Configurare il trasferimento di file MDS 9000 SCP senza password

Sommario

Introduzione

In questo documento viene descritto come configurare Multilayer Data Switch (MDS) 9000 in modo che trasferisca le informazioni tramite il protocollo SSH (Secure Shell) senza fornire una password per l'utente.

Problema

Per impostazione predefinita, il trasferimento di file da uno switch MDS su SSH tramite protocolli come Secure Copy (SCP) richiede una password. L'immissione interattiva di una password SSH può essere scomoda e alcuni script utente esterni potrebbero non essere in grado di fornire la password in modo interattivo.

Soluzione

Generare una coppia di chiavi pubblica/privata sullo switch MDS e aggiungere la chiave pubblica a un file authorized_keys dell'account utente sul server SSH.

Prerequisiti

Per questo esempio, un server Linux generico (RedHat, Ubuntu, ecc.) configurato con un server SSH e un client installato.

Panoramica

Questo documento descrive i passaggi necessari per un trasferimento SSH da MDS 9000 a un server Linux senza fornire una password, descritta in quattro passaggi.

- Configurazione della coppia di chiavi pubblica/privata per l'account utente che verrà

configurato per "copiare" i dati dallo switch. (ossia l'account da cui verrà eseguito il comando SSH o SCP, nell'esempio "testuser")
- Configurare la coppia di chiavi pubblica/privata per l'account utente sull'host Linux in modo che l'utente "testuser" possa copiare o spostare le informazioni fuori dallo switch senza dover fornire la password dal prompt dello switch.
- Verificare l'SCP tra lo switch e l'host Linux.

Configurazione della coppia di chiavi pubblica/privata per l'account utente su MDS

Dallo switch MDS 9000, creare il nome utente "testuser" con password e ruolo di amministratore di rete. Assicurarsi di creare l'utente e l'utente con il ruolo di amministratore di rete affinché la generazione delle chiavi funzioni.

```
sw12# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw12(config)# username testuser password cisco_123 role network-admin
sw12(config)# cop run start
[########################################] 100%
sw12(config)#
```

SSH sullo switch dall'host Linux con il nome utente creato nel passaggio precedente:

```
sj-lnx[85]:~$ ssh testuser@192.168.12.112
User Access Verification
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2010, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
sw12#
```

Generare la coppia di chiavi per l'utente testuser utilizzando rsa con lunghezza di 1024 bit.

```
sw12# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw12(config)# username testuser keypair generate rsa 1024
generating rsa key(1024 bits)......
generated rsa key
sw12(config)# show username testuser keypair
**********************************

rsa Keys generated:Tue Apr 16 15:05:18 2013
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAs3RocZLGp0y0sTdKXydmJDQVG//wAWXys7xk2DrcgQco
fY8+bRUBAUfMasoOVUvrCvV0qOdC8woV4KgF0nQgfX/mhuKqjWHW6IEBMmPY8v+OjXn+Avj3CH8K7h1z
tmbtFPo04rR7ivJx/boPQopk7mlpeocEzpVihOCIRiVJaj0=
```

```
bitcount:1024
fingerprint:
8b:d8:7b:2f:bf:14:ee:bc:a4:d3:54:0a:9a:4d:db:60
************************************
could not retrieve dsa key information
************************************
sw12(config)# cop run start
[########################################] 100%
sw12(config)#
```

Esportare la coppia di chiavi in bootflash:, fornire la **passphrase** (qualsiasi cosa si voglia, prendere nota di esso da qualche parte).

```
sw12(config)# username testuser keypair export bootflash:testuser_rsa rsa
Enter Passphrase:
sw12(config)# dir bootflash:
      16384    Apr 15 15:21:31 2012  lost+found/
   18693120    Apr 15 15:22:55 2012  m9100-s3ek9-kickstart-mz.5.0.1a.bin
  73579433    Apr 15 15:23:53 2012  m9100-s3ek9-mz.5.0.1a.bin
      5778    Apr 15 15:24:48 2013  mts.log
       951    Apr 16 15:07:01 2013  testuser_rsa
       219    Apr 16 15:07:02 2013  testuser_rsa.pub
Usage for bootflash://sup-local
 143622144 bytes used
 533487616 bytes free
 677109760 bytes total
sw12(config)#
```

Configurazione della coppia di chiavi pubblica/privata per l'account utente sull'host Linux

Copiare la chiave pubblica rsa per l'utente testuser dallo switch all'host Linux con il nome utente "testuser" già presente. Notare che è necessario fornire la password per username testuser, che può essere o non essere la stessa di quella precedentemente creata sullo switch.

> **Nota:** In queste istruzioni viene utilizzato un esempio in cui il percorso dell'account testuser è **/users/testuser**. A seconda della versione di Linux in uso, questo percorso potrebbe essere diverso.

```
sw12(config)# copy bootflash:testuser_rsa.pub scp://testuser@192.168.12.100/users/testuser/.ssh
The authenticity of host '192.168.12.100 (192.168.12.100)' can't be established.
RSA key fingerprint is 91:42:28:58:f9:51:31:4d:ba:ac:95:50:51:09:96:74.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.12.100' (RSA) to the list of known hosts.


testuser@192.168.12.100's password:
testuser_rsa.pub                              100%  219     0.2KB/s   00:00

sw12(config)# dir bootflash:
     16384    Apr 15 15:21:31 2012  lost+found/
  18693120    Apr 15 15:22:55 2012  m9100-s3ek9-kickstart-mz.5.0.1a.bin
  73579433    Apr 15 15:23:53 2012  m9100-s3ek9-mz.5.0.1a.bin
      5778    Apr 15 15:24:48 2013  mts.log
       951    Apr 16 15:07:01 2013  testuser_rsa
       219    Apr 16 15:07:02 2013  testuser_rsa.pub

Usage for bootflash://sup-local
 143622144 bytes used
```

```
 533487616 bytes free
 677109760 bytes total

sw12(config)#
```

Sul server Linux è necessario aggiungere il contenuto del file testuser_rsa.pub al file authorized_keys (o al file authorized_keys2 a seconda della versione di SSH in uso):

```
sj-lnx[91]:~/$ cd .ssh
sj-lnx[92]:~/.ssh$ chmod 644 authorized_keys2
sj-lnx[93]:~/.ssh$ ls -lrt
lrwxrwxrwx 1 testuser  eng    16 Apr  7  2005 authorized_keys -> authorized_keys2
-rw-r--r-- 1 testuser eng  1327 Apr 16 15:04 authorized_keys2
-rw-r--r-- 1 testuser eng   219 Apr 16 15:13 testuser_rsa.pub

sj-lnx[94]:~/.ssh$ cat testuser_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAs3RocZLGp0y0sTdKXydmJDQVG//wAWXys7xk2DrcgQcofY8+bRUBAUfMasoOVUvrCvV0
qOdC8woV4KgF0nQgfX/mhuKqjWHW6IEBMmPY8v+OjXn+Avj3CH8K7h1ztmbtFPo04rR7ivJx/boPQopk7mlpeocEzpVihOCI
RiVJaj0= root@sw12
sj-lnx[95]:~/.ssh$ cat testuser_ras.pub >> authorized_keys2
sj-lnx[96]:~/.ssh$ cat authorized_keys2
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA1XMy4dbF5Vy4+wvYWS7s/luE/HoyX+HD6Kwrre5lEP7ZRKm1S3blWxZeYIYuhL7kU714
ZM0r4NzEcV2Jdt6/7Hai5FlnKqA04AOAYH6jiPcw0fjdLB98q96B4G5XvaoV7VP2HTNn7Uw5DpQ3+ODwjCgQE7PvBOS2yGKt
9gYbLd8= root@sw12
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAs3RocZLGp0y0sTdKXydmJDQVG//wAWXys7xk2DrcgQcofY8+bRUBAUfMasoOVUvrCvV0
qOdC8woV4KgF0nQgfX/mhuKqjWHW6IEBMmPY8v+OjXn+Avj3CH8K7h1ztmbtFPo04rR7ivJx/boPQopk7mlpeocEzpVihOCI
RiVJaj0= root@sw12

sj-lnx[97]:~/.ssh$
```

Verificare l'SCP tra lo switch e l'host Linux.

Verificare SCP dallo switch al server Linux e verificare la copia dallo switch al server senza fornire la password. (Si noti che non viene richiesta alcuna password...)

```
sw12(config)# dir bootflash:
     16384    Apr 15 15:21:31 2012  lost+found/
  18693120    Apr 15 15:22:55 2012  m9100-s3ek9-kickstart-mz.5.0.1a.bin
  73579433    Apr 15 15:23:53 2012  m9100-s3ek9-mz.5.0.1a.bin
      5778    Apr 15 15:24:48 2013  mts.log
       951    Apr 16 15:07:01 2013  testuser_rsa
       219    Apr 16 15:07:02 2013  testuser_rsa.pub

Usage for bootflash://sup-local
 143622144 bytes used
 533487616 bytes free
 677109760 bytes total

sw12(config)# copy bootflash:mts.log scp://testuser@192.168.12.100/users/testuser


mts.log                                       100% 5778     5.6KB/s   00:00
sw12(config)#
```