Configurer le transfert de fichiers SCP MDS 9000 sans mot de passe

Contenu

Introduction

Ce document décrit comment configurer le commutateur de données multicouche (MDS) 9000 pour transférer des informations via le protocole SSH (Secure Shell) sans fournir de mot de passe à l'utilisateur.

Problème

Le transfert de fichiers à partir d'un commutateur MDS sur SSH, à l'aide de protocoles tels que Secure Copy (SCP), nécessite un mot de passe par défaut. La fourniture interactive d'un mot de passe SSH peut s'avérer gênante et certains scripts utilisateur externes peuvent ne pas être en mesure de fournir le mot de passe de manière interactive.

Solution

Générez des paires de clés publiques/privées sur le commutateur MDS et ajoutez la clé publique à un fichier de clés autorisées de compte d'utilisateur sur le serveur SSH.

Conditions préalables

Pour cet exemple, un serveur Linux générique (RedHat, Ubuntu, etc.) configuré avec un serveur et un client SSH installé.

Aperçu

Ce document décrit les étapes requises pour un transfert SSH du MDS 9000 vers un serveur Linux sans fournir de mot de passe, qui est décrit en quatre étapes.

- Configuration de la paire de clés publique/privée pour le compte d'utilisateur qui sera

configuré pour “ la copie ” données à partir du commutateur. (c'est-à-dire le compte à partir duquel la commande SSH ou SCP sera exécutée, dans cet exemple “ testuser ”)
- Configuration de la paire de clés publique/privée pour le compte d'utilisateur sur l'hôte Linux de sorte que l'utilisateur “ testeur ” utilisateur copie ou déplace les informations hors du commutateur sans avoir à fournir le mot de passe à partir de l'invite du commutateur.
- Testez SCP du commutateur vers l'hôte Linux.

Configuration de la paire de clés publique/privée pour le compte d'utilisateur sur le MDS

Àpartir du commutateur MDS 9000, créez le nom d'utilisateur “ tesuser user ” avec mot de passe et rôle en tant qu'administrateur réseau. Veillez à créer l'utilisateur et l'utilisateur du rôle d'administrateur réseau pour que la génération de paires de clés fonctionne.

```
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 dans le commutateur à partir de l'hôte Linux avec le nom d'utilisateur créé à l'étape précédente :

```
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#
```

Générez la paire de clés pour l'utilisateur testuser à l'aide de rsa d'une longueur de 1 024 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)#
```

Exportez la paire de clés vers bootflash:, fournissez la **phrase de passe** (Peu importe ce que vous voulez, faites-en une note quelque part.)

```
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)#
```

Configuration de la paire de clés publique/privée pour le compte d'utilisateur sur l'hôte Linux

Copiez la clé publique rsa pour l'utilisateur testuser à partir du commutateur sur l'hôte Linux avec le nom d'utilisateur « testuser » déjà présent. Veuillez noter que vous devrez fournir le mot de passe de username testuser qui peut être identique ou non à celui précédemment créé sur le commutateur.

> **Note**: Ces instructions utilisent un exemple où le chemin du compte testuser est **/users/testuser**. Selon votre version Linux, ce chemin peut être différent.

```
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)#
```

Sur le serveur Linux, vous devez ajouter le contenu du fichier testuser_rsa.pub au fichier allowed_keys (ou au fichier Authorized_keys2 selon votre version 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$
```

Testez SCP du commutateur vers l'hôte Linux.

Testez SCP du commutateur au serveur Linux et vérifiez la copie du commutateur au serveur sans fournir le mot de passe. (Veuillez noter que “ mot de passe n'est pas demandé... ”)

```
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)#
```