VRF-kompatibles Management für ASR-Konfigurationen

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Managementprotokolle](#)
[SCP](#)
[Konfigurieren](#)
[Überprüfen](#)
[TFTP](#)
[Konfigurieren](#)
[Überprüfen](#)
[FTP](#)
[Konfigurieren](#)
[Überprüfen](#)
[Management-Zugriffsprotokolle](#)
[Regulärer Zugriff](#)
[SSH](#)
[Telnet](#)
[HTTP](#)
[Persistenter Zugriff](#)
[Dauerhafte SSH](#)
[Persistent Telnet](#)
[Persistent HTTP](#)
[Fehlerbehebung](#)
[RSA-Schlüssel](#)
[Zertifikat](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Verwendung von VRF-orientiertem (Virtual Routing and Forwarding-Aware) Management auf dem Cisco Aggregation Services Router der Serie 1000 (ASR1K) mit der Verwaltungsschnittstelle (**GigabitEthernet0**) beschrieben. Sofern nicht ausdrücklich anders angegeben, gelten die Informationen auch für alle anderen Schnittstellen in einer VRF-Instanz. Es

werden verschiedene Zugriffsprotokolle für **die** jeweils **sofort** einsatzbereite Verbindung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Verwaltungsprotokolle wie SSH, Telnet und HTTP
- Dateiübertragungsprotokolle wie Secure Copy Protocol (SCP), TFTP und FTP
- VRFs

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® XE Version 3.5S (15.2(1)S) oder spätere Cisco IOS-XE-Versionen
  Hinweis: VRF-kompatibles SCP erfordert mindestens diese Version, während andere in diesem Dokument beschriebene Protokolle auch mit früheren Versionen kompatibel sind.
- ASR1K

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines verwendeten Befehls verstehen.

Hintergrundinformationen

Verwaltungsschnittstelle: Der Zweck einer Verwaltungsschnittstelle besteht darin, Benutzern die Durchführung von Verwaltungsaufgaben auf dem Router zu ermöglichen. Es handelt sich im Grunde um eine Schnittstelle, die Datenverkehr an die Datenebene nicht weiterleiten sollte und kann. Andernfalls kann sie für den Remote-Zugriff auf den Router, häufig über Telnet und Secure Shell (SSH), und für die meisten Verwaltungsaufgaben auf dem Router verwendet werden. Die Schnittstelle ist vor Beginn des Routings eines Routers oder bei Problembehebungsszenarien besonders nützlich, wenn die SPA-Schnittstellen (Shared Port Adapter) inaktiv sind. Auf dem ASR1K befindet sich die Verwaltungsschnittstelle in einer Standard-VRF-Instanz mit dem Namen **Mgmt-intf**.

Der Befehl **ip *<protocol>*source-interface** wird in diesem Dokument umfassend verwendet (wobei das *<protocol>*-Schlüsselwort SSH, FTP, TFTP sein kann). Mit diesem Befehl wird die IP-Adresse einer Schnittstelle angegeben, die als Quelladresse verwendet werden soll, wenn ASR das Client-Gerät in einer Verbindung ist (z. B. wird die Verbindung vom ASR oder vom Posteingang aus initiiert). Dies bedeutet auch, dass, wenn ASR nicht der Initiator der Verbindung ist, der Befehl **ip *<protocol>* Source-Interface** nicht anwendbar ist und ASR diese IP-Adresse nicht für den Antwortverkehr verwendet. Stattdessen wird die IP-Adresse der Schnittstelle verwendet, die dem

Ziel am nächsten liegt. Mit diesem Befehl können Sie Datenverkehr (für die unterstützten Protokolle) von einer VRF-kompatiblen Schnittstelle auslösen.

Managementprotokolle

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Artikel verwendeten Befehlen zu erhalten.

SCP

Verwenden Sie diese Konfiguration, um den SCP-Client-Service auf einem ASR von einer VRF-fähigen Schnittstelle zu verwenden.

Konfigurieren

Der Befehl **ip ssh source-interface** wird verwendet, um die Management-Schnittstelle für SSH- und SCP-Clientdienste auf die **Mgmt-intf-**VRF-Instanz zu verweisen, da SCP SSH verwendet. Der Befehl **copy scp** bietet keine andere Option zum Angeben der VRF-Instanz. Aus diesem Grund müssen Sie den Befehl **ip ssh source-interface** verwenden. Die gleiche Logik gilt für alle anderen VRF-fähigen Schnittstellen.

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

> **Hinweis**: Auf der ASR1k-Plattform funktioniert VRF-kompatibles SCP erst mit Version XE3.5S (15.2(1)S).

Überprüfen

Verwenden Sie diese Befehle, um die Konfiguration zu überprüfen.

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

Geben Sie den folgenden Befehl ein, um eine Datei von ASR auf ein Remote-Gerät mit SCP zu kopieren:

```
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#
```

Geben Sie den folgenden Befehl ein, um eine Datei von einem Remote-Gerät mit SCP in ASR zu kopieren:

```
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

Verwenden Sie diese Konfiguration, um den TFTP-Client-Dienst auf einem ASR1k von einer VRF-fähigen Schnittstelle zu verwenden.

Konfigurieren

Die Option **ip tftp source-interface** wird verwendet, um die Management-Schnittstelle auf die **Mgmt-intf-**VRF zu verweisen. Der Befehl **copy tftp** bietet keine andere Option zum Angeben der VRF-Instanz. Daher müssen Sie diesen Befehl **ip tftp source-interface** verwenden. Die gleiche Logik gilt für alle anderen VRF-fähigen Schnittstellen.

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

Überprüfen

Verwenden Sie diese Befehle, um die Konfiguration zu überprüfen.

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

Geben Sie den folgenden Befehl ein, um eine Datei vom ASR auf den TFTP-Server zu kopieren:

```
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#
```

Geben Sie den folgenden Befehl ein, um eine Datei vom TFTP-Server in den ASR-Bootflash zu kopieren:

```
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

Verwenden Sie diese Konfiguration, um den FTP-Client-Dienst auf einem ASR von einer VRF-fähigen Schnittstelle zu verwenden.

Konfigurieren

Die Option **ip ftp source-interface** wird verwendet, um die Management-Schnittstelle auf die **Mgmt-intf-**VRF zu verweisen. Der Befehl **copy ftp** bietet keine andere Option zum Angeben der VRF-Instanz. Daher müssen Sie den Befehl **ip ftp source-interface** verwenden. Die gleiche Logik gilt für alle anderen VRF-fähigen Schnittstellen.

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

Überprüfen

Verwenden Sie diese Befehle, um die Konfiguration zu überprüfen.

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

Geben Sie den folgenden Befehl ein, um eine Datei vom ASR auf einen FTP-Server zu kopieren:

```
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#
```

Geben Sie den folgenden Befehl ein, um eine Datei vom FTP-Server in den ASR-Bootflash zu kopieren:

```
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#
```

Management-Zugriffsprotokolle

Regulärer Zugriff

SSH

> **Vorsicht**: Ein häufiges Problem bei ASR1ks ist, dass das SSH aufgrund eines niedrigen Speichers fehlschlägt. Weitere Informationen zu diesem Problem finden Sie im Cisco-Artikel SSH Authentication Failure Wegen Low Memory Conditions (SSH-Authentifizierungsfehler aufgrund von Bedingungen für niedrigen Arbeitsspeicher).

Für die Ausführung des SSH-Clientdienstes auf dem ASR (SSH von vorn) werden zwei Optionen verwendet. Eine Möglichkeit besteht darin, den VRF-Namen im Befehl **ssh** selbst anzugeben, damit Sie SSH-Datenverkehr von einer bestimmten VRF-Instanz beziehen können.

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

Die andere Option besteht darin, die Option **ip ssh source-interface** zu verwenden, um SSH-Datenverkehr von einer bestimmten VRF-fähigen Schnittstelle zu beziehen.

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

Um den SSH-Serverdienst (SSH to the Box) zu verwenden, gehen Sie wie folgt vor, um SSH auf einem anderen Cisco IOS-Router zu aktivieren. Weitere Informationen finden Sie im Abschnitt Telnet und SSH Overview für die Router der Cisco Serie ASR 1000 im **Software-Konfigurationsleitfaden für Cisco Aggregation Services Router der Serie ASR 1000**.

Telnet

Es gibt zwei Optionen, um den Telnet-Client-Service auf dem ASR (Telnet von der Box aus) auszuführen. Eine Möglichkeit besteht darin, die Quell-Schnittstelle oder die VRF-Instanz im Befehl **telnet** selbst anzugeben, wie hier gezeigt:

```
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#
```

Die andere Option ist die Verwendung des Befehls **ip telnet source-interface**. Sie müssen den VRF-Namen trotzdem im nächsten Schritt mit dem Befehl **telnet** angeben, wie hier gezeigt:

```
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#
```

Um den Telnet-Serverdienst (Telnet-to-the-box) zu verwenden, gehen Sie wie folgt vor, um Telnet auf einem anderen Router zu aktivieren. Weitere Informationen finden Sie im Abschnitt Telnet und SSH Overview für die Router der Cisco Serie ASR 1000 im **Software-Konfigurationsleitfaden für Cisco Aggregation Services Router der Serie ASR 1000**.

HTTP

Die veraltete Web-Benutzeroberfläche, die für alle Router verfügbar ist, ist auch für den ASR1K verfügbar. Aktivieren Sie den HTTP-Server- oder Client-Service auf dem ASR, wie in diesem Abschnitt gezeigt.

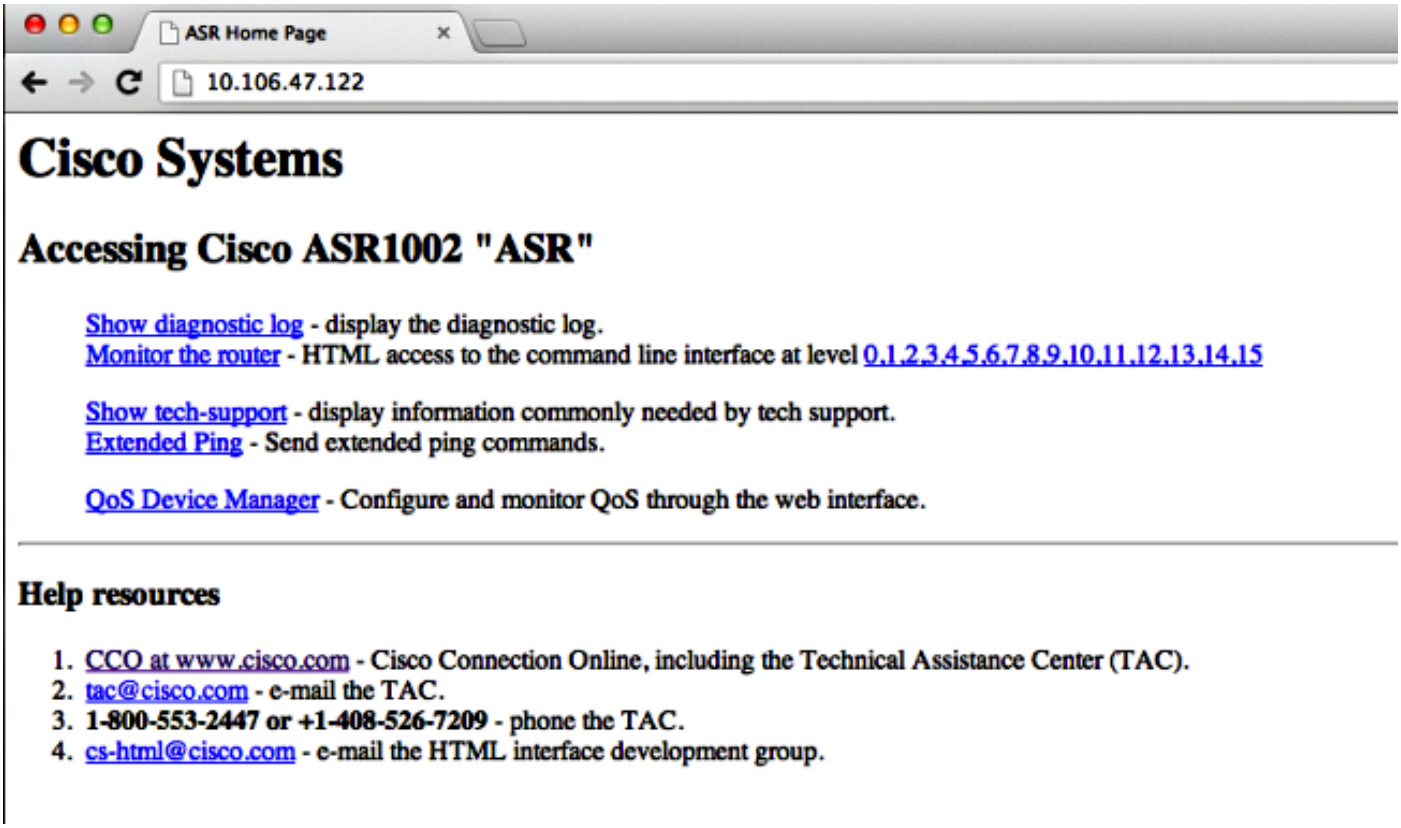
Um den veralteten HTTP-Zugriff auf den Posteingang-Service (Server) zu aktivieren und den webbasierten GUI-Zugriff zu verwenden, verwenden Sie diese Konfiguration mit lokaler Authentifizierung (Sie können auch einen externen AAA-Server (Authentication, Authorization, Accounting) verwenden).

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

Die folgende Konfiguration dient zum Aktivieren des sicheren HTTP-Servers (HTTPS):

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

Navigieren Sie zur IP-Adresse einer Schnittstelle auf dem ASR, und melden Sie sich mit dem von Ihnen erstellten Benutzerkonto an. Hier ein Screenshot:



Um den HTTP-Client-Dienst zu verwenden, geben Sie die **ip http client source-interface <interface name>** Befehlsquelle für den HTTP-Client-Datenverkehr von einer VRF-fähigen Schnittstelle ein, wie folgt:

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

Im folgenden Beispiel wird die Verwendung des HTTP-Clientdiensts veranschaulicht, um ein Bild von einem entfernten HTTP-Server in den Flash zu kopieren:

```
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#
```

Persistenter Zugriff

Dieser Abschnitt gilt nur für interne Telnet-/SSH-/HTTP-Verbindungen.

Mit persistenten SSHs und persistenten Telnet-Verbindungen können Sie eine Transportübersicht konfigurieren, die die Behandlung des eingehenden SSH- oder Telnet-Datenverkehrs auf der Management Ethernet-Schnittstelle definiert. Dadurch wird der Zugriff auf den Router auch dann über den Diagnosemodus möglich, wenn der Cisco IOS-Prozess nicht aktiv ist. Weitere Informationen zum Diagnosemodus finden Sie im Abschnitt Understanding the Diagnostic Mode (Diagnosemodus) im Software-Konfigurationsleitfaden für Cisco Aggregation Services Router der Serie ASR 1000.

Hinweis: Persistent SSH oder persistentes Telnet kann nur auf der Management-

Schnittstelle **GigabitEthernet0** konfiguriert werden.

Hinweis: In Versionen, die nicht über die Behebung der Cisco Bug-ID CSCuj37515 verfügen, hängt die Authentifizierungsmethode für den permanenten Zugriff von der Methode ab, die unter Leitung **VTY** verwendet wird. Für den permanenten Zugriff ist eine lokale Authentifizierung erforderlich, sodass der Diagnosemodus-Zugriff auch dann funktioniert, wenn die externe Authentifizierung fehlschlägt. Das bedeutet, dass für jeden normalen SSH- und Telnet-Zugriff auch eine lokale Authentifizierung erforderlich ist.

Vorsicht: In Versionen, die nicht die Behebung für die Cisco Bug-ID CSCug77654 aufweisen, schränkt die Verwendung der standardmäßigen AAA-Methode die Benutzer ein, die SSH-Eingabeaufforderung einzugeben, wenn persistentes SSH verwendet wird. Der Benutzer muss immer die Diagnoseaufforderung eingeben. Für diese Versionen empfiehlt Cisco die Verwendung einer Namensauthentifizierungsmethode oder die Aktivierung von normalem SSH und Telnet.

Dauerhafte SSH

Erstellen Sie eine Transportübersicht, um persistentes SSH zuzulassen, wie im nächsten Abschnitt gezeigt:

Konfigurieren

```
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
```

Sie müssen jetzt die lokale Authentifizierung für persistente SSH aktivieren. Dies kann entweder mit dem Befehl **aaa new-model** oder ohne den Befehl erfolgen. Beide Szenarien werden hier beschrieben. (Stellen Sie in beiden Fällen sicher, dass Sie über ein lokales Benutzername/Kennwort-Konto auf dem Router verfügen.)

Sie können die Konfiguration basierend darauf auswählen, ob AAA auf dem ASR aktiviert ist.

1. Bei aktiviertem AAA:

```
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. Ohne AAA-Aktivierung:

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

Überprüfen

SSH an den ASR mit der IP-Adresse der VRF-fähigen **GigabitEthernet0-**Schnittstelle. Nach Eingabe des Kennworts müssen Sie die Unterbrechungsfolge eingeben (**Strg-C** oder **Strg-Umschalt-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)#
```

> **Hinweis**: Geben Sie die Break-Sequenz (**Strg-C** oder **Strg-Umschalt-6**) ein, wenn **—Wartet auf VTY-Zeile—** im Terminal angezeigt wird, um in den Diagnosemodus zu wechseln.

Persistent Telnet

Konfigurieren

Erstellen Sie mit ähnlicher Logik, wie im vorherigen Abschnitt für SSH beschrieben, eine Transportübersicht für persistentes Telnet, wie hier gezeigt:

```
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
```

Wie im letzten Abschnitt zu SSH erläutert, gibt es zwei Möglichkeiten, die lokale Authentifizierung zu konfigurieren, wie hier gezeigt:

1. Bei aktiviertem AAA:

```
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. Ohne AAA:

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

Überprüfen

Telnet an die IP-Adresse der **GigabitEthernet0-**Schnittstelle. Wenn Sie die Anmeldeinformationen eingegeben haben, geben Sie die Break-Sequenz ein, und warten Sie einige Sekunden (manchmal kann es eine Weile dauern), bevor Sie sich im Diagnosemodus anmelden.

```
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)#
```

> **Hinweis**: Geben Sie die Break-Sequenz **Strg+C** oder **Strg+Umschalt+6 ein**, und warten Sie einige Sekunden. Wenn **- Warten auf den IOS-Prozess -** im Terminal angezeigt wird, können Sie in den Diagnosemodus wechseln.

Persistent HTTP

Verwenden Sie diese Konfiguration mit lokaler Authentifizierung (Sie können auch einen externen AAA-Server verwenden), um den permanenten HTTP-Zugriff auf das Gerät zu aktivieren (HTTP von der Box oder HTTP-Client-Service ist nicht verfügbar) und den neuen webbasierten GUI-Zugriff zu verwenden.

Konfigurieren

In diesen Konfigurationen sind **http-webui** und **https-webui** die Namen der transport-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
```

Die folgende Konfiguration dient zum Aktivieren von HTTPS (HTTP Secure Server).

```
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
```

Überprüfen

Navigieren Sie zur IP-Adresse einer Schnittstelle auf dem ASR. Melden Sie sich mit dem von Ihnen erstellten Benutzernamen/Kennwort an, um die Startseite zu starten. Es werden Informationen zum Zustand und zur Überwachung sowie eine IOS-Webbenutzeroberfläche angezeigt, auf die Befehle angewendet werden können. Screenshot der Homepage:

Fehlerbehebung

Wenn die WebUI nicht über HTTPS verfügbar ist, überprüfen Sie, ob das Zertifikat und der Rivest-Shamir-Adleman (RSA)-Schlüssel vorhanden und betriebsbereit sind. Sie können diesen **debug**-Befehl verwenden, um den Grund zu bestimmen, warum die WebUI nicht ordnungsgemäß startet:

```
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-Schlüssel

Geben Sie den folgenden Befehl ein, um das Vorhandensein des RSA-Schlüssels zu überprüfen:

```
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#
```

Notieren Sie sich den Schlüsselnamen, der zum Erstellen des Zertifikats erforderlich ist. Wenn kein Schlüssel vorhanden ist, können Sie einen mithilfe der folgenden Befehle erstellen:

```
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
```

Zertifikat

Sobald der Schlüssel vorhanden ist, können Sie den folgenden Befehl eingeben, um das Zertifikat zu überprüfen:

```
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
```

Wenn das Zertifikat ungültig oder nicht vorhanden ist, können Sie das Zertifikat mit den folgenden Befehlen erstellen:

```
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
```

Wenn der RSA-Schlüssel und das RSA-Zertifikat aktualisiert wurden und gültig sind, kann das Zertifikat der HTTPS-Konfiguration zugeordnet werden:

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

Anschließend können Sie die WebUI deaktivieren und erneut aktivieren, um sicherzustellen, dass sie funktioniert:

```
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
```

Zugehörige Informationen

- Konsolenport, Telnet und SSH-Verarbeitung
- Diagnosemodus
- Technischer Support und Dokumentation - Cisco Systems