Infrastructure technologique et virtualisation

Module 5 : Accès distant

Source sur SSH : https://linuxhandbook.com/ssh-basics

Comment accéder à distance un serveur

- **Telnet** : terminal network(Port TCP 23) **à proscrire**.
  - Échange des lignes de textes et reçois également sous forme de texte. S'utilise en mode console (terminal).
  - Était notamment utilisé pour administrer des serveurs UNIX distants ou de l'équipement réseau, avant de tomber en désuétude par défaut de sécurisation (le texte étant échangé en clair) et l'adoption de **SSH**.
- **SSH** : secure shell (Port TCP 22)
  - Un programme informatique et un protocole de communication sécurisé.
  - L'authentification peut se faire sans l'utilisation de mot de passe ou de phrase secrète en utilisant la cryptographie asymétrique.
- **FTP** : File Transfert Protocol (Port TCP 20 donnés , TCP 21 écoute et gestion)
  Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.
- Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.
- **Autres** (VNC, Remote Desktop, etc.) ne font pas partie des services utilisés dans le cours.

SSH

Votre serveur peut se trouver n'importe où dans le monde et vous pouvez vous y connecter à partir de votre machine locale.

ssh est le moyen le plus populaire de se connecter de manière sécurisée à des systèmes distants.

Il stocke **une clé publique dans le système distant** et **une clé privée dans le système client**. Ces clés sont produites sous la forme d'une paire mathématique. Lorsque les deux sont appliquées à une fonction bivariable, il en résulte une valeur qui sera utilisée pour vérifier si la paire est valide ou non

Générer les clés SSH : ssh-keygen

Le programme vous demandera un emplacement de clé (où la clé sera enregistrée) et une phrase de passe (c'est-à-dire un mot de passe). La phrase de passe est facultative.

Par défaut, les clés ssh sont stockées dans le répertoire .ssh sous votre répertoire personnel.

Le fichier de la clé privée que vous ne devez partager avec personne **DIR_PATH/keypairforssh**

Le fichier de clé publique **DIR_PATH/keypairforssh.pub**
Ce fichier peut être partagé avec des systèmes distants (par le biais d'autres moyens de communication fiables tels que le courrier, le transfert physique et d'autres outils de communication sécurisés)

Connexion distante avec SSH

ssh [nom d'utilisateur]@hostname

- Où le nom d'utilisateur doit être un utilisateur valide sur le système distant
- Le nom d'hôte est reconnaissable par DNS ou une adresse IP afin que ssh puisse contacter le système distant et demander une connexion.

Elle autorise la connexion si et seulement si la paire de clés est valide et génère un Shell (le type dépend de la configuration de l'utilisateur sur le système distant) pour votre utilisation.

Copie de fichiers entre un client et un système distant

La commande scp est un outil construit sur le dessus de ssh. Elle permet aux utilisateurs de copier des fichiers et des répertoires d'un système distant vers un système client et vice versa.

```
scp ~/Documents/documentForLinux.txt jpduches@10.100.2.450:~/Documents
```

Pour copier le même fichier en sens inverse :

```
scp jpduches@10.100.2.450:~/Documents/documentForLinux.txt  ~/Documents
```

Montage d'un système de fichiers ou d'un répertoire distant

Pour monter les répertoires du système distant sur le client, sshfs est l'outil développé dans ce but précis.

```
sshfs name@server:/path/to/remote/folder /path/to/local/mount/point
```

Dans certains systèmes, sshfs peut ne pas être disponible, installez-le si vous en avez besoin.

Quitter SSH

Si vous êtes connecté à un système Linux distant via SSH, il vous suffit d'utiliser la commande exit pour vous déconnecter de SSH.

Fichier de configuration des machines

```
jpduches@VM-DevOpsJPD:~$ cat .ssh/config
Host srvdev
        Hostname 10.100.2.50
        User jpduches
        Port 22

Host srvmysql
        Hostname 10.100.1.107
        User jpduches
        Port  22
jpduches@VM-DevOpsJPD:~$
```

Utilisation d’un fichier de configuration

```
jpduches@VM-DevOpsJPD:~$ ssh srvmysql
jpduches@10.100.1.107's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jun  1 14:18:57 UTC 2021

  System load:    0.63             Processes:               232
  Usage of /home: 0.4% of 9.78GB   Users logged in:         1
  Memory usage:   10%              IPv4 address for ens160: 10.100.1.107
  Swap usage:     0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue Jun  1 14:16:39 2021 from 10.100.2.136
```

Exemple de clé non reconnu :

```
jpduches@VM-DevOpsJPD:~/.ssh$ cat config
Host srvdev
        Hostname 10.100.2.50
        User jpduches
        Port 22
jpduches@VM-DevOpsJPD:~/.ssh$ ssh srvdev
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:53yBWGlQU6CwNuAzc8iHfiX2NameYSz3LNaKFiGrlgo.
Please contact your system administrator.
Add correct host key in /home/jpduches/.ssh/known_hosts to get rid of this messa
ge.
Offending ECDSA key in /home/jpduches/.ssh/known_hosts:2
  remove with:
  ssh-keygen -f "/home/jpduches/.ssh/known_hosts" -R "10.100.2.50"
ECDSA host key for 10.100.2.50 has changed and you have requested strict checkin
g.
Host key verification failed.
jpduches@VM-DevOpsJPD:~/.ssh$ ssh-keygen -f "/home/jpduches/.ssh/known_hosts" -R
  "10.100.2.50"
# Host 10.100.2.50 found: line 2
/home/jpduches/.ssh/known_hosts updated.
Original contents retained as /home/jpduches/.ssh/known_hosts.old
```

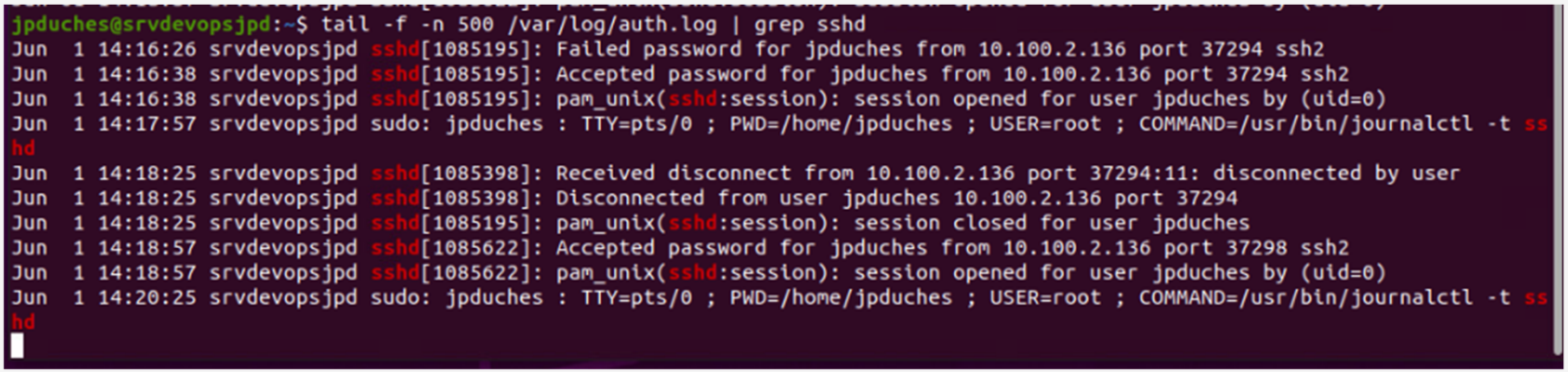
Commande utiles :

$sudo journalctl –t sshd

```
jpduches@srvdevopsjpd:~$ sudo journalctl -t sshd
[sudo] password for jpduches:
-- Logs begin at Sat 2021-05-15 22:23:10 UTC, end at Tue 2021-06-01 14:20:25 UTC. --
May 15 22:23:16 srvdevopsjpd sshd[1259]: Server listening on 0.0.0.0 port 22.
May 15 22:23:16 srvdevopsjpd sshd[1259]: Server listening on :: port 22.
May 15 22:23:21 srvdevopsjpd sshd[1259]: Received signal 15; terminating.
May 15 22:23:21 srvdevopsjpd sshd[1765]: Server listening on 0.0.0.0 port 22.
May 15 22:23:21 srvdevopsjpd sshd[1765]: Server listening on :: port 22.
May 19 20:33:54 srvdevopsjpd sshd[53987]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=>
May 19 20:33:56 srvdevopsjpd sshd[53987]: Failed password for jpduches from 10.100.1.138 port 59872 ssh2
May 19 20:34:38 srvdevopsjpd sshd[53987]: Accepted password for jpduches from 10.100.1.138 port 59872 ssh2
May 19 20:34:38 srvdevopsjpd sshd[53987]: pam_unix(sshd:session): session opened for user jpduches by (uid=0)
May 19 20:37:20 srvdevopsjpd sshd[54308]: Received disconnect from 10.100.1.138 port 59872:11: disconnected by user
May 19 20:37:20 srvdevopsjpd sshd[54308]: Disconnected from user jpduches 10.100.1.138 port 59872
May 19 20:37:20 srvdevopsjpd sshd[53987]: pam_unix(sshd:session): session closed for user jpduches
May 19 20:38:16 srvdevopsjpd sshd[54652]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=>
May 19 20:38:18 srvdevopsjpd sshd[54652]: Failed password for tamima from 10.100.1.138 port 59878 ssh2
May 19 20:38:25 srvdevopsjpd sshd[54652]: Accepted password for tamima from 10.100.1.138 port 59878 ssh2
May 19 20:38:25 srvdevopsjpd sshd[54652]: pam_unix(sshd:session): session opened for user tamima by (uid=0)
May 20 15:31:50 srvdevopsjpd sshd[54768]: Received disconnect from 10.100.1.138 port 59878:11: disconnected by user
May 20 15:31:50 srvdevopsjpd sshd[54768]: Disconnected from user tamima 10.100.1.138 port 59878
May 20 15:31:50 srvdevopsjpd sshd[54652]: pam_unix(sshd:session): session closed for user tamima
Jun 01 14:16:26 srvdevopsjpd sshd[1085195]: Failed password for jpduches from 10.100.2.136 port 37294 ssh2
Jun 01 14:16:38 srvdevopsjpd sshd[1085195]: Accepted password for jpduches from 10.100.2.136 port 37294 ssh2
Jun 01 14:16:38 srvdevopsjpd sshd[1085195]: pam_unix(sshd:session): session opened for user jpduches by (uid=0)
Jun 01 14:18:25 srvdevopsjpd sshd[1085398]: Received disconnect from 10.100.2.136 port 37294:11: disconnected by user
Jun 01 14:18:25 srvdevopsjpd sshd[1085398]: Disconnected from user jpduches 10.100.2.136 port 37294
Jun 01 14:18:25 srvdevopsjpd sshd[1085195]: pam_unix(sshd:session): session closed for user jpduches
Jun 01 14:18:57 srvdevopsjpd sshd[1085622]: Accepted password for jpduches from 10.100.2.136 port 37298 ssh2
Jun 01 14:18:57 srvdevopsjpd sshd[1085622]: pam_unix(sshd:session): session opened for user jpduches by (uid=0)
lines 1-28/28 (END)
```

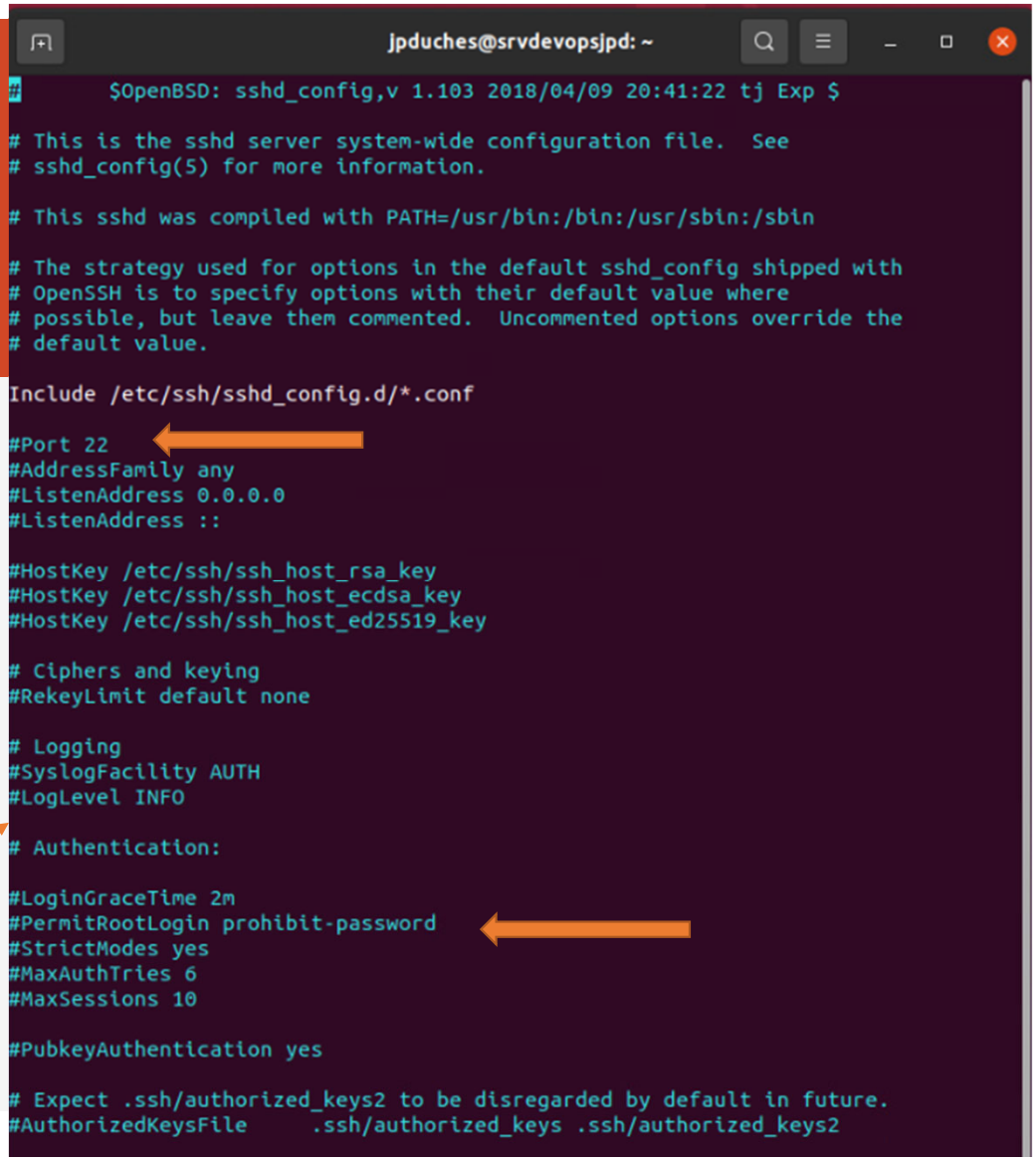
Commande utiles :

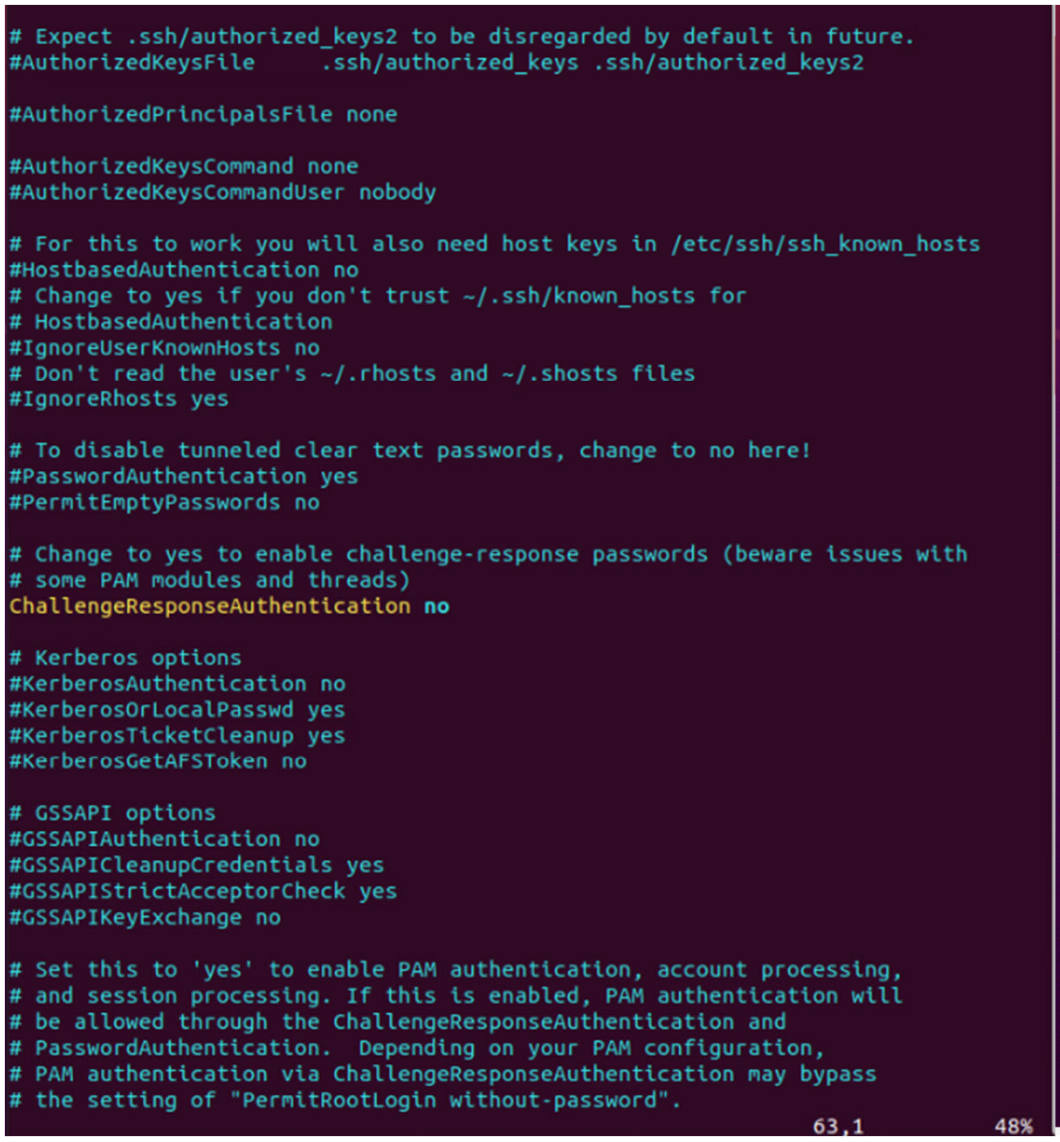
$tail –f –n 500 /var/log/auth.log | grep sshd



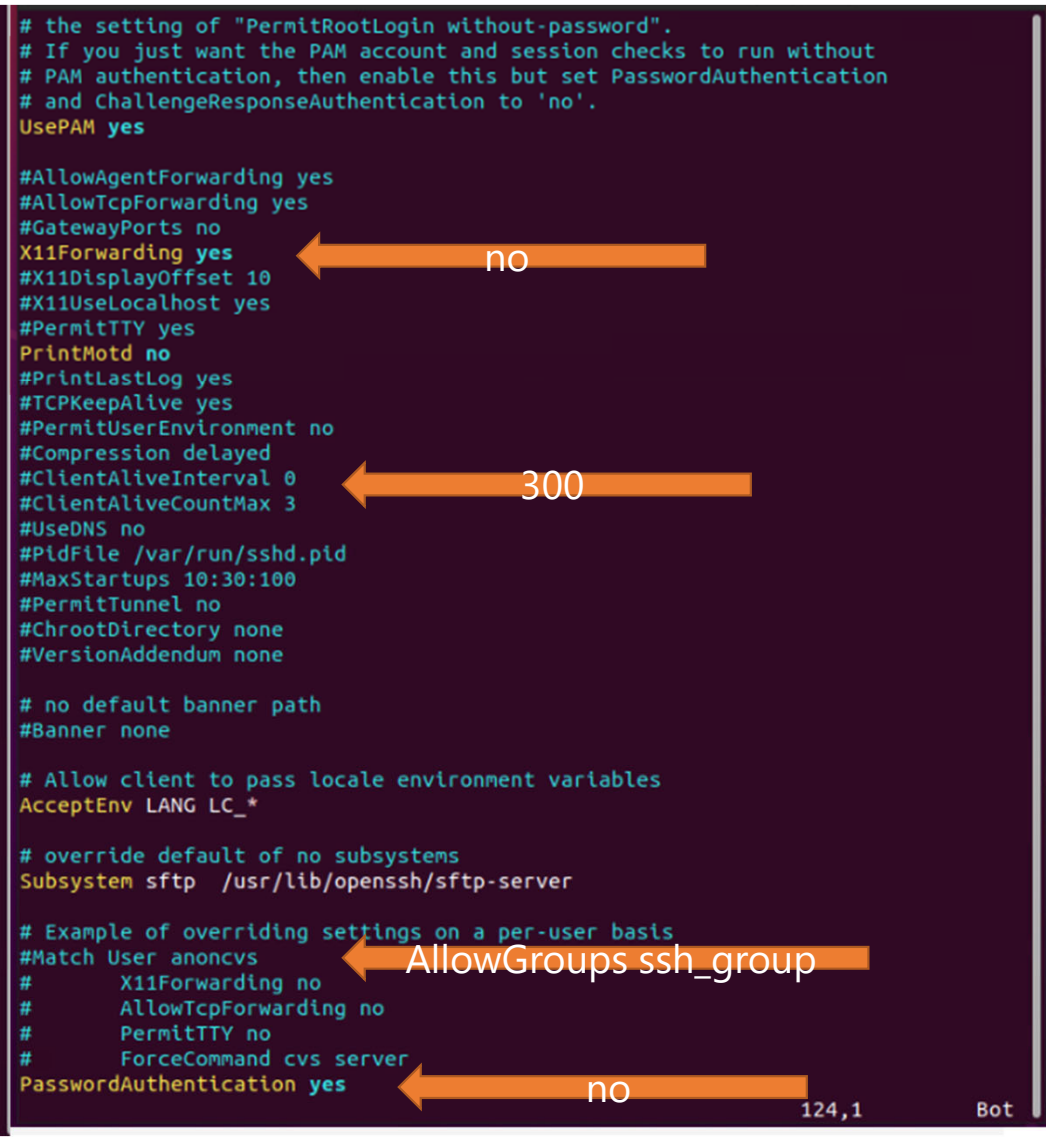
Modification de la configuration sshd

```
jpduches@srvdevops2jpd:/etc/ssh$ ls -al
total 588
drwxr-xr-x   4 root root   4096 Jun  1 13:12 .
drwxr-xr-x 102 root root   4096 May 28 17:26 ..
-rw-r--r--   1 root root 535195 May 29  2020 moduli
-rw-r--r--   1 root root   1603 May 29  2020 ssh_config
drwxr-xr-x   2 root root   4096 May 29  2020 ssh_config.d
-rw-------   1 root root   1381 May 16 20:33 ssh_host_dsa_key
-rw-r--r--   1 root root    608 May 16 20:33 ssh_host_dsa_key.pub
-rw-------   1 root root    513 May 16 20:33 ssh_host_ecdsa_key
-rw-r--r--   1 root root    180 May 16 20:33 ssh_host_ecdsa_key.pub
-rw-------   1 root root    411 May 16 20:33 ssh_host_ed25519_key
-rw-r--r--   1 root root    100 May 16 20:33 ssh_host_ed25519_key.pub
-rw-------   1 root root   2602 May 16 20:33 ssh_host_rsa_key
-rw-r--r--   1 root root    572 May 16 20:33 ssh_host_rsa_key.pub
-rw-r--r--   1 root root    342 May 16 20:25 ssh_import_id
-rw-r--r--   1 root root   3316 May 16 20:34 sshd_config
drwxr-xr-x   2 root root   4096 May 29  2020 sshd_config.d
-rw-r--r--   1 root root   3316 Jun  1 13:12 sshd_configOld
jpduches@srvdevops2jpd:/etc/ssh$ _
```





Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile	.ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
Change to yes if you don't trust ~/.ssh/known_hosts for
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
Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
ChallengeResponseAuthentication no
Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange 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".
63,1 48%



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'.
UsePAM yes
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
300
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
no default banner path
#Banner none
Allow client to pass locale environment variables
AcceptEnv LANG LC_*
override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server
Example of overriding settings on a per-user basis
#Match User anoncvs
AllowGroups ssh_group
#	X11Forwarding no
#	AllowTcpForwarding no
#	PermitTTY no
#	ForceCommand cvs server
PasswordAuthentication yes
no
124,1 Bot