ASR での VRF 認識型管理の設定例

内容

概要

このドキュメントでは、管理インターフェイス（GigabitEthernet0）を使用した Cisco アグリゲーション サービス ルータ 1000 シリーズ（ASR1K）での Virtual Routing and Forwarding 対応（VRF 対応）管理の使用について説明します。 情報は、他に明示的な規定のない限り、VRF の他のインターフェイスにも適用できます。**to-the-box および from-the-box の両方の接続シナリオ向けのさまざまなアクセス プロトコルについて説明します。**

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SSH、Telnet、HTTP などの管理プロトコル
- Secure Copy Protocol（SCP）、TFTP、FTP などの File Transfer Protocol
- VRF

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® XE バージョン 3.5S（15.2(1)S）以降の Cisco IOS-XE バージョン
  注：VRF 対応 SCP には少なくともこのバージョンが必要ですが、このドキュメントに記載されている他のプロトコルは以前のバージョンでも同様に動作します。
- ASR1K

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、使用されているコマンドの影響について十分に理解したうえで作業してください。

背景説明

管理インターフェイス：管理インターフェイスの目的は、ユーザがルータの管理タスクを実行できるようにすることです。基本的には、これはデータプレーン トラフィックを転送してはならない、またはできないインターフェイスですが、そうではない場合、多くの場合は Telnet およびセキュア シェル（SSH）経由でのルータへのリモート アクセスのため、およびルータ上の大部分の管理タスクを実行するために使用されます。このインターフェイスは、ルータがルーティングを開始する前か、または共有ポート アダプタ（SPA）インターフェイスが非アクティブ時にトラブルシューティングを行う場合に有用な機能を提供します。ASR1K では、管理インターフェイスは **Mgmt-intf** という名前のデフォルトの VRF です。

このドキュメントでは **ip *<protocol> source-interface コマンドが広範に使用されています（ここでは <protocol> キーワードに SSH、FTP、TFTP を指定できます）。*** このコマンドは、ASR が接続におけるクライアント デバイスである場合に、発信元アドレスとして使用するインターフェイスの IP アドレスを指定するために使用されます（たとえば、接続が ASR または from-the-box トラフィックから開始されます）。 これはまた、ASR が接続の開始側でない場合は **ip *<protocol> source-interface コマンドは適用可能ではなく、ASR は応答トラフィックにこの IP アドレスを使用しないことを意味します。*** 代わりに、接続先に最も近いインターフェイスの IP アドレスを使用します。このコマンドを使用すると、VRF 対応インターフェイスから（サポートされているプロトコルの）トラフィックを送信できます。

管理プロトコル

注：この記事で使用されているコマンドの詳細を確認するには、Command Lookup Tool（登録ユーザ専用）を使用してください。

SCP

VRF 対応インターフェイスから ASR で SCP クライアント サービスを使用するには、この設定を使用します。

設定

ip ssh source-interfaceコマンドは、SCPがSSHを使用するため、管理インターフェイスをSSHとSCPの両方のクライアントサービスの**Mgmt-intf** VRFにポイントするために使用されます。**copy scp**コマンドには、VRFを指定する以外のオプションはありません。したがって、この **ip ssh source-interface コマンドを使用する必要があります。**同じロジックが、他の VRF 対応インターフェイスに適用されます。

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

注：ASR1k プラットフォームで、VRF 対応 SCP はバージョン XE3.5S（15.2(1)S）以前では動作しません。

確認

設定を検証するには、次のコマンドを使用します。

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

ASR から SCP を使用するリモート デバイスにファイルをコピーするには、次のコマンドを入力します。

```
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#
```

リモート デバイスから SCP を使用する ASR にファイルをコピーするには、次のコマンドを入力します。

```
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 対応インターフェイスから ASR1k 上の TFTP クライアント サービスを使用するには、次の設定を使用します。

設定

管理インターフェイスを Mgmt-intf VRF にポイントするには、ip tftp source-interface オプションを使用します。copy tftp コマンドには VRF を指定するその他のオプションはありません。したがって、この ip tftp source-interface コマンドを使用する必要があります。同じロジックが、他の VRF 対応インターフェイスに適用されます。

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

確認

設定を検証するには、次のコマンドを使用します。

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

ASR から TFTP サーバにファイルをコピーするには、次のコマンドを入力します。

```
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 サーバから ASR ブートフラッシュにファイルをコピーするには、次のコマンドを入力します。

```
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 対応インターフェイスから ASR 上の FTP クライアントを使用するには、次の設定を使用します。

設定

管理インターフェイスを Mgmt-intf VRF にポイントするには、ip ftp source-interface オプションを使用します。copy ftp コマンドには VRF を指定するその他のオプションはありません。したがって、ip ftp source-interface コマンドを使用する必要があります。同じロジックが、他の VRF 対応インターフェイスに適用されます。

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

確認

設定を検証するには、次のコマンドを使用します。

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

ASR から FTP サーバにファイルをコピーするには、次のコマンドを入力します。

```
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 サーバから ASR ブートフラッシュにファイルをコピーするには、次のコマンドを入力します。

```
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#
```

管理アクセス プロトコル

通常のアクセス

SSH

> **注意**：ASR1k にみられる一般的な問題の 1 つとして、メモリ不足のために SSH が失敗します。この問題に関する詳細については、シスコの記事「メモリ不足の状態による SSH 認証の失敗」を参照してください。

SSH クライアント サービスを ASR (SSH from-the-box) で実行するために使用するオプションには 2 つあります。 1 つのオプションとして **ssh コマンド自体に VRF 名を指定することで、特定の VRF から SSH トラフィックを送信できます。**

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

または、ip ssh source-interface オプションを使用して、特定の VRF 対応インターフェイスから SSH トラフィックを送信します。

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

SSH サーバ サービス (SSH to-the-box) を使用するには、手順に従って SSH を他の Cisco IOS ルータで有効にします。詳細については、**『Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ ソフトウェア設定ガイド』の「**Cisco ASR 1000 シリーズ ルータ向けの Telnet と SSH の概要」の項を参照してください。

Telnet

Telnet クライアント サービスを ASR (Telnet from-the-box) で実行するために使用するオプションには 2 つあります。 1 つのオプションとして、次の示すように telnet コマンド自体に送信元インターフェイスまたは VRF を指定します。

```
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#
```

または、ip telnet source-interface コマンドを使用します。それでも次の手順で、次に示すように **telnet コマンドを使用して VRF 名を指定する必要があります。**

```
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#
```

Telnet サーバ サービス（Telnet to-the-box）を使用するには、手順に従って Telnet を他のルータで有効にします。詳細については、『**Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ ソフトウェア設定ガイド**』の「Cisco ASR 1000 シリーズ ルータ向けの Telnet と SSH の概要」の項を参照してください。

HTTP

すべてのルータで利用可能なレガシー Web ユーザ インターフェイスは、ASR1K でも利用できます。この項で示すように、ASR の HTTP サーバまたはクライアント サービスを有効にします。

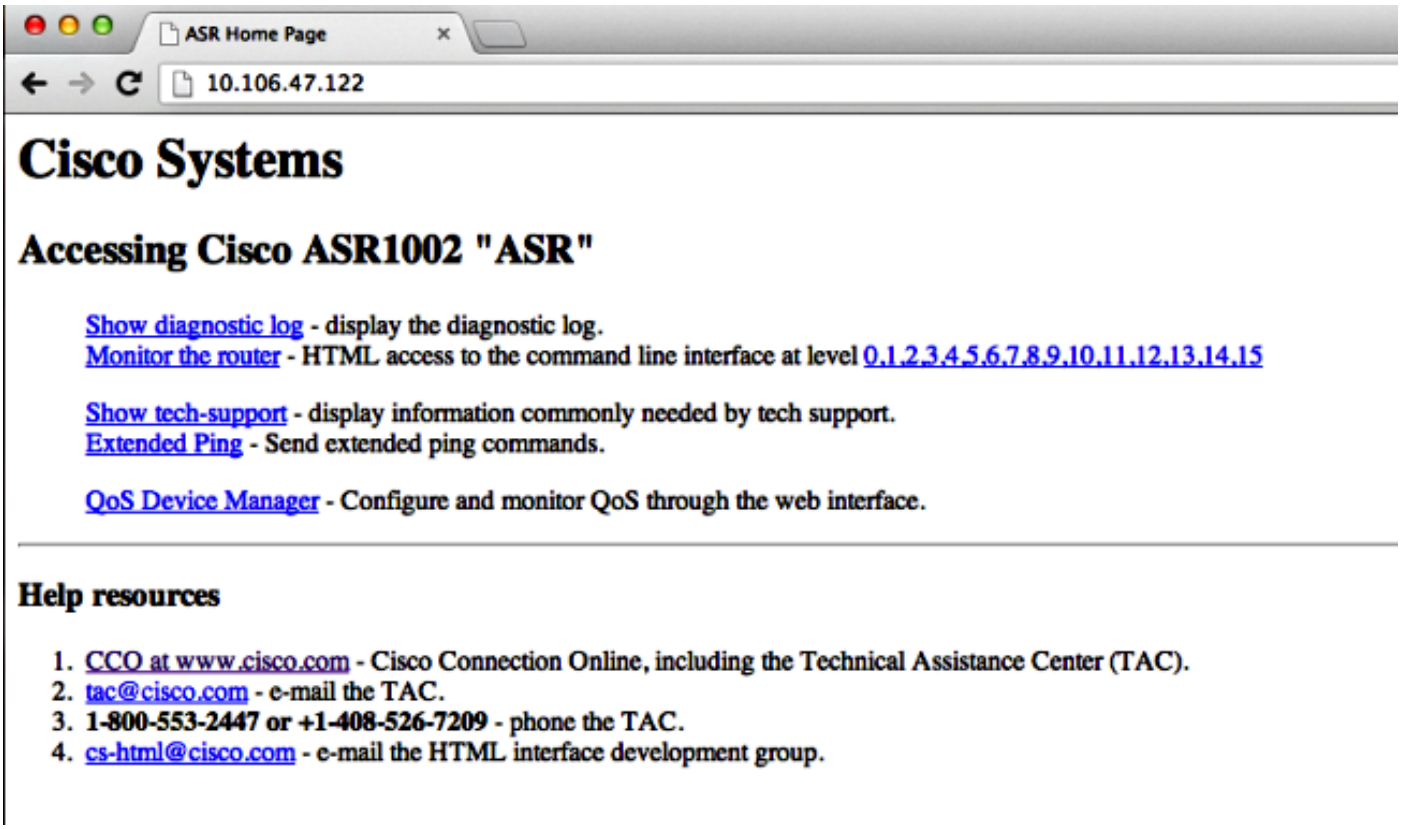
レガシー HTTP アクセス to-the-box サービス（サーバ）を有効にして、Web ベースの GUI を使用するには、ローカル認証を使用するこの設定を使用します（または外部の認証、認可、およびアカウンティング（AAA）サーバを使用することもできます）。

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

HTTP セキュア サーバ（HTTPS）を有効にする設定を次に示します。

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

ASR のインターフェイスの IP アドレスを参照し、作成したユーザ アカウントでログインします。次にスクリーンショットを示します。



HTTP クライアント サービスを使用するには、次に示すように VRF 対応のインターフェイスから HTTP クライアント トラフィックの **ip http client source-interface <interface name> コマンド ソースを入力します。**

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

イメージをリモート HTTP サーバからフラッシュにコピーするための HTTP クライアント サービスの使用例を次に示します。

```
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#
```

永続アクセス

この項は、to-the-box Telnet/SSH/HTTP 接続の場合にのみ適用されます。

持続性 SSH および持続性 Telnet を使用すると、管理イーサネット インターフェイスの着信 SSH トラフィックまたは Telnet トラフィックの処理を定義するトランスポート マップを設定できます。そのため Cisco IOS プロセスが非アクティブな場合でも、診断モード経由でルータにアクセスできます。診断モードの詳細については、『Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ ソフトウェア設定ガイド』の「診断モードの概要」の項を参照してください。

> **注：持続性 SSH または持続性 Telnet は、管理インターフェイス GigabitEthernet0 でのみ設定できます。**

> **注：**Cisco Bug ID CSCuj37515 の修正が実施されていないバージョンでの永続アクセス向けの認証方式は、**VTY** の行で使用されている方式によって異なります。外部認証が失敗しても診断モードでのアクセスは動作し続けるようにするために、永続アクセスでは認証がローカルであることが必要です。これは、通常の SSH および Telnet アクセスでもローカル認証を使用する必要があることを意味します。

> **注意**：Cisco Bug ID CSCug77654 の修正が実施されていないバージョンでデフォルトの AAA 方式を使用すると、持続性 SSH が使用されている場合に SSH プロンプトに入力するユーザー機能が制限されます。ユーザは、診断プロンプトを入力するように常に強制されます。これらのバージョンについては、シスコでは名前認証方式を使用するか、通常の SSH および Telnet が有効になっていることを確認することをお勧めします。

持続性 SSH

次の項で示すように持続性 SSH を許可するにはトランスポート マップを作成します。

設定

```
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
```

ここでは持続性 SSH の口ーカル認証を有効にする必要があります。これは aaa new-model コマンドを使用するか、または使用しなくても実行できます。両方のシナリオについてここで説明します (どちらの場合でも、ルータの口ーカルのユーザ名およびパスワードのアカウントがあることを確認します) 。

ASR で AAA が有効になっているかどうかによって、どの設定を使用するかを選択できます。

1. AAA が有効である場合：

```
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. AAA が有効ではない場合：

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

確認

VRF 対応の Gigabitethernet0 インターフェイスの IP アドレスをもつ ASR に SSH で接続します。パスワードを入力したら、ブレーク シーケンス (Ctrl-C または Ctrl-Shift-6) を入力する必要があります。

```
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：診断モードに入るためにターミナルにWaiting for vty lineが表示されたら、ブレークシ

ーケンス(Ctrl-CまたはCtrl-Shift-6)を入力します。

持続性 Telnet

設定

SSH について前の節で説明した口ジックと同様に、次に示すように持続性 Telnet のトランスポート マップを作成します。

```
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
```

SSH について直前の節で説明したように、ローカル認証を設定する方法は次のように 2 つあります。

1. AAA が有効である場合：

   ```
   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. AAA がない場合：

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

確認

GigabitEthernet0 インターフェイスの IP アドレスに Telnet で接続します。クレデンシャルを入力したら、ブレーク シーケンスを入力し、診断モードにログインするまで数秒間待機します（しばらくかかる場合があります）。

```
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：ブレーク シーケンス **Ctrl+C または Ctrl+Shift+6** を入力して、数秒待ちます。端末に **Waiting for IOS Processが表示さ**れると、診断モードに入ることができます。

持続性 HTTP

持続性 HTTP アクセス to-the-box（HTTP from-the-box または HTTP クライアント サービスを利用できない）を有効にして、新しい Web ベースの GUI アクセスを使用するには、ローカル認証を活用するこの設定を使用します（外部 AAA サーバを使用することもできます）。

設定

これらの設定では、**http-webui および https-webui は、トランスポート マップの名前です。**

```
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
```

次に、HTTP セキュア サーバ（HTTPS）を有効にするために使用する設定を示します。

```
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
```

確認

ASR のインターフェイスの IP アドレスを参照します。ホームページを表示するために作成したユーザ名とパスワードでログインします。コマンドを適用できる **IOS WebUI とともに、ヘルスおよびモニタリング関連の情報が表示されます。**次に、ホームページのスクリーンショットを示します。

トラブルシュート

WebUIがHTTPSで使用できない場合は、証明書とRivest-Shamir-Adleman(RSA)キーが存在し、動作していることを確認します。次のdebugコマンドを使用して、WebUIが正しく起動しない理由を判別できます。

```
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キー

RSAキーが存在することを確認するには、次のコマンドを入力します。

```
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#
```

証明書を作成するために必要なキー名をメモします。キーがない場合は、次のコマンドを使用してキーを作成できます。

```
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
```

証明書

キーが存在したら、次のコマンドを入力して証明書を確認できます。

```
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
```

証明書が無効であるか、存在しない場合は、次のコマンドを使用して証明書を作成できます。

```
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キーと証明書が更新されて有効になると、証明書をHTTPS設定に関連付けることができます

。

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

次に、WebUIが機能していることを確認するために、WebUIを無効にしてから再度有効にします。

```
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
```

関連情報

- コンソール ポート、Telnet、および SSH の処理
- 診断モードの概要
- テクニカル サポートとドキュメント – Cisco Systems