface Ethernet de gerenciamento. Isso cria a capacidade de acessar o roteador através do modo de diagnóstico mesmo quando o processo do Cisco IOS não está ativo. Para obter mais informações sobre o modo de diagnóstico, consulte a seção Understanding the Diagnostic Mode do Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide.

> **Note**: SSH persistente ou Telnet persistente só podem ser configurados na interface de gerenciamento, **GigabitEthernet0.**

Note: Em versões que não têm a correção para o bug da Cisco ID CSCuj37515, o método de autenticação para acesso persistente depende do método usado na linha **VTY**. O acesso persistente exige que a autenticação seja local, de modo que o acesso ao modo de diagnóstico ainda funcione quando a autenticação externa falhar. Isso significa que qualquer SSH normal e acesso Telnet também exige o uso da autenticação local.

Caution: Em versões que não têm a correção para o bug da Cisco ID CSCug7654, o uso do método AAA padrão restringe a capacidade do usuário de entrar no prompt SSH quando o SSH persistente é usado. O usuário é sempre forçado a entrar no prompt de diagnóstico. Para essas versões, a Cisco recomenda que você use um método de autenticação de nome ou assegure-se de que o SSH e o Telnet normais estejam ativados.

SSH persistente

Crie um mapa de transporte para permitir SSH persistente como mostrado na próxima seção:

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
```

Agora você deve habilitar a autenticação local para SSH persistente. Isso pode ser feito com o comando **aaa new-model** ou sem ele. Os dois cenários são descritos aqui. (Em ambos os casos, verifique se você tem uma conta local de nome de usuário/senha no roteador).

Você pode escolher qual configuração com base se a AAA está habilitada no ASR.

1. Com 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. Sem AAA habilitado:

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

Verificar

SSH para o ASR com o endereço IP da interface **Gigabitethernet0** habilitada para VRF. Depois que a senha for digitada, você deverá inserir a sequência de interrupção (**Ctrl-C** ou **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)#
```

> **Note**: Insira a sequência de interrupção (**Ctrl-C** ou **Ctrl-Shift-6**) quando **—Esperando pela linha vty—** for exibido no terminal para entrar no modo de diagnóstico.

Telnet persistente

Configurar

Com uma lógica semelhante à descrita na seção anterior para SSH, crie um mapa de transporte para Telnet persistente, como mostrado aqui:

```
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
```

Conforme discutido na última seção para SSH, há duas maneiras de configurar a autenticação local, como mostrado aqui:

1. Com 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. Sem AAA:

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

Verificar

Faça Telnet para o endereço IP da interface **GigabitEthernet0**. Depois de inserir as credenciais, insira a sequência de interrupção e aguarde alguns segundos (às vezes, pode demorar um pouco) antes de fazer login no 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)#
```

> **Note**: Digite a sequência de interrupção **Ctrl+C** ou **Ctrl+Shift+6**, e aguarde alguns segundos. Quando **—Aguardando o processo do IOS—** for exibido no terminal, você poderá entrar no modo de diagnóstico.

HTTP persistente

Para habilitar o acesso HTTP persistente à caixa (o HTTP da caixa ou o serviço cliente HTTP não está disponível) e usar o novo acesso GUI baseado na Web, use esta configuração que utiliza autenticação local (você também pode usar um servidor AAA externo).

Configurar

Nessas configurações, **http-webui** e **https-webui** são os nomes dos 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 é a configuração usada para habilitar o HTTP secure server (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
```

Verificar

Navegue até o endereço IP de uma interface no ASR. Faça login com o nome de usuário/senha que você criou para iniciar a página inicial. As informações relacionadas à integridade e ao monitoramento são exibidas juntamente com uma **IU** da **Web do IOS** onde você pode aplicar comandos. Aqui está uma imagem da página inicial:

Troubleshoot

Se a WebUI não estiver disponível via HTTPS, verifique se o certificado e a chave Rivest-Shamir-

Adleman (RSA) estão presentes e operacionais. Você pode usar este comando **debug** para determinar o motivo pelo qual a WebUI não é iniciada corretamente:

```
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
```

chave RSA

Para verificar a presença da chave RSA, insira 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#
```

Anote o nome da chave, conforme necessário, para criar o certificado. Se uma chave não estiver presente, você pode criar uma com estes 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

Quando a chave estiver presente, você poderá inserir este comando para verificar o 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
```

Se o certificado for inválido ou não estiver presente, você poderá criar o certificado com estes 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
```

Depois que a chave e o certificado RSA são atualizados e válidos, o certificado pode ser associado à configuração HTTPS:

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

Em seguida, você pode desativar e reativar a WebUI para garantir que ela esteja funcional:

```
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
```

Informações Relacionadas

- Porta de Console, Telnet e Manuseio SSH
- Entendendo o modo de diagnóstico
- Suporte Técnico e Documentação - Cisco Systems