Esempi di gestione compatibile con VRF su configurazioni ASR

Sommario

Introduzione

In questo documento viene descritto l'utilizzo della gestione con supporto di Routing e inoltro virtuale (VRF-Aware) su Cisco Aggregation Services Router serie 1000 (ASR1K) con interfaccia di gestione (**Gigabit Ethernet0**). Le informazioni sono applicabili anche a qualsiasi altra interfaccia in un VRF, se non diversamente specificato. Sono descritti vari protocolli **di** accesso **per** gli scenari di

connessione **diretta** e **diretta**.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocolli di gestione, ad esempio SSH, Telnet e HTTP
- Protocolli di trasferimento file, ad esempio SCP (Secure Copy Protocol), TFTP e FTP
- VRF

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS® XE versione 3.5S (15.2(1)S) o successive versioni Cisco IOS-XE
  Nota: VRF-Aware SCP richiede almeno questa versione, mentre altri protocolli descritti in questo documento funzionano anche con le versioni precedenti.
- ASR1K

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Interfaccia di gestione: Lo scopo di un'interfaccia di gestione è quello di consentire agli utenti di eseguire le attività di gestione sul router. Si tratta fondamentalmente di un'interfaccia che non deve, e spesso non può, inoltrare il traffico della corsia dati. In caso contrario, può essere utilizzata per l'accesso remoto al router, spesso tramite Telnet e Secure Shell (SSH), e per eseguire la maggior parte delle attività di gestione sul router. L'interfaccia è più utile prima che un router inizi il routing o in scenari di risoluzione dei problemi quando le interfacce Shared Port Adapter (SPA) sono inattive. Su ASR1K, l'interfaccia di gestione si trova in un VRF predefinito denominato **Mgmt-intf**.

il comando **ip** ***<protocollo>*** **source-interface** viene usato ampiamente in questo documento (la parola chiave *<protocollo>* può essere SSH, FTP, TFTP). Questo comando è usato per specificare l'indirizzo IP di un'interfaccia da usare come indirizzo di origine quando l'ASR è il dispositivo client in una connessione (ad esempio, la connessione viene avviata dall'ASR o dal traffico locale). Ciò significa anche che se l'ASR non è l'iniziatore della connessione, il comando **ip** ***<protocol>*** **source-interface** non è applicabile e l'ASR non utilizza questo indirizzo IP per il traffico di risposta; utilizza invece l'indirizzo IP dell'interfaccia più vicina alla destinazione. Questo comando consente di generare il traffico (per i protocolli supportati) da un'interfaccia compatibile con VRF.

Protocolli di gestione

> **Nota:** per ulteriori informazioni sui comandi menzionati in questo articolo, usare lo strumento di ricerca dei comandi (solo utenti registrati).

SCP

Per utilizzare il servizio client SCP su un ASR da un'interfaccia abilitata per VRF, utilizzare questa configurazione.

Configurazione

Il comando **ip ssh source-interface** viene usato per indirizzare l'interfaccia di gestione al VRF **Mgmt-intf** sia per i servizi client SSH che SCP, in quanto SCP usa SSH. Il comando **copy scp** non include altre opzioni per specificare il VRF. Pertanto, è necessario usare questo comando **ip ssh source-interface**. La stessa logica si applica a qualsiasi altra interfaccia abilitata per VRF.

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

> **Nota:** Sulla piattaforma ASR1k, SCP compatibile con VRF funziona solo nella versione XE3.5S (15.2(1)S).

Verifica

Utilizzare questi comandi per verificare la configurazione.

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

Per copiare un file da ASR a un dispositivo remoto con SCP, immettere questo 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#
```

Per copiare un file da una periferica remota ad ASR con SCP, immettere questo 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

Per utilizzare il servizio client TFTP su un'ASR1k da un'interfaccia abilitata per VRF, utilizzare questa configurazione.

Configurazione

L'opzione **ip tftp source-interface** viene usata per indirizzare l'interfaccia di gestione al VRF **Mgmt-intf**. Il comando **copy tftp** non include altre opzioni per specificare il VRF. Pertanto, è necessario utilizzare questo comando **ip tftp source-interface**. La stessa logica si applica a qualsiasi altra interfaccia abilitata per VRF.

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

Verifica

Utilizzare questi comandi per verificare la configurazione.

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

Per copiare un file da ASR al server TFTP, immettere questo 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#
```

Per copiare un file dal server TFTP al bootflash ASR, immettere questo 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

Per utilizzare il servizio client FTP su un ASR da un'interfaccia abilitata per VRF, utilizzare questa

configurazione.

Configurazione

L'opzione **ip ftp source-interface** viene usata per indirizzare l'interfaccia di gestione al VRF **Mgmt-intf**. Il comando **copy ftp** non contiene altre opzioni per specificare il VRF. È necessario quindi usare il comando **ip ftp source-interface**. La stessa logica si applica a qualsiasi altra interfaccia abilitata per VRF.

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

Verifica

Utilizzare questi comandi per verificare la configurazione.

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

Per copiare un file da ASR a un server FTP, immettere questo 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#
```

Per copiare un file dal server FTP al file bootflash ASR, immettere questo 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#
```

Protocolli di accesso alla gestione

Accesso regolare

SSH

> **Attenzione:** Uno dei problemi più comuni riscontrati con gli ASR1k è che il protocollo SSH ha esito negativo a causa di memoria insufficiente. Per ulteriori informazioni sul problema, consultare l'articolo SSH Authentication Failure to Low Memory Conditions (Errore di

autenticazione SSH a causa di memoria insufficiente) di Cisco.

Per eseguire il servizio client SSH sull'ASR (SSH preconfigurato), sono disponibili due opzioni. In un caso, è possibile specificare il nome del VRF nello stesso comando **ssh**, in modo da poter originare il traffico SSH da un determinato VRF.

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

In alternativa, è possibile usare l'opzione **ip ssh source-interface** per indirizzare il traffico SSH da un'interfaccia VRF specifica.

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

Per utilizzare il servizio server SSH (SSH incluso), seguire la procedura per abilitare SSH su qualsiasi altro router Cisco IOS. Per ulteriori informazioni, consultare la sezione Telnet e SSH Overview for the Cisco ASR 1000 Series Router in **Cisco ASR 1000 Aggregation Services Router Software Configuration Guide**.

Telnet

Per eseguire il servizio client Telnet sull'ASR, è possibile utilizzare due opzioni (Telnet dall'inizio). È possibile specificare l'interfaccia di origine o il VRF nel comando **telnet** stesso, come mostrato di seguito:

```
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#
```

In alternativa, è possibile usare il comando **ip telnet source-interface**. È comunque necessario specificare il nome VRF nel passaggio successivo con il comando **telnet**, come mostrato di seguito:

```
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#
```

Per utilizzare il servizio server Telnet (Telnet to the box), seguire la procedura per abilitare Telnet su qualsiasi altro router. Per ulteriori informazioni, consultare la sezione Telnet e SSH Overview for the Cisco ASR 1000 Series Router in **Cisco ASR 1000 Aggregation Services Router Software Configuration Guide**.

HTTP

L'interfaccia utente Web legacy disponibile per tutti i router è disponibile anche per ASR1K. Abilitare il server HTTP o il servizio client su ASR come mostrato in questa sezione.

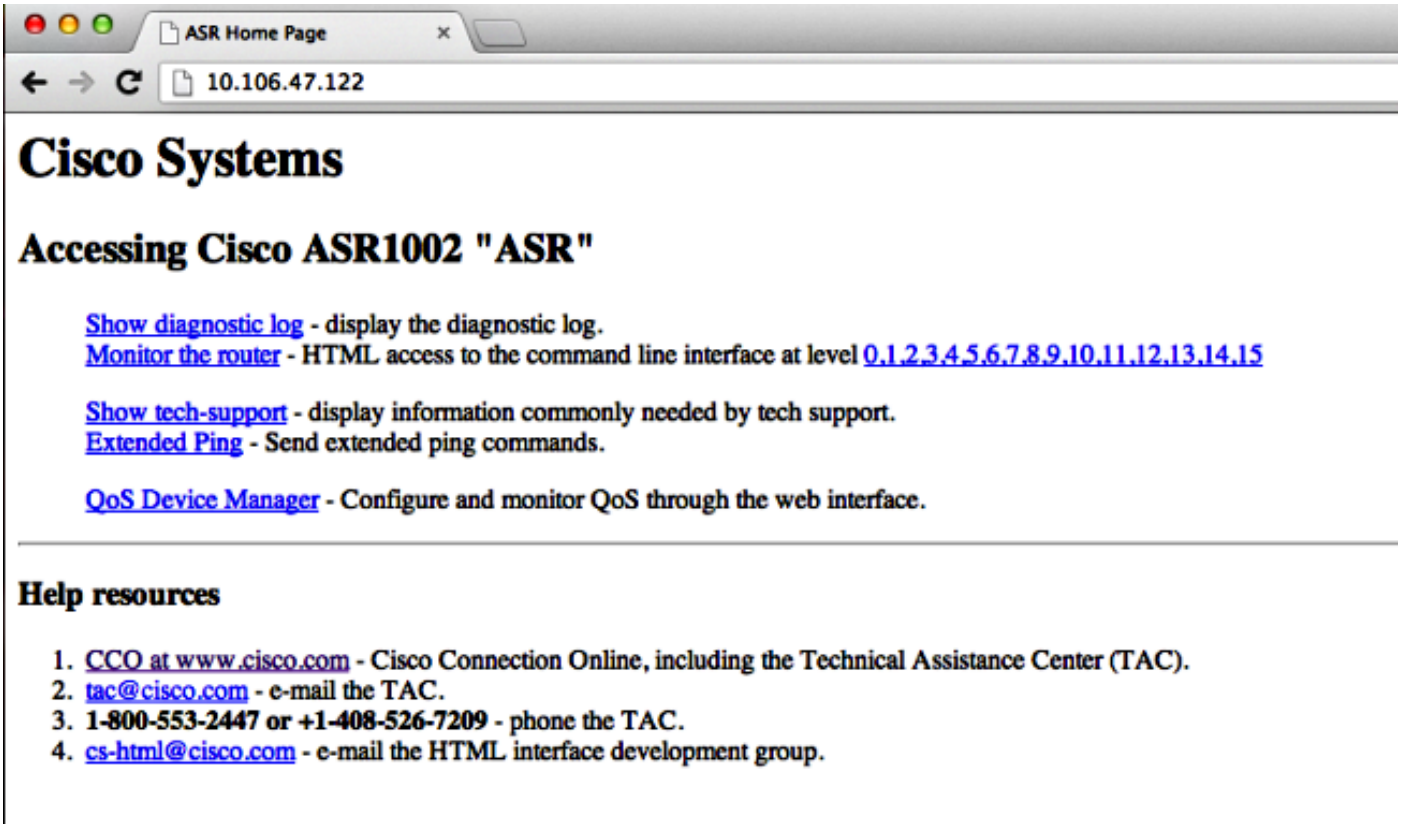
Per abilitare l'accesso HTTP legacy al servizio preconfigurato (server) e utilizzare l'accesso GUI basato sul Web, utilizzare questa configurazione che utilizza l'autenticazione locale (è possibile utilizzare anche un server AAA (Authentication, Authorization, and Accounting) esterno).

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

Di seguito è riportata la configurazione per abilitare il server sicuro HTTP (HTTPS):

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

Individuare l'indirizzo IP di un'interfaccia sull'ASR e accedere con l'account utente creato. Ecco uno screenshot:



Per utilizzare il servizio client HTTP, immettere il comando **ip http client source-interface <nome interfaccia>** per il traffico del client HTTP da un'interfaccia abilitata per VRF, come mostrato:

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

Di seguito è riportato un esempio che illustra l'utilizzo del servizio client HTTP per copiare un'immagine da un server HTTP remoto alla memoria 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#
```

Accesso permanente

Questa sezione è applicabile solo alle connessioni Telnet/SSH/HTTP predefinite.

Con il protocollo SSH persistente e il protocollo Telnet persistente, è possibile configurare una mappa di trasporto che definisce il trattamento del traffico SSH o Telnet in arrivo sull'interfaccia Ethernet di gestione. In questo modo è possibile accedere al router tramite la modalità diagnostica anche quando il processo Cisco IOS non è attivo. Per ulteriori informazioni sulla modalità diagnostica, fare riferimento alla sezione Descrizione della modalità diagnostica nella guida alla configurazione del software dei router Cisco ASR serie 1000 Aggregation Services.

> **Nota:** Il protocollo SSH persistente o Telnet persistente può essere configurato solo sull'interfaccia di gestione **Gigabit Ethernet0.**

Nota: Nelle versioni in cui non è disponibile la correzione per l'ID bug Cisco CSCuj37515, il metodo di autenticazione per l'accesso permanente dipende dal metodo usato alla riga **VTY**. Per l'accesso permanente è necessario che l'autenticazione sia locale, in modo che l'accesso in modalità diagnostica funzioni anche in caso di errore dell'autenticazione esterna. Ciò significa che ogni normale accesso SSH e Telnet richiede anche l'uso dell'autenticazione locale.

Attenzione: Nelle versioni in cui non è disponibile la correzione per l'ID bug Cisco CSCug77654, l'uso del metodo AAA predefinito limita la possibilità per l'utente di immettere il prompt SSH quando si usa il protocollo SSH persistente. L'utente è sempre obbligato a immettere il prompt di diagnostica. Per queste versioni, Cisco consiglia di utilizzare un metodo di autenticazione dei nomi o di verificare che i normali protocolli SSH e Telnet siano abilitati.

SSH permanente

Creare una mappa del trasporto per consentire il protocollo SSH persistente, come mostrato nella sezione successiva:

Configurazione

```
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
```

A questo punto, è necessario abilitare l'autenticazione locale per il protocollo SSH permanente. A tale scopo, è possibile usare il comando **aaa new-model** o senza di esso. Entrambi gli scenari sono descritti qui. In entrambi i casi, verificare di disporre di un account con nome utente e password locale sul router.

Èpossibile scegliere la configurazione a seconda che il server AAA sia abilitato o meno sull'ASR.

1. Con AAA abilitato:

```
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. Senza AAA abilitato:

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

Verifica

SSH all'ASR con l'indirizzo IP dell'interfaccia **Gigabit Ethernet0** abilitata per VRF. Una volta immessa la password, è necessario immettere la sequenza di interruzione (**Ctrl-C** o **Ctrl-Maiusc-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)#
```

> **Nota:** Immettere la sequenza di interruzione (**Ctrl-C** o **Ctrl-Maiusc-6**) quando sul terminale viene visualizzato **—In attesa della linea vty** per accedere alla modalità diagnostica.

Persistent Telnet

Configurazione

Con una logica simile a quella descritta nella sezione precedente per SSH, creare una mappa del trasporto per Telnet persistente, come mostrato di seguito:

```
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
```

Come indicato nell'ultima sezione per SSH, sono disponibili due metodi per configurare l'autenticazione locale, come mostrato di seguito:

1. Con AAA abilitato:

```
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. Senza AAA:

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

Verifica

Telnet su indirizzo IP dell'interfaccia **Gigabit Ethernet0**. Dopo aver immesso le credenziali, immettere la sequenza di interruzione e attendere alcuni secondi (a volte potrebbe essere necessario del tempo) prima di accedere alla modalità diagnostica.

```
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)#
```

> **Nota:** Immettere la sequenza di interruzione **Ctrl+C** o **Ctrl+Maiusc+6**, quindi attendere alcuni secondi. Quando sul terminale viene visualizzato **—In attesa del processo IOS**, è possibile accedere alla modalità diagnostica.

HTTP permanente

Per abilitare l'accesso HTTP permanente alla console (il servizio client HTTP dalla console o non è disponibile) e utilizzare il nuovo accesso GUI basato sul Web, utilizzare questa configurazione che utilizza l'autenticazione locale (è possibile utilizzare anche un server AAA esterno).

Configurazione

In queste configurazioni, **http-webui** e **https-webui** sono i nomi delle mappe di trasporto.

```
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
```

Di seguito è riportata la configurazione utilizzata per abilitare il server sicuro HTTP (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
```

Verifica

Selezionare l'indirizzo IP di un'interfaccia sull'ASR. Accedere con il nome utente/password creati per avviare la home page. Vengono visualizzate le informazioni relative allo stato e al monitoraggio, insieme a una **IOS WebUI** dove è possibile applicare i comandi. Ecco uno screenshot della homepage:

Risoluzione dei problemi

Se WebUI non è disponibile tramite HTTPS, verificare che il certificato e la chiave Rivest-Shamir-Adleman (RSA) siano presenti e funzionanti. È possibile utilizzare questo comando **debug** per determinare il motivo per cui WebUI non viene avviato correttamente:

```
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
```

Chiave RSA

Per verificare la presenza della chiave RSA, immettere questo 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#
```

Prendere nota del nome della chiave, in quanto necessario per creare il certificato. Se non è presente una chiave, è possibile crearne una con i seguenti comandi:

```
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
```

Certificato

Una volta trovata la chiave, è possibile immettere questo comando per verificare il certificato:

```
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 il certificato non è valido o non è presente, è possibile crearlo con i seguenti comandi:

```
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
```

Una volta che la chiave RSA e il certificato sono stati aggiornati e sono validi, il certificato può essere associato alla configurazione HTTPS:

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

Èquindi possibile disattivare e riattivare WebUI per garantirne il corretto funzionamento:

```
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

Informazioni correlate

- Gestione porta console, Telnet e SSH
- Informazioni sulla modalità diagnostica
- Documentazione e supporto tecnico – Cisco Systems