ASR上的VRF感知管理配置示例

目录

简介

本文档介绍在带有管理接口(GigabitEthernet0)的思科聚合服务路由器1000系列(ASR1K)上使用虚拟路由和转发感知(VRF-Aware)**管理**。 除非明确指定，否则该信息也适用于VRF中的任何其他接口。描述了用于**机箱间和机箱间连接方案的**各种访问协议。

先决条件

要求

Cisco 建议您了解以下主题：

- 管理协议，例如SSH、Telnet和HTTP
- 文件传输协议，如安全复制协议(SCP)、TFTP和FTP
- VRF

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® XE版本3.5S(15.2(1)S)或更高版本Cisco IOS-XE版本
  注意：VRF感知SCP至少需要此版本，而本文档中描述的其他协议也适用于以前的版本。
- ASR1K

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解使用的任何命令的潜在影响。

背景信息

管理接口:管理接口的目的是允许用户在路由器上执行管理任务。它基本上是一个不应转发数据平面流量的接口，而且通常不能转发数据平面流量。否则，它可用于远程访问路由器(通常通过Telnet和安全外壳(SSH))，以及在路由器上执行大多数管理任务。该接口在路由器开始路由之前或在共享端口适配器(SPA)接口处于非活动状态的故障排除场景中最有用。在ASR1K上，管理接口位于名为Mgmt-intf的**默认VRF中**。

本文**中*广泛使用*ip *<protocol> source-interface*命令(*其中*<*protocol*>**关键字可以是SSH、FTP、TFTP)。 当ASR是连接中的客户端设备时，此命令用于指定要用作源地址的接口的IP地址（例如，从ASR或设备流量发起连接）。 这也意味着，如果ASR不是连接的发起者，则**ip *<protocol>* source-interface** 命令不适用，并且ASR不将此IP地址用于应答流量；相反，它使用距离目的地最近的接口的IP地址。此命令允许您从VRF感知接口（针对支持的协议）来源流量。

管理协议

> **注意**：使用命令查找工具(仅注册客户)可获取有关本文中使用的命令的详细信息。

SCP

要从启用VRF的接口在ASR上使用SCP客户端服务，请使用此配置。

配置

由于SCP使用SSH，因此**ip ssh source-interface** 命令用于将管理接口指向**Mgmt-intf** VRF，以用于

SSH和SCP客户端服务。**copy scp** 命令中没有其他选项来指定VRF。因此，您必须使用**此ip ssh source-interface命**令。同样的逻辑适用于任何其他启用VRF的接口。

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

注意：在ASR1k平台上，VRF感知SCP直到版本XE3.5S(15.2(1)S)才起作用。

验证

使用以下命令检验配置。

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

要使用SCP将文件从ASR复制到远程设备，请输入以下命令：

```
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#
```

要使用SCP将文件从远程设备复制到ASR，请输入以下命令：

```
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

要从启用VRF的接口在ASR1k上使用TFTP客户端服务，请使用此配置。

配置

使**用ip tftp source-interface**选项将管理接口指向**Mgmt-intf VRF**。copy tftp命令中没有其他选项**来指定VRF。**因此，您必须使用**ip tftp source-interface命**令。同样的逻辑适用于任何其他启用VRF的接口。

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

验证

使用以下命令检验配置。

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

要将文件从ASR复制到TFTP服务器，请输入以下命令：

```
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#
```

要将文件从TFTP服务器复制到ASR bootflash，请输入以下命令：

```
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

要从启用VRF的接口在ASR上使用FTP客户端服务，请使用此配置。

配置

使用**ip ftp source-interface选项**将管理接口指向Mgmt-intf **VRF**。copy ftp命令中没有其他**选项**可指定VRF。因此，您必须使用**ip ftp source-interface**命令。同样的逻辑适用于任何其他启用VRF的接口。

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

验证

使用以下命令检验配置。

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

要将文件从ASR复制到FTP服务器，请输入以下命令：

```
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#
```

要将文件从FTP服务器复制到ASR bootflash，请输入以下命令：

```
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#
```

管理访问协议

常规访问

SSH

> **警告**：ASR1k中出现的一个常见问题是SSH因内存不足而失败。有关此问题的详细信息，请参阅“SSH Authentication Failure Due To Low Memory Conditions（由于内存不足导致SSH身份验证失败）”一文。

在ASR（SSH出厂）上运行SSH客户端服务时，使用了两个选项。 一个选项是在**ssh**命令本身中指定VRF名称，以便您可以从特定VRF源SSH流量。

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

另一个选项是使用**ip ssh source-interface**选项，以便从启用VRF的特定接口发送SSH流量。

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

要使用SSH服务器服务（SSH到机箱），请按照程序在任何其他Cisco IOS路由器上启用SSH。有关详细信息，请参阅《Cisco ASR 1000系列聚合服务路由器软件配置指南》中的**Telnet和SSH概述**部分。

Telnet

在ASR上运行Telnet客户端服务（从机箱Telnet）时使用两个选项。 一个选项是在**telnet**命令本身中指定源接口或VRF，如下所示：

```
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#
```

另一个选项是使用**ip telnet source-interface**命令。在下一步中，您仍必须使用**telnet**命令指定VRF名称，如下所示：

```
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#
```

要使用Telnet服务器服务（Telnet到设备），请按照程序在任何其他路由器上启用Telnet。有关详细信息，请参阅《Cisco ASR 1000系列聚合服务路由器软件配置指南》中的**Telnet和SSH概述**部分。

HTTP

ASR1K也提供适用于所有路由器的传统Web用户界面。在ASR上启用HTTP服务器或客户端服务，如本部分所示。

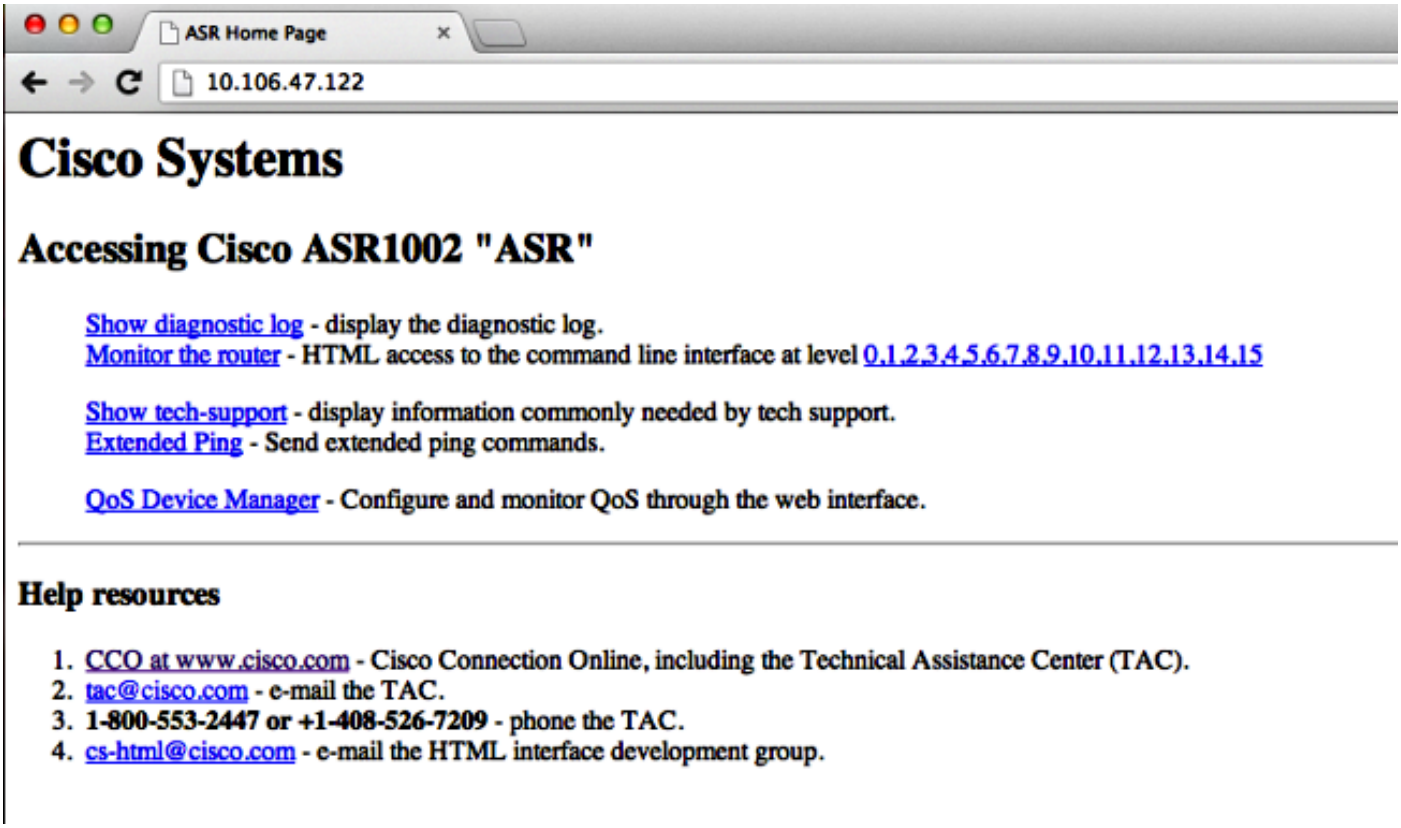
要启用传统HTTP对设备服务（服务器）的访问并使用基于Web的GUI访问，请使用使用本地身份验证的此配置(您还可以使用外部身份验证、授权和记帐(AAA)服务器)。

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

以下是启用HTTP安全服务器(HTTPS)的配置：

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

浏览到ASR上接口的IP地址，然后使用您创建的用户帐户登录。以下是屏幕截图：



要使用HTTP客户端服务，请输入**ip http client source-interface <interface name>**命令源，用于从启用VRF的接口传输HTTP客户端流量，如图所示：

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

以下示例说明使用HTTP客户端服务将镜像从远程HTTP服务器复制到闪存：

```
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#
```

持久访问

本节仅适用于开箱即用的Telnet/SSH/HTTP连接。

通过持久SSH和持久Telnet，您可以配置传输映射，该映射定义管理以太网接口上传入SSH或Telnet流量的处理。因此，即使Cisco IOS进程处于非活动状态，也能通过诊断模式访问路由器。有关诊断模式的详细信息，请参阅《Cisco ASR 1000系列聚合服务路由器软件配置指南》的“了解诊断模式”部分。

注意：只能在管理接口GigabitEthernet0上配置持久SSH或持久**Telnet。**

注意：在没有修复Cisco Bug ID CSCuj37515的版本中，永久访问的身份验证方法取决于线路VTY下使用的**方法**。持久访问要求身份验证是本地的，这样，当外部身份验证失败时，诊断模式访问仍然有效。这意味着任何正常的SSH和Telnet访问也需要使用本地身份验证。

警告：在没有修复Cisco Bug ID CSCug77654的版本中，使用默认AAA方法会限制用户在使用永久SSH时进入SSH提示的能力。用户始终被强制进入诊断提示。对于这些版本，思科建议您使用名称身份验证方法，或确保启用正常的SSH和Telnet。

持久SSH

创建传输映射以允许持久SSH，如下一节所示：

配置

```
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
```

现在，您必须为永久SSH启用本地身份验证。这可以使用aaa new-model**命令或不**使用它来完成。这里描述了这两种情况。（无论哪种情况，请确保路由器上有本地用户名/密码帐户）。

您可以根据是否在ASR上启用了AAA来选择配置。

1. 启用AAA时：

```
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. 未启用AAA:

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

验证

使用启用VRF的Gigabitethernet0接口的IP地址SSH**到ASR**。输入密码后，必须输入中断序列(**Ctrl-C**或**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)#
```

注意：当 — Waiting for vty line — 显示在终端上以进入诊断模式时，输入中断序列（Ctrl-C或Ctrl-Shift-6）。

持久Telnet

配置

使用上一节所述的类似SSH逻辑，创建持久性Telnet的传输映射，如下所示：

```
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
```

如SSH的最后一节所述，配置本地身份验证有两种方法，如下所示：

1. 启用AAA时：

```
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. 没有AAA:

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

验证

Telnet至GigabitEthernet0接口的IP地址。在输入凭证后，输入中断序列，并等待几秒钟（有时可能需要一段时间），然后登录诊断模式。

```
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)#
```

> **注意：**输入中断**序列Ctrl+C**或**Ctrl+Shift+6**，然后等待几秒钟。When **- Waiting for IOS Process -**在终端上显示，您可以进入诊断模式。

持久HTTP

要启用永久的HTTP随机访问（HTTP随机访问或HTTP客户端服务不可用）并使用新的基于Web的GUI访问，请使用此配置（使用外部AAA服务器）来进行本地身份验证。

配置

在这些配置中，**http-webui**和**https-webui**是传输映射的名称。

```
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
```

以下是用于启用HTTP安全服务器(HTTPS)的配置。

```
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
```

验证

浏览到ASR上接口的IP地址。使用您为启动主页而创建的用户名/密码登录。系统随即会显示运行状况和监控相关信息，**以及可**以在其中应用命令的IOS WebUI。以下是主页的截图：

故障排除

如果WebUI不能通过HTTPS使用，则验证证书和Rivest-Shamir-Adleman(RSA)密钥是否存在且可操作。您可以使用此**debug**命令来确定WebUI未正确启动的原因：

```
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 密钥

要验证是否存在RSA密钥，请输入以下命令：

```
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#
```

请注意密钥名称，因为创建证书时需要该名称。如果密钥不存在，可以使用以下命令创建一个密钥

：

```
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
```

证书

一旦密钥存在，您可以输入以下命令以验证证书：

```
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
```

如果证书无效或不存在，则可以使用以下命令创建证书：

```
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
```

更新RSA密钥和证书并使其有效后，证书可以与HTTPS配置关联：

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

然后，您可以禁用并重新启用WebUI，以确保其正常运行：

```
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
```

相关信息

- 控制台端口、Telnet和SSH处理
- 了解诊断模式
- 技术支持和文档 - Cisco Systems