Configurar transferência de arquivo MDS9000 SCP sem uma senha

Índice

Introdução

Este documento descreve como setup o switch de dados Multilayer (MDS) 9000 para transferir a informação através do protocolo do Shell Seguro (ssh) sem fornecer uma senha para o usuário.

Problema

Transferir arquiva de um interruptor MDS sobre o SSH, usando protocolos como o Secure Copy (SCP), exige uma senha à revelia. Interativamente fornecer uma senha SSH pode ser incômodo e alguns scripts do usuário externo não podem poder fornecer interativamente a senha.

Solução

Gerencia keypairs públicos/privados no interruptor MDS e adicionar a chave pública aos authorized_keys de uma conta de usuário arquivam no servidor de SSH.

Condições prévias

Para este exemplo, um servidor Linux genérico (RedHat, Ubuntu, etc.) configurado com um servidor de SSH e o cliente instalado.

Visão geral

Este documento esboça as etapas exigidas para transferência SSH do MDS9000 a um server do linux sem fornecer uma senha, que seja descrita em quatro etapas.

- Estabelecendo os pares do público/chave privada para a conta de usuário que setup “para copiar” os dados fora do interruptor. (isto é a conta de que o comando SSH ou SCP será executada, usuário de teste neste exemplo “")

- Estabelecendo os pares do público/chave privada para a conta de usuário no host de Linux de modo que o usuário “usuário de teste” deva copiar ou mover a informação fora do interruptor sem ter que fornecer a senha da alerta do interruptor.
- Teste o SCP do interruptor ao host de Linux.

Estabelecendo os pares do público/chave privada para a conta de usuário no MDS

Do interruptor MDS9000, crie o username “usuário de teste” com a senha e o papel como o rede-admin. Certifique-se criar o usuário e o usuário do papel rede-admin para que a geração do keypair trabalhe.

```
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 no interruptor do host de Linux com o username criado na etapa 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#
```

Gerencia o keypair para o usuário de teste do usuário usando rsa com comprimento de 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)#
```

Exporte o keypair para o bootflash: , forneça a **frase de passagem** (o que quer que você quer, apenas fazem uma anotação dela em algum lugar.)

```
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)#
```

Estabelecendo os pares do público/chave privada para a conta de usuário no host de Linux

Copie a chave pública dos rsa para o usuário de teste do usuário do interruptor no host de Linux com username presente do “usuário de teste” já. Note por favor que você precisará de fornecer a senha para o usuário de teste username que pode ou não pode ser o mesmo como o que foi criado previamente no interruptor.

> Nota: Estas instruções usam um exemplo onde o trajeto da conta do usuário de teste seja **/users/testuser**. Segundo sua versão linux este trajeto pode 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)#
```

No servidor Linux você precisa de adicionar índices do arquivo testuser_rsa.pub ao arquivo dos authorized_keys (ou ao arquivo authorized_keys2 segundo sua versão do 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$
```

Teste o SCP do interruptor ao host de Linux.

Teste o SCP do interruptor ao servidor Linux e verifique a cópia do interruptor ao server sem fornecer a senha. (Note por favor que “nenhuma senha está alertada 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)#
```