Dernière mise-à-jour : 2020/01/30 03:27

212.3 - SSH (4/60)

LPI 212.3 - Secure shell (SSH)

Weight: 4

Description: Candidates should be able to configure and secure an SSH daemon. This objective includes managing keys and configuring SSH for users. Candidates should also be able to forward an application protocol over SSH and manage the SSH login.

Key Knowledge Areas:

- OpenSSH configuration files, tools and utilities
- Login restrictions for the superuser and the normal users
- Managing and using server and client keys to login with and without password
- Usage of multiple connections from multiple hosts to guard against loss of connection to remote host following configuration changes

Terms and Utilities:

- ssh
- sshd
- /etc/ssh/sshd_config
- /etc/ssh/
- Private and public key files
- PermitRootLogin, PubKeyAuthentication, AllowUsers, PasswordAuthentication, Protocol

Introduction

La commande **ssh** est le successeur et la remplaçante de la commande **rlogin**. Il permet d'établir des connexions sécurisées avec une machine

distante. SSH comporte cinq acteurs :

- Le **serveur SSH**
  - le démon sshd, qui s'occupe des authentifications et autorisations des clients,
- Le **client SSH**
  - ssh ou scp, qui assure la connexion et le dialogue avec le serveur,
- La **session** qui représente la connexion courante et qui commence juste après l'authentification réussie,
- Les **clefs**
  - **Couple de clef utilisateur asymétriques** et persistantes qui assurent l'identité d'un utilisateur et qui sont stockés sur disque dur,
  - **Clef hôte asymétrique et persistante** garantissant l'identité du serveur er qui est conservé sur disque dur
  - **Clef serveur asymétrique et temporaire** utilisée par le protocole SSH1 qui sert au chiffrement de la clé de session,
  - **Clef de session symétrique qui est générée aléatoirement** et qui permet le chiiffrement de la communication entre le client et le serveur. Elle est détruite en fin de session. SSH-1 utilise une seule clef tandis que SSH-2 utilise une clef par direction de la communication,
- La **base de données des hôtes connus** qui stocke les clés des connexions précédentes.

SSH fonctionne de la manière suivante pour la la mise en place d'un canal sécurisé:

- Le client contacte le serveur sur son port 22,
- Les client et le serveur échangent leur version de SSH. En cas de non-compatibilité de versions, l'un des deux met fin au processus,
- Le serveur SSH s'identifie auprès du client en lui fournissant :
  - Sa clé hôte,
  - Sa clé serveur,
  - Une séquence aléatoire de huit octets à inclure dans les futures réponses du client,
  - Une liste de méthodes de chiffrage, compression et authentification,
- Le client et le serveur produisent un identifiant identique, un haché MD5 long de 128 bits contenant la clé hôte, la clé serveur et la séquence aléatoire,
- Le client génère sa clé de session symétrique et la chiffre deux fois de suite, une fois avec la clé hôte du serveur et la deuxième fois avec la clé serveur. Le client envoie cette clé au serveur accompagnée de la séquence aléatoire et un choix d'algorithmes supportés,
- Le serveur déchiffre la clé de session,
- Le client et le serveur mettent en place le canal sécurisé.

SSH-1

SSH-1 utilise une paire de clefs de type RSA1. Il assure l'intégrité des données par une **Contrôle de Redondance Cyclique** (CRC) et est un bloc dit **monolithique**.

Afin de s'identifier, le client essaie chacune des six méthodes suivantes :

- **Kerberos**,
- **Rhosts**,
- **RhostsRSA**,
- Par **clef asymétrique**,
- **TIS**,
- Par **mot de passe**.

SSH-2

SSH-2 utilise **DSA** ou **RSA**. Il assure l'intégrité des données par l'algorithme **HMAC**. SSH-2 est organisé en trois **couches** :

- **SSH-TRANS** – Transport Layer Protocol,
- **SSH-AUTH** – Authentification Protocol,
- **SSH-CONN** – Connection Protocol.

SSH-2 diffère de SSH-1 essentiellement dans la phase authentification.

Trois méthodes d'authentification :

- Par **clef asymétrique**,
  - Identique à SSH-1 sauf avec l'algorithme DSA,
- **RhostsRSA**,
- Par **mot de passe**.

Options de la commande

Les options de cette commande sont :

```
[root@centos6 ~]# ssh --help
usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-e escape_char] [-F configfile]
           [-i identity_file] [-L [bind_address:]port:host:hostport]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-R [bind_address:]port:host:hostport] [-S ctl_path]
           [-w local_tun[:remote_tun]] [user@]hostname [command]
```

L'authentification par mot de passe

L'utilisateur fournit un mot de passe au client ssh. Le client ssh le transmet de façon sécurisée au serveur ssh puis le serveur vérifie le mot de passe et l'accepte ou non.

Avantage:

- Aucune configuration de clef asymétrique n'est nécessaire.

Inconvénients:

- L'utilisateur doit fournir à chaque connexion un identifiant et un mot de passe,
- Moins sécurisé qu'un système par clef asymétrique.

L'authentification par clef asymétrique

- Le **client** envoie au serveur une requête d'authentification par clé asymétrique qui contient le module de la clé à utiliser,
- Le **serveur** recherche une correspondance pour ce module dans le fichier des clés autorisés **~/.ssh/authorized_keys**,
  - Dans le cas où une correspondance n'est pas trouvée, le serveur met fin à la communication,
  - Dans le cas contraire le serveur génère une chaîne aléatoire de 256 bits appelée un **challenge** et la chiffre avec la **clé publique du client**,
- Le **client** reçoit le challenge et le décrypte avec la partie privée de sa clé. Il combine le challenge avec l'identifiant de session et chiffre le résultat. Ensuite il envoie le résultat chiffré au serveur.

- Le **serveur** génère le même haché et le compare avec celui reçu du client. Si les deux hachés sont identiques, l'authentification est réussie.

Installation

Pour installer/mettre à jour le serveur **sshd**, utilisez **yum** :

```
[root@centos7 ~]# yum install openssh-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: ftp.ciril.fr
 * updates: centos.mirrors.ovh.net
Package openssh-server-6.6.1p1-25.el7_2.x86_64 already installed and latest version
Nothing to do
```

Important - Pour les stations de travail, installez le client : **openssh-clients**.

Options de la commande

Les options de la commande sont :

```
SYNOPSIS
     sshd [-46DdeiqTt] [-b bits] [-C connection_spec] [-f config_file] [-g login_grace_time] [-h host_key_file]
[-k key_gen_time] [-o option] [-p port]  [-u len]
```

Configuration

Important - La configuration doit s'effectuer dans la fenêtre de la VM sous VirtualBox. Les connexions en ssh doivent de faire à partir d'un terminal ou à partir de l'application putty.

Serveur

La configuration du serveur s'effectue dans le fichier **/etc/ssh/sshd_config** :

```
[root@centos7 ~]# cat /etc/ssh/sshd_config
#   $OpenBSD: sshd_config,v 1.93 2014/01/10 05:59:19 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
```

```
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile  .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
```

```
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in Red Hat Enterprise Linux and may cause several
# problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
```

```
#UseLogin no
UsePrivilegeSeparation sandbox      # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem   sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server
```

Pour ôter les lignes de commentaires dans ce fichier, utilisez la commande suivante :

```
[root@centos7 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/ssh/sshd_config > sshd_config
[root@centos7 tmp]# cat sshd_config
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile  .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem   sftp    /usr/libexec/openssh/sftp-server
```

Pour sécuriser le serveur ssh, ajoutez ou modifiez les directives suivantes :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
```

```
X11Forwarding no
```

Votre fichier ressemblera à celui-ci :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile  .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem   sftp    /usr/libexec/openssh/sftp-server
```

A Faire - Renommez le fichier **/etc/ssh/sshd_config** en **/etc/ssh/sshd_config.old** puis copiez le fichier **/tmp/sshd_config** vers **/etc/sshd/**. Redémarrez ensuite le service sshd. N'oubliez pas de mettre l'utilisateur **trainee** dans le groupe **adm** !

Pour générer les clefs sur le serveur saisissez la commande suivante en tant que **root**:

Lors de la génération des clefs, la passphrase doit être **vide**.

```
[root@centos7 ~]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa): /etc/ssh/ssh_host_dsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
d5:54:d3:30:1c:f5:da:f8:21:15:1f:c8:6c:3b:b1:ff root@centos7.fenestros.loc
The key's randomart image is:
+--[ DSA 1024]----+
|            +oBB.|
|           o *.o*|
|          . o +.o|
|         .   +.+ |
|        S    .=..|
|              .o.|
|                o|
|                E|
|                 |
+-----------------+
```

Le chemin à indiquer pour le fichier est **/etc/ssh/ssh_host_dsa_key**. De la même façon, il est possible de générer les clefs au format

RSA, **ECDSA** et **ED25519**.

Les clefs publiques générées possèdent l'extension **.pub**. Les clefs privées n'ont pas d'extension :

```
[root@centos7 ~]# ls /etc/ssh
moduli      sshd_config       ssh_host_dsa_key.pub  ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub
ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_ecdsa_key    ssh_host_ed25519_key    ssh_host_rsa_key
```

Re-démarrez ensuite le service sshd :

```
[root@centos7 ~]# systemctl restart sshd.service
```

Saisissez maintenant les commandes suivantes en tant que **trainee** :

Lors de la génération des clefs, la passphrase doit être **vide**.

```
[trainee@centos7 ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_dsa):
Created directory '/home/trainee/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_dsa.
Your public key has been saved in /home/trainee/.ssh/id_dsa.pub.
The key fingerprint is:
97:92:85:d1:ae:97:f7:64:d2:54:45:89:eb:57:b1:66 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ DSA 1024]----+
```

```
|        ..    ..=|
|         o.  . o.|
|        ...   ..o|
|         o.. ..E.|
|        S.o..oo .|
|        .oo o.+. |
|         . . =.  |
|              .  |
|                 |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_rsa.
Your public key has been saved in /home/trainee/.ssh/id_rsa.pub.
The key fingerprint is:
80:4c:5a:bf:d0:2f:d1:a1:34:7c:09:a1:9c:0d:ed:2d trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ RSA 2048]----+
|    +o=o..       |
|   * Xo+o.       |
|  . B.Bo.        |
|     .E=.        |
|      o.S        |
|       .         |
|                 |
|                 |
|                 |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ecdsa):
```

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ecdsa.
Your public key has been saved in /home/trainee/.ssh/id_ecdsa.pub.
The key fingerprint is:
41:5d:64:cf:d6:4a:ce:8e:a9:a8:4a:62:04:57:09:fc trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ECDSA  256]---+
| .....  .. o+    |
|  ...  .  .. o . |
|. ..    .     = .|
| o  E    .   = . |
|  .     S     +  |
| .           +   |
|  o .       o .  |
| . o     . .     |
|    ..... .      |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ed25519.
Your public key has been saved in /home/trainee/.ssh/id_ed25519.pub.
The key fingerprint is:
66:3a:83:d1:6d:79:46:48:88:7c:d9:65:59:bb:e6:d0 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ED25519  256--+
|   . . +..oo.    |
|    o +..o.  .   |
|     .  . . .    |
|     . . o . .   |
|    . . S + E    |
```

```
|     o = o +     |
|    . +     .    |
|       o         |
|                 |
+-----------------+
```

Les clés générées seront placées dans le répertoire **~/.ssh/**.

Utilisation

La commande ssh prend la forme suivante:

```
ssh -l nom_de_compte numero_ip (nom_de_machine)
```

En saisissant cette commande sur votre propre machine, vous obtiendrez un résultat similaire à celle-ci :

```
[trainee@centos7 ~]$ su -
Mot de passe :
Dernière connexion : lundi  9 mai 2016 à 22:47:48 CEST sur pts/0

[root@centos7 ~]# ssh -l trainee localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
trainee@localhost's password: trainee
Last login: Mon May  9 23:25:15 2016 from localhost.localdomain
```

Tunnels SSH

Le protocole SSH peut être utilisé pour sécuriser les protocoles tels telnet, pop3 etc.. En effet, on peut créer un *tunnel* SSH dans lequel passe les communications du protocole non-sécurisé.

La commande pour créer un tunnel ssh prend la forme suivante :

```
ssh -N -f compte@hôte -Lport-local:localhost:port_distant
```

Dans votre cas, vous allez créer un tunnel dans votre propre vm entre le port 15023 et le port 23 :

```
[root@centos7 ~]# ssh -N -f trainee@localhost -L15023:localhost:23
trainee@localhost's password:
```

Installez maintenant le client et le serveur telnet :

```
[root@centos7 ~]# yum install telnet telnet-server
```

Telnet n'est ni démarré ni activé. Il convient donc de le démarrer et de l'activer :

```
[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

[root@centos7 ~]# systemctl start telnet.socket

[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
```

```
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 3s ago
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.

[root@centos7 ~]# systemctl enable telnet.socket
Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to
/usr/lib/systemd/system/telnet.socket.
[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disabled)
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 36s ago
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.
```

Connectez-vous ensuite via telnet sur le port 15023, vous constaterez que votre connexion n'aboutit pas :

```
[root@centos7 ~]# telnet localhost 15023
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Kernel 3.10.0-327.13.1.el7.x86_64 on an x86_64
centos7 login: trainee
Password:
Last login: Mon May  9 23:26:32 from localhost.localdomain
[trainee@centos7 ~]$
```

Notez bien que votre communication telnet passe par le tunnel SSH.

SCP

Introduction

La commande **scp** est le successeur et la remplaçante de la commande **rcp** de la famille des commandes **remote**. Il permet de faire des transferts sécurisés à partir d'une machine distante :

```
$ scp compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant /chemin_local/fichier_local
```

ou vers une machine distante :

```
$ scp /chemin_local/fichier_local compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant
```

Utilisation

Nous allons maintenant utiliser **scp** pour chercher un fichier sur le «serveur» :

Créez le fichier **/home/trainee/scp_test** :

```
[trainee@centos7 ~]$ pwd
/home/trainee
[trainee@centos7 ~]$ touch scp_test
```

Récupérez le fichier **scp_test** en utilisant scp :

```
[trainee@centos7 ~]$ touch /home/trainee/scp_test
[trainee@centos7 ~]$ scp trainee@127.0.0.1:/home/trainee/scp_test /tmp/scp_test
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
trainee@127.0.0.1's password: trainee
scp_test                                                                                    100%    0
0.0KB/s   00:00
[trainee@centos7 ~]$ ls /tmp/scp_test
/tmp/scp_test
```

Mise en place des clefs

Il convient maintenant de se connecter sur le «serveur» en utilisant ssh et vérifiez la présence du répertoire ~/.ssh :

En saisissant cette commande, vous obtiendrez une fenêtre similaire à celle-ci :

```
[trainee@centos7 ~]$ ssh -l trainee 127.0.0.1
trainee@127.0.0.1's password:
Last login: Mon May  9 23:42:46 2016 from localhost.localdomain
[trainee@centos7 ~]$ ls -la | grep .ssh
drwx------.  2 trainee trainee 4096 May  9 23:25 .ssh
[trainee@centos7 ~]$ exit
logout
Connection to 127.0.0.1 closed.
```

Si le dossier distant .ssh n'existe pas dans le répertoire personnel de l'utilisateur connecté, il faut le créer avec des permissions de 700. Dans votre cas, puisque votre machine joue le rôle de serveur **et** du client, le dossier /home/trainee/.ssh existe **déjà**.

Ensuite, il convient de transférer le fichier local **.ssh/id_ecdsa.pub** du «client» vers le «serveur» en le renommant en **authorized_keys** :

```
[trainee@centos7 ~]$ scp .ssh/id_ecdsa.pub trainee@127.0.0.1:/home/trainee/.ssh/authorized_keys
trainee@127.0.0.1's password: trainee
id_ecdsa.pub                                                                                  100%  227
0.2KB/s   00:00
```

Connectez-vous via telnet et insérer les clefs publiques restantes dans le fichier .ssh/authorized_keys :

```
root@centos7 ~]# ssh -l trainee localhost
trainee@localhost's password: trainee
Last login: Tue May 10 01:39:33 2016 from localhost.localdomain
[trainee@centos7 ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_dsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_ed25519.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/authorized_keys
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5BtOMFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dlUXgaPyEJXuwHO0pxcdbr
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC9KOuEH5+kyihhm99Na8UTA4Gi5AfiOVeJyS3UzH7ta73ewmv7JZqaXzar1NlHcpEMkCUs2yKxHyO/yAfjb
CSdow5vfwJiuJTes+HbpvsJqKp1+OR7tf+OMgjDcajoGi7DYuybIs9QrbWgh57QclbldHQXRO+xbeUTykxcRun7AvR5uWZe4zMooBAmVVEms+l1rn
8CUi+D811jqQGSpU39PxkojTAwgbxlevT/Twy4sfeRR47UHc3AbrHb8SgyKqbx5/S9UxkbkhJjckx0s58fnAwf9nX5rKE7RdCQisRvdLeLHozq3EO
omvc7kzejefBtUDWxBEjnSeAgIP3+OEQl trainee@centos7.fenestros.loc
ssh-dss
AAAAB3NzaC1kc3MAAACBAK9/4siucBnf/NAHBMjZWIx1coA/wYVBjfudVyKArip1fVUuYqf0Ri9vTorG8KJ2zzLRbW5z7V5ZDSn4f6P5Kv7K5xVPn
e9dYQHxImkZIljpFseUW56BwCvcgTNZVLD0tYZzF+B0/Py4waJW+pnTDfZush6DYyAhVnEuxIPI4i+PAAAAFQCeCZyDRo1o41lf19qWGJTG7W+ChQ
AAAIAKtQe9QlkW4CA9kP+q4v3N07WR5TzWsvfZARjGXgrSqTo0BeQgMLwRJHeEOhdsgJ30cNbl6QXlB4G4J6dUoTiN/sY1dFbXzjzsT/MHLedsllV
fXXRQxgvN2nsbsKEUnmqEBWzgw5s6KOkGX33+0Six0E3xvOrYxkMNLP/5VT4aQwAAAIEAmOS94peBeo78yCKzCvSFnEL72dUCFFA6CGFGqgffhK1v
P5H5pG5vQxzBn9NnIXURCACF7ZxtZaxohSoB1M0/s0DfrfNIvXRMGvsJpZ9B2psTMDl9qBffIfIARnwkWKG1gC/lWaovUpDByE1wl09ZCDCnZp/16
ULJY0zvJ566Seg= trainee@centos7.fenestros.loc
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIENas3A3hmXFj1cb+lrn2NAt6g95Pla6qUFQHd1wg2y1 trainee@centos7.fenestros.loc
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5BtOMFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dlUXgaPyEJXuwHO0pxcdbr
```

```
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
```

Lors de la connexion suivante au serveur, l'authentification utilise le couple de clefs asymétrique et aucun mot de passe n'est requis :

```
[trainee@centos7 ~]$ ssh -l trainee localhost
Last login: Tue May 10 01:50:39 2016 from localhost.localdomain
[trainee@centos7 ~]$ exit
déconnexion
Connection to localhost closed.
```

Le fichier **authorized_keys** doit avoir les permissions de 600.
