Configuración de la transferencia de archivos SCP MDS 9000 sin contraseña

Contenido

Introducción

Este documento describe cómo configurar el switch de datos multicapa (MDS) 9000 para transferir información a través del protocolo Secure Shell (SSH) sin proporcionar una contraseña para el usuario.

Problema

La transferencia de archivos desde un switch MDS a través de SSH, mediante protocolos como Secure Copy (SCP), requiere una contraseña de forma predeterminada. Proporcionar de forma interactiva una contraseña SSH puede ser inconveniente y es posible que algunos scripts de usuario externos no puedan proporcionar la contraseña de forma interactiva.

Solución

Genere pares de llaves públicas/privadas en el switch MDS y agregue la clave pública a un archivo authorized_keys de cuenta de usuario en el servidor SSH.

Requisitos previos

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

Overview

Este documento describe los pasos necesarios para una transferencia SSH desde el MDS 9000 a un servidor Linux sin proporcionar una contraseña, que se describe en cuatro pasos.

- Configuración del par de claves pública/privada para la cuenta de usuario que se configurará

para "copiar" los datos del switch. (es decir, la cuenta desde la que se ejecutará el comando SSH o SCP, en este ejemplo "testuser")
- Configuración del par de claves pública/privada para la cuenta de usuario en el host Linux para que el usuario "testuser" copie o mueva la información fuera del switch sin tener que proporcionar la contraseña desde el prompt del switch.
- Pruebe SCP del switch al host Linux.

Configuración del par de claves pública/privada para la cuenta de usuario en el MDS

Desde el switch MDS 9000, cree el nombre de usuario "testuser" con contraseña y función como administrador de red. Asegúrese de crear el usuario y el usuario de rol administrador de red para que funcione la generación de pares de claves.

```
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 desde el host 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 par de claves para el usuario testuser usando rsa con una 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)#
```

Exportar el par de claves a la memoria flash de inicialización:, proporcione la **frase de paso** (lo que sea que desee, sólo tenga en cuenta 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)#
```

Configuración del par de claves pública/privada para la cuenta de usuario en el host Linux

Copie la clave pública rsa para el usuario testuser del switch en el host Linux con el nombre de usuario "testuser" ya presente. Tenga en cuenta que deberá proporcionar la contraseña para el usuario testuser que puede o no ser la misma que la que se creó previamente en el switch.

> **Nota:** Estas instrucciones utilizan un ejemplo donde la trayectoria de la cuenta del usuario testuser es **/users/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 debe agregar el contenido del archivo testuser_rsa.pub al archivo authorized_keys (o 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@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$
```

Pruebe SCP del switch al host Linux.

Pruebe SCP del switch al servidor Linux y verifique la copia del switch al servidor sin proporcionar la contraseña. (Tenga en cuenta que "No se solicita ninguna contraseña para...")

```
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)#
```