

Copia protetta delle immagini Cisco IOS su router e switch

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come copiare in modo sicuro il file di immagine Cisco IOS® dal PC Windows/ Linux/ macOS locale ai router e agli switch Cisco.

Prerequisiti

Requisiti

Cisco consiglia di essere a conoscenza della raggiungibilità SSH (Secure Shell) del dispositivo con accesso di livello 15.

Componenti usati

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

- Cisco ISR 3945 CGR2010 router
- Sistema operativo Windows 10
- Sistema operativo Linux RedHat

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

In questo documento viene descritto come copiare in modo sicuro il file di immagine Cisco IOS dal PC locale Windows/ Linux/ macOS ai router e agli switch Cisco senza dover usare server o software esterni, ad esempio il protocollo TFTP (Trivial File Transfer Protocol), il protocollo FTP

(File Transfer Protocol), il protocollo SFTP (Secure File Transfer Protocol) o il protocollo SCP (Secure Copy Protocol).

Problema

A volte, in un ambiente sicuro, è difficile raggiungere un server TFTP/ FTP/ SFTP/ SCP per copiare l'immagine Cisco IOS su router e switch. Il firewall potrebbe bloccare le porte utilizzate da uno dei protocolli menzionati in precedenza tra i dispositivi di origine e di destinazione.

Soluzione

Se SCP è abilitato sul dispositivo Cisco, è possibile copiare il file da un PC locale su dispositivi senza alcun server o applicazione. Ottenere l'immagine software Cisco IOS dal portale di download, annotare l'MD5 dell'immagine e convalidarla sul PC locale.

Linux:

```
[root@root ios]# ls -lshr
total 183M
80M   -rw-r--r--. 1 root root 80M Mar 23 11:52 cgr2010-universalk9-mz.SPA.157-3.M6.bin
103M -rw-r--r--. 1 root root 103M Mar 24 09:35 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
[root@root ios]# md5sum c3900e-universalk9-mz.SPA.155-1.T2.bin
19c881db6ea7ad92dc71f35807a44b82 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

Gli utenti di Windows possono utilizzare WinMD5 o un'applicazione simile, in grado di calcolare l'MD5 del file. Il macOS ha una riga di comando simile a Linux.

L'MD5 dell'immagine Cisco IOS deve essere lo stesso per escludere eventuali danneggiamenti al momento del trasferimento. Verificare di disporre dell'accesso SSH dal PC locale al dispositivo con livello di accesso 15 e dei diritti di amministratore per apportare modifiche alla configurazione sui dispositivi.

Ecco la configurazione minima richiesta sul dispositivo.

```
hostname CGR2010
!
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
no shut
!
ip route 0.0.0.0 0.0.0.0 x.x.x.x
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
ip domain name cisco.com
!
```

```
!--- key used in this example is 1024

!
crypto key generate rsa
!
username cisco privilege 15 secret 5 $1$jv8O$1VC3PmgNX9o.rsDD3DKeV1
!
line vty 0 4
transport input ssh
!
ip scp server enable
!
end
```

!--- optional

```
!
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2
!
```

Copiare le immagini Cisco IOS con questo comando:

```
scp ios_filename username@<ip_address_of_the_device>:ios_filename
```

Windows 10:

```
Microsoft Windows [Version 10.0.17134.1365]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\mmehtabu>cd /
C:\>cd ios
```

```
C:\ios>dir
Volume in drive C is OSDisk
Volume Serial Number is 0003-4095
```

Directory of C:\ios

```
04/10/2020 01:43 PM <DIR> .
03/24/2020 09:35 AM 107,892,232 c3900e-universalk9-mz.SPA.155-1.T2.bin
1 File(s) 107,892,232 bytes
2 Dir(s) 84,203,741,184 bytes free
```

```
C:\ios>scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-universalk9-
mz.SPA.155-1.T2.bin
```

```
Password:
c3900e-universalk9-mz.SPA.155-1.T2.bin 100%
103MB 61.8KB/s 28:26
```

Linux:

```
[root@root ios]# scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-
universalk9-mz.SPA.155-1.T2.bin
```

```
Password:
c3900e-universalk9-mz.SPA.155-1.T2.bin 100%
103MB 517.1KB/s 03:23
```

```
Connection to 10.106.37.44 closed by remote host.
```

Il macOS ha un comando simile:

```
scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

A questo punto, verificare il MD5 del file sul dispositivo.

```
login as: cisco
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
```

```
CISCO3945#dir
```

```
Directory of flash0:/
```

```
1 -rw- 106362996 Apr 10 2020 07:07:06 +00:00 c3900e-universalk9-mz.SPA.154-3.M3.bin
2 -rw- 107892232 Apr 10 2020 07:16:50 +00:00 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
1024655360 bytes total (810369024 bytes free)
```

```
CISCO3945#verify flash0:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
Starting image verification
Hash Computation: 100% Done!
.. omitted for brevity ...
```

```
CCO Hash MD5 : 19C881DB6EA7AD92DC71F35807A44B82
```

```
Digital signature successfully verified in file flash0:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

In tutti i casi, MD5 deve corrispondere per escludere qualsiasi danneggiamento del file al momento del trasferimento da Cisco.com al PC e ad altri dispositivi.

Informazioni correlate

- [Guida alla configurazione di Secure Shell](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).