Konfigurieren der SCP-Dateiübertragung MDS 9000 ohne Kennwort

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Multilayer Data Switch (MDS) 9000 so eingerichtet wird, dass Informationen über das Secure Shell (SSH)-Protokoll übertragen werden, ohne dass ein Kennwort für den Benutzer angegeben wird.

Problem

Die Übertragung von Dateien von einem MDS-Switch über SSH mithilfe von Protokollen wie Secure Copy (SCP) erfordert standardmäßig ein Kennwort. Die interaktive Bereitstellung eines SSH-Kennworts kann unbequem sein, und einige externe Benutzerskripts können das Kennwort möglicherweise nicht interaktiv bereitstellen.

Lösung

Generieren Sie öffentliche/private Tastenanschläge auf dem MDS-Switch, und fügen Sie den öffentlichen Schlüssel einer Datei für autorisierte Benutzerkonten auf dem SSH-Server hinzu.

Voraussetzungen

In diesem Beispiel ein generischer Linux-Server (RedHat, Ubuntu usw.), der mit einem SSH-Server konfiguriert ist und auf dem ein Client installiert ist.

Übersicht

In diesem Dokument werden die Schritte beschrieben, die für eine SSH-Übertragung vom MDS 9000 auf einen Linux-Server ohne Eingabe eines Kennworts erforderlich sind. Dies wird in vier Schritten beschrieben.

- Einrichten des öffentlichen/privaten Schlüsselpaars für das Benutzerkonto, das eingerichtet wird, um die Daten aus dem Switch zu "kopieren". (d. h. das Konto, von dem aus der SSH- oder SCP-Befehl ausgeführt wird, in diesem Beispiel "testuser")
- Einrichten des öffentlichen/privaten Schlüsselpaars für das Benutzerkonto auf dem Linux-Host, sodass der Benutzer "testuser" die Informationen kopieren oder aus dem Switch verschieben kann, ohne das Kennwort von der Switch-Eingabeaufforderung eingeben zu müssen.
- Testen Sie SCP vom Switch zum Linux-Host.

Einrichten des öffentlichen/privaten Schlüsselpaars für das Benutzerkonto auf dem MDS

Erstellen Sie auf dem MDS 9000-Switch den Benutzernamen "testuser" mit Kennwort und Rolle als "network-admin". Stellen Sie sicher, dass Sie den Benutzer und die Rolle "network-admin" erstellen, damit die Tastenanschlag-Generierung funktioniert.

```
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 vom Linux-Host zum Switch mit dem im vorherigen Schritt erstellten Benutzernamen:

```
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#
```

Generieren Sie den Tastenfeld für den Benutzer-Testbenutzer mit einer Länge von 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)#
```

Exportieren Sie den Tastenfeld in bootflash:, geben Sie die **Passphrase ein** (egal, was Sie möchten, notieren Sie sich die Passphrase einfach irgendwo.)

```
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)#
```

Einrichten des öffentlichen/privaten Schlüsselpaars für das Benutzerkonto auf dem Linux-Host

Kopieren Sie den öffentlichen rsa-Schlüssel für den Benutzer-Testuser vom Switch auf den Linux-Host, wobei der Benutzername "testuser" bereits vorhanden ist. Bitte beachten Sie, dass Sie das Kennwort für den Benutzernamen-Testbenutzer angeben müssen, das möglicherweise mit dem auf dem Switch erstellten Kennwort übereinstimmt.

> **Hinweis**: In diesen Anweisungen wird ein Beispiel verwendet, in dem der Pfad des Testbenutzerkontos **/Benutzer/Testuser** lautet. Abhängig von Ihrer Linux-Version kann dieser Pfad unterschiedlich sein.

```
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)#
```

Auf dem Linux-Server müssen Sie der Datei authorized_keys (oder der Datei authorized_keys2, abhängig von Ihrer Version von SSH) den Inhalt der Datei testuser_rsa.pub hinzufügen:

```
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$
```

Testen Sie SCP vom Switch zum Linux-Host.

Testen Sie SCP vom Switch zum Linux-Server, und überprüfen Sie die Kopie vom Switch zum Server, ohne das Kennwort einzugeben. (Bitte beachten Sie, dass "Es wird kein Kennwort zur Eingabe von ... eingegeben.".)

```
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)#
```