Configurar a transferência de arquivo SCP MDS 9000 sem uma senha

Contents

Introduction

Este documento descreve como configurar o Multilayer Data Switch (MDS) 9000 para transferir informações através do protocolo Secure Shell (SSH) sem fornecer uma senha ao usuário.

Problema

A transferência de arquivos de um switch MDS sobre SSH, usando protocolos como o Secure Copy (SCP), requer uma senha por padrão. O fornecimento interativo de uma senha SSH pode ser inconveniente e alguns scripts de usuário externo talvez não consigam fornecer a senha interativamente.

Solução

Gere pares de chaves públicos/privados no switch MDS e adicione a chave pública a um arquivo user account authorized_keys no servidor SSH.

Pré-requisitos

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

Overview

Este documento descreve as etapas necessárias para uma transferência SSH do MDS 9000 para um servidor linux sem fornecer uma senha, que é descrita em quatro etapas.

- Configurar o par de chaves públicas/privadas para a conta de usuário que será configurada para "copiar" os dados do switch. (ou seja, a conta da qual o comando SSH ou SCP será

executado, neste exemplo, "testuser")
- Configurar o par de chaves públicas/privadas para a conta de usuário no host Linux para que o usuário "testuser" copie ou mova as informações para fora do switch sem precisar fornecer a senha do prompt do switch.
- Teste a SCP do switch para o host Linux.

Configurar o par de chaves públicas/privadas para a conta de usuário no MDS

A partir do switch MDS 9000, crie o nome de usuário "testuser" com senha e função como network-admin. Certifique-se de criar o usuário e o usuário da função de administrador de rede para que a geração de pares de chaves funcione.

```
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)#
```

Faça SSH no switch a partir do host Linux com o nome de usuário criado na etapa 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#
```

Gere o par de chaves para usuário testuser usando rsa com comprimento 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 o par de chaves para bootflash:, forneça a **senha** (o que você quiser, apenas anote-a 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)#
```

Configurando o par de chaves públicas/privadas para a conta de usuário no host Linux

Copie a chave pública rsa para o usuário testado do switch para o host Linux com o nome de usuário "testuser" já presente. Observe que você precisará fornecer a senha para o usuário testuser que pode ser ou não a mesma que foi criada anteriormente no switch.

> **Note**: Essas instruções usam um exemplo em que o caminho da conta do usuário de teste é **/users/testuser**. Dependendo da versão do Linux, esse caminho 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 adicionar conteúdo do arquivo testuser_rsa.pub ao arquivo authorized_keys (ou authorized_keys2, dependendo da 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 a SCP do switch para o host Linux.

Teste a SCP do switch para o servidor Linux e verifique a cópia do switch para o servidor sem fornecer a senha. (Observe que "Nenhuma senha é solicitada...")

```
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)#
```