

Transferencia de archivos de la configuración MDS9000 SCP sin una contraseña

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Requisitos previos](#)

[Información general](#)

[Configurar los pares del público/de clave privada para la cuenta de usuario en el MDS](#)

[Configurar los pares del público/de clave privada para la cuenta de usuario en el host de Linux](#)

[Pruebe SCP del Switch al host de Linux.](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento describe cómo poner el switch de datos de múltiples capas (MDS) 9000 para transferir la información vía el protocolo del Secure Shell (SSH) sin proporcionar a una contraseña para el usuario.

Problema

La transferencia clasifia de un Switch MDS sobre SSH, usando los protocolos como el Secure Copy (SCP), requiere una contraseña por abandono. Recíprocamente proporcionar a una contraseña de SSH puede ser incómodo y algunos scripts del usuario externo pueden no poder proporcionar la contraseña recíprocamente.

Solución

Genere los keypairs públicos/privados en el Switch MDS y agregue la clave pública a los `authorized_keys` de una cuenta de usuario clasifian en el servidor SSH.

Requisitos previos

Por este ejemplo, un servidor Linux genérico (RedHat, Ubuntu, etc.) configurado con un servidor SSH y el cliente instalado.

Información general

Este documento delinea los pasos requeridos para una transferencia SSH del MDS9000 a un servidor del linux sin proporcionar a una contraseña, que se describe en cuatro pasos.

- Configurando los pares del público/de clave privada para la cuenta de usuario que será

puesta “para copiar” el Switch de los de los datos. (es decir la cuenta de las cuales el comando de SSH o de SCP será ejecutada, en testuser de este ejemplo “”)

- Configurar los pares del público/de clave privada para la cuenta de usuario en el host de Linux de modo que el usuario “testuser” deba copiar o mover el Switch de los de la información sin tener que proporcionar la contraseña del prompt del Switch.
- Pruebe SCP del Switch al host de Linux.

Configurar los pares del público/de clave privada para la cuenta de usuario en el MDS

Del Switch MDS9000, cree el nombre de usuario “testuser” con la contraseña y el papel como red-admin. Asegurese crear el usuario y al usuario del papel red-admin para que la generación del keypair trabaje.

```
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 en el Switch del host de Linux con el nombre de usuario creado en el paso anterior:

```
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#
```

Genere el keypair para el testuser del usuario usando el rsa con la longitud de 1024 bits.

```
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)#
```

Exporte el keypair al bootflash: , proporcione el **passphrase** (sea cual sea usted quiere, apenas anota él en alguna 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)#
```

Configurar los pares del público/de clave privada para la cuenta de usuario en el host de Linux

Copie la clave pública rsa para el testuser del usuario del Switch sobre el host de Linux con el nombre de usuario presente del “testuser” ya. Observe por favor que usted necesitará proporcionar la contraseña para el testuser del nombre de usuario que pueden o no pueden ser lo mismo que lo que fue creada previamente en el Switch.

Nota: Estas instrucciones utilizan un ejemplo donde está **/users/testuser** la trayectoria de la cuenta del testuser. Dependiendo de su versión de Linux esta trayectoria puede ser diferente.

```
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)#
```

En el servidor Linux usted necesita agregar el contenido del archivo testuser_rsa.pub al archivo

de los `authorized_keys` (o al archivo `authorized_keys2` dependiendo de su versión de SSH):

```
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@swl2
sj-lnx[95]:~/ .ssh$ cat testuser_ras.pub >> authorized_keys2
sj-lnx[96]:~/ .ssh$ cat authorized_keys2
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA1XMy4dbF5Vy4+wwVWS7s/luE/HoyX+HD6Kwrre5lEP7ZRKm1S3blWxZeYIYuhL7kU714
ZM0r4NzEcV2Jdt6/7Hai5FlnKqA04A0AYH6jiPcw0fjdLB98q96B4G5XvaoV7VP2HTNn7Uw5DpQ3+ODwjCgQE7PvBOS2yGKT
9gYbLd8= root@swl2
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAs3RocZLGp0y0sTdKXydmJDQVG//wAWXys7xk2DrcgQcofY8+bRUBAUfMasoOVUvrCvV0
qOdC8woV4KgF0nQgfX/mhuKqjWHW6IEBMmPY8v+OjXn+Avj3CH8K7h1ztmbtFPo04rR7ivJx/boPQopk7mlpeocEzpVihOCI
RiVJaj0= root@swl2

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

Pruebe SCP del Switch al host de Linux.

Pruebe SCP del Switch al servidor Linux y verifique la copia del Switch al servidor sin proporcionar a la contraseña. (Observe por favor que no se indica "ninguna contraseña para... ")

```
swl2(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

swl2(config)# copy bootflash:mts.log scp://testuser@192.168.12.100/users/testuser

mts.log                               100% 5778      5.6KB/s   00:00
swl2(config)#
```