ASR의 VRF 인식 관리 컨피그레이션 예

목차

소개

이 문서에서는 관리 인터페이스(**GigabitEthernet0**)와 함께 Cisco Aggregation Services Router 1000 Series(ASR1K)에서 VRF 인식(Virtual Routing and Forwarding-Aware) 관리를 사용하는 방법에 대해 설명합니다. 이 정보는 명시적으로 지정되지 않은 한 VRF의 다른 인터페이스에도 적용됩니다.to-the-box 및 **from-the-box** 연결 시나리오에 대한 다양한 액세스 프로토콜**에** 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SSH, 텔넷, HTTP 등의 관리 프로토콜
- SCP(Secure Copy Protocol), TFTP, FTP 등의 파일 전송 프로토콜
- VRF

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE 버전 3.5S(15.2(1)S) 이상 Cisco IOS-XE 버전
  참고:VRF 인식 SCP에는 적어도 이 버전이 필요한 반면, 이 문서에 설명된 다른 프로토콜은 이전 버전에서도 작동합니다.
- ASR1K

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 사용된 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

관리 인터페이스:관리 인터페이스의 목적은 사용자가 라우터에서 관리 작업을 수행할 수 있도록 하는 것입니다.기본적으로 이 인터페이스는 데이터 플레인 트래픽을 전달하지 않아야 하고, 종종 전달할 수 없습니다.그렇지 않으면, 대개 텔넷과 SSH(Secure Shell)를 통해 라우터에 대한 원격 액세스와 라우터에서 대부분의 관리 작업을 수행하는 데 사용할 수 있습니다.이 인터페이스는 라우터가 라우팅을 시작하기 전이나 SPA(Shared Port Adapter) 인터페이스가 비활성 상태일 때 문제 해결 시나리오에서 가장 유용합니다.ASR1K에서 관리 인터페이스는 Mgmt-intf라는 기본 VRF에 **있습니다**.

ip *<protocol>* source-interface 명령은 이 문서에서 광범위하게 사용됩니다(여기서 *<protocol>* 키워드는 SSH, FTP, TFTP일 수 있음). 이 명령은 ASR이 연결의 클라이언트 디바이스인 경우(예: 연결이 ASR 또는 from-the-box 트래픽에서 시작됨) 소스 주소로 사용할 인터페이스의 IP 주소를 지정하는 데 사용됩니다. 이는 ASR이 연결의 개시자가 아닌 경우 **ip *<protocol>* source-interface** 명령을 적용할 수 없고 ASR은 회신 트래픽에 이 IP 주소를 사용하지 않음을 의미합니다.대신 목적지에 가장 가까운 인터페이스의 IP 주소를 사용합니다.이 명령을 사용하면 VRF 인식 인터페이스에서 (지원되는 프로토콜의 경우) 트래픽을 소스 처리할 수 있습니다.

관리 프로토콜

> **참고:**이 문서에서 사용하는 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

SCP

VRF 지원 인터페이스에서 ASR에서 SCP 클라이언트 서비스를 사용하려면 이 구성을 사용합니다.

구성

SCP는 SSH를 사용하므로 SSH 및 SCP 클라이언트 서비스에 대해 관리 인터페이스를 Mgmt-intf VRF로 가리키도록 **ip ssh source-interface** 명령을 사용합니다. **copy scp** 명령에 VRF를 지정하는 다른 옵션은 없습니다.따라서 이 **ip ssh source-interface** 명령을 사용해야 합니다.다른 VRF 지원 인터페이스도 동일한 논리가 적용됩니다.

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

참고:ASR1k 플랫폼에서 VRF 인식 SCP는 버전 XE3.5S(15.2(1)S)가 되어야 작동합니다.

다음을 확인합니다.

컨피그레이션을 확인하려면 다음 명령을 사용합니다.

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

SCP를 사용하여 ASR에서 원격 디바이스로 파일을 복사하려면 다음 명령을 입력합니다.

```
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#
```

SCP를 사용하여 원격 디바이스에서 ASR로 파일을 복사하려면 다음 명령을 입력합니다.

```
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

VRF 지원 인터페이스에서 ASR1k에서 TFTP 클라이언트 서비스를 사용하려면 이 컨피그레이션을 사용합니다.

구성

ip tftp source-interface 옵션은 관리 인터페이스를 Mgmt-**intf** VRF로 가리키도록 사용됩니다.copy tftp 명령에 VRF를 지정하기 위한 다른 옵션은 없습니다.따라서 이 **ip tftp source-interface** 명령을 사용해야 합니다.다른 VRF 지원 인터페이스도 동일한 논리가 적용됩니다.

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

다음을 확인합니다.

컨피그레이션을 확인하려면 다음 명령을 사용합니다.

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

ASR에서 TFTP 서버로 파일을 복사하려면 다음 명령을 입력합니다.

```
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#
```

TFTP 서버에서 ASR bootflash로 파일을 복사하려면 다음 명령을 입력합니다.

```
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

VRF 지원 인터페이스에서 ASR에서 FTP 클라이언트 서비스를 사용하려면 이 구성을 사용합니다.

구성

ip ftp source-interface 옵션은 관리 인터페이스를 Mgmt-**intf** VRF로 가리키도록 사용됩니다.copy ftp 명령에 VRF를 지정하기 위한 다른 옵션은 없습니다.따라서 **ip ftp source-interface** 명령을 사용해야 합니다.다른 VRF 지원 인터페이스도 동일한 논리가 적용됩니다.

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

다음을 확인합니다.

컨피그레이션을 확인하려면 다음 명령을 사용합니다.

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

ASR에서 FTP 서버로 파일을 복사하려면 다음 명령을 입력합니다.

```
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#
```

FTP 서버에서 ASR bootflash로 파일을 복사하려면 다음 명령을 입력합니다.

```
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#
```

관리 액세스 프로토콜

일반 액세스

SSH

> **주의:**ASR1ks에 나타나는 일반적인 문제 중 하나는 메모리가 부족하여 SSH가 실패한다는 것입니다.이 문제에 대한 자세한 내용은 Cisco의 메모리 부족으로 인한 SSH 인증 실패 문서를 참조하십시오.

ASR에서 SSH 클라이언트 서비스(SSH from-the-box)를 실행하기 위해 두 가지 옵션이 사용됩니다. 한 가지 옵션은 **ssh** 명령 자체에서 VRF 이름을 지정하여 특정 VRF에서 SSH 트래픽을 소스 지정할 수 있도록 하는 것입니다.

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

다른 옵션은 특정 VRF 지원 인터페이스에서 SSH 트래픽을 소스**로** 지정하려면 ip ssh source-**interface** 옵션을 사용하는 것입니다.

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

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

SSH 서버 서비스(SSH to-the-box)를 사용하려면 다른 Cisco IOS 라우터에서 SSH를 활성화하는 절차를 수행합니다.자세한 내용은 **Cisco ASR** 1000 Series Aggregation Services Routers Software Configuration Guide의 Cisco ASR 1000 Series Routers 섹션에 대한 텔넷 및 SSH 개요를 참조하십시오.

Telnet

ASR(Telnet from-the-box)에서 텔넷 클라이언트 서비스를 실행하기 위해 두 가지 옵션이 사용됩니다. 한 가지 옵션은 다음과 같이 **telnet** 명령 자체에서 소스 인터페이스 또는 VRF를 지정하는 것입니다.

```
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#
```

다른 옵션은 **ip telnet source-interface** 명령을 사용하는 것입니다.**telnet** 명령과 함께 다음 단계에서 VRF 이름을 지정해야 합니다. 이는 다음과 같습니다.

```
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#
```

텔넷 서버 서비스(Telnet to-the-box)를 사용하려면 다음 절차에 따라 다른 라우터에서 텔넷을 활성화합니다.자세한 내용은 **Cisco ASR** 1000 Series Aggregation Services Routers Software Configuration Guide의 Cisco ASR 1000 Series Routers 섹션에 대한 텔넷 및 SSH 개요를 참조하십시오.

HTTP

모든 라우터에 사용할 수 있는 레거시 웹 사용자 인터페이스는 ASR1K에서도 사용할 수 있습니다 .이 섹션에 표시된 대로 ASR에서 HTTP 서버 또는 클라이언트 서비스를 활성화합니다.

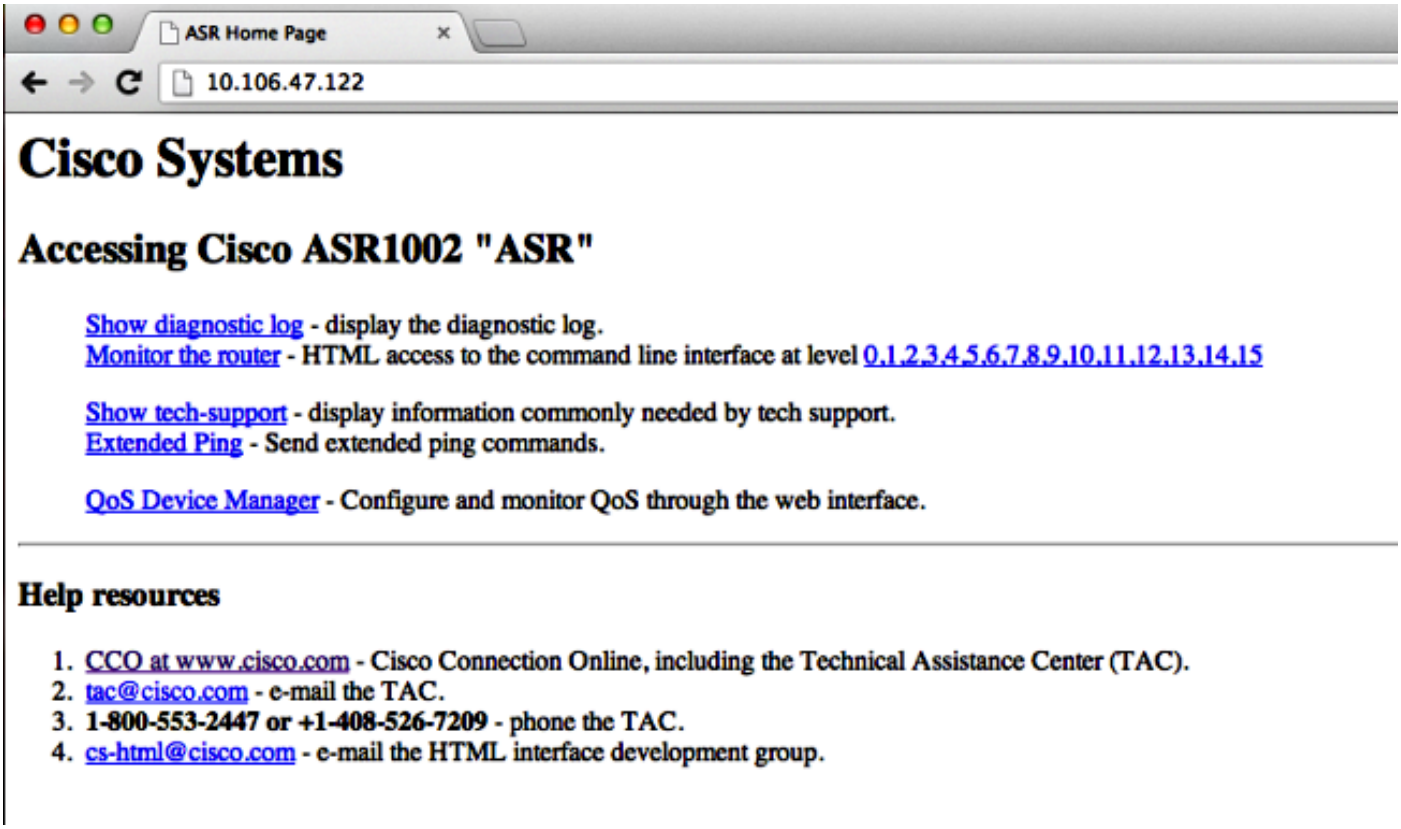
기존 HTTP 액세스를 기본 서비스(서버)에 활성화하고 웹 기반 GUI 액세스를 사용하려면 로컬 인증을 사용하는 이 컨피그레이션을 사용합니다(외부 AAA(Authentication, Authorization, and Accounting) 서버를 사용할 수도 있음).

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

다음은 HTTP 보안 서버(HTTPS)를 활성화하는 컨피그레이션입니다.

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

ASR에서 인터페이스의 IP 주소를 찾아 생성한 사용자 계정으로 로그인합니다.스크린샷:



HTTP 클라이언트 서비스를 사용하려면 VRF 지원 인터페이스에서 HTTP 클라이언트 트래픽에 대한 **ip http 클라이언트 source-interface <interface name>** 명령 소스를 다음과 같이 입력합니다.

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

다음은 원격 HTTP 서버에서 플래시로 이미지를 복사하기 위해 HTTP 클라이언트 서비스를 사용하는 방법을 보여주는 예입니다.

```
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#
```

영구 액세스

이 섹션은 to-the-box Telnet/SSH/HTTP 연결에만 적용됩니다.

영구 SSH 및 영구 텔넷을 통해 관리 이더넷 인터페이스에서 수신 SSH 또는 텔넷 트래픽의 처리를 정의하는 전송 맵을 구성할 수 있습니다.따라서 Cisco IOS 프로세스가 활성화되지 않은 경우에도 진단 모드를 통해 라우터에 액세스할 수 있습니다.진단 모드에 대한 자세한 내용은 Cisco ASR 1000 Series Aggregation Services Routers 소프트웨어 구성 설명서의 진단 모드 이해 섹션을 참조하십시오.

> **참고:**영구 SSH 또는 영구 텔넷은 관리 인터페이스인 GigabitEthernet **0**에서만 구성할 수 있습니다**.**

> **참고:**Cisco 버그 ID CSCuj37515에 대한 수정 사항이 없는 버전에서는 주변 장치 액세스에 대한 인증 방법은 라인 VTY에서 사용되는 방법에 따라 **결정됩니다**.영구 액세스를 위해서는 인증이 로컬이어야 하므로 외부 인증이 실패할 경우에도 진단 모드 액세스가 계속 작동합니다.이는 정상적인 SSH 및 텔넷 액세스도 로컬 인증을 사용해야 함을 의미합니다.

> **주의:**Cisco 버그 ID CSCug77654에 대한 수정 사항이 없는 버전에서는 기본 AAA 방법을 사용하면 영구 SSH를 사용할 때 SSH 프롬프트를 입력할 수 있는 사용자 기능이 제한됩니다.사용자는 항상 진단 프롬프트를 입력해야 합니다.이러한 버전의 경우 이름 인증 방법을 사용하거나 일반 SSH 및 텔넷이 활성화되어 있는지 확인하는 것이 좋습니다.

영구 SSH

다음 섹션에 표시된 대로 영구 SSH를 허용하려면 전송 맵을 만듭니다.

구성

```
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
```

이제 영구 SSH에 대한 로컬 인증을 활성화해야 합니다.이는 aaa **new-model** 명령을 사용하거나 사용하지 않고 수행할 수 있습니다.두 시나리오 모두 여기에 설명되어 있습니다.(두 경우 모두 라우터에 로컬 사용자 이름/비밀번호 계정이 있는지 확인합니다.)

ASR에서 AAA를 활성화했는지 여부에 따라 어떤 컨피그레이션을 선택할 수 있습니다.

1. AAA가 활성화된 경우:

```
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. AAA가 활성화되지 않은 경우:

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

다음을 확인합니다.

VRF 지원 Gigabitethernet**0** 인터페이스의 IP 주소를 사용하여 ASR에 **대한 SSH**비밀번호를 입력하면 브레이크 시퀀스(**Ctrl-C** 또는 **Ctrl-Shift-6**)를 입력해야 합니다.

```
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)#
```

> **참고:**진단 모드를 시작하기 위해 터미널에 브레이크 시퀀스(**Ctrl-C** 또는 **Ctrl-Shift-6**)를 표시할 때**(Waiting for vty line**) 가 표시됩니다.

영구 텔넷

구성

SSH에 대한 이전 섹션에서 설명한 것과 유사한 로직을 사용하여 다음과 같이 영구 텔넷에 대한 전송 맵을 만듭니다.

```
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
```

SSH에 대한 마지막 섹션에서 설명한 것처럼, 다음 두 가지 방법으로 로컬 인증을 구성할 수 있습니다.

1. AAA가 활성화된 경우:

```
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. AAA가 없는 경우:

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

다음을 확인합니다.

GigabitEthernet 0 인터페이스의 IP 주소에 텔넷합니다.자격 증명을 입력한 후 중단 시퀀스를 입력하고 진단 모드에 로그인하기 전에 몇 초(때로는 시간이 걸릴 수 있음)을 기다립니다.

```
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)#
```

> **참고:**브레이크 시퀀스 Ctrl+C 또는 Ctrl+Shift+6을 입력하고 몇 초 동안 기다립니다.Waiting for IOS Process(IOS 프로세스 대기 중)가 터미널에 표시되면 진단 모드를 시작할 수 있습니다.

영구 HTTP

Persistent HTTP access to-the-box(HTTP from-the-box 또는 HTTP 클라이언트 서비스를 사용할 수 없음)를 활성화하고 새 웹 기반 GUI 액세스를 사용하려면 로컬 인증을 사용하는 이 컨피그레이션을 사용합니다(외부 AAA 서버도 사용할 수 있음).

구성

이러한 컨피그레이션에서는 http-webui 및 https-webui가 transport-map의 이름입니다.

```
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
```

다음은 HTTP 보안 서버(HTTPS)를 활성화하는 데 사용되는 컨피그레이션입니다.

```
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
```

다음을 확인합니다.

ASR에서 인터페이스의 IP 주소를 찾습니다.홈 페이지를 시작하려면 생성한 사용자 이름/비밀번호로 로그인합니다.명령을 적용할 수 있는 IOS WebUI와 함께 상태 및 모니터링 관련 정보가 표시됩니다.다음은 홈 페이지의 스크린샷입니다.

문제 해결

HTTPS를 통해 WebUI를 사용할 수 없는 경우 인증서 및 RSA(Rivest-Shamir-Adleman) 키가 존재하고 작동 가능한지 확인합니다.WebUI가 제대로 시작되지 않는 이유를 확인하려면 다음 **debug** 명령을 사용할 수 있습니다.

```
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 키

RSA 키가 있는지 확인하려면 다음 명령을 입력합니다.

```
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#
```

인증서를 만드는 데 필요한 키 이름을 기록해 두십시오. 키가 없는 경우 다음 명령으로 키 이름을 만들 수 있습니다.

```
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
```

인증서

키가 있으면 다음 명령을 입력하여 인증서를 확인할 수 있습니다.

```
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
```

인증서가 유효하지 않거나 없는 경우 다음 명령을 사용하여 인증서를 생성할 수 있습니다.

```
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
```

RSA 키 및 인증서가 업데이트되고 유효하면 인증서가 HTTPS 컨피그레이션과 연결될 수 있습니다

.

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

그런 다음 WebUI가 작동하는지 확인하기 위해 WebUI를 비활성화하고 다시 활성화할 수 있습니다.

```
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
```

관련 정보

- 콘솔 포트, 텔넷 및 SSH 처리
- 진단 모드 이해
- 기술 지원 및 문서 – Cisco Systems