SSH a Debian12 szerveren

http://ubuntuhandbook.org/index.php/2016/04/enable-ssh-ubuntu-16-04-lts/
https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/

Secure Shell (SSH) egy kriptográfiai hálózati protokoll, amelyet az ügyfél és a szerver közötti biztonságos kapcsolathoz használnak.

Nézzük meg, hogy lehet engedélyezni a Secure Shell (SSH) szolgáltatást a Debian szerven a biztonságos távoli bejelentkezés és az egyéb hálózati kommunikáció engedélyezéséhez.

Szükség lesz egy SSH szolgáltatásra, melyet az **OpenSSH** (**OpenBSD Secure Shell**) biztosítja, amely egy biztonsághoz kapcsolódó hálózati szintű segédprogram és az SSH protokollon alapul.

általános parancs leírás:
ssh *felhasználónév_a_szerveren@szerverIPcíme(vagyDomainNeve)*

Lépjen be a kliens Terminál felületére és tesztelje, hogy mi történik akkor, ha még nincs telepítve ssh szolgáltatás és megpróbáljuk elérni a szervert:

ssh

```
tanulo@ubuntu:~$ ssh
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] [user@]hostname [command]
tanulo@ubuntu:~$
```

ssh tanulo@192.168.0.1

```
ssh: connect to host 192.168.0.1 port 22: Connection refused
```

I. SSH telepítése a szerveren

A szerveren végezze el a következőket:

1. A telepítéshez futtassa a következő parancssorokat:

```
sudo apt-get update
sudo apt-get install openssh-server
```

2. Ezt követően engedélyeznie kell az SSH szolgáltatást a rendszerében, ellenőrizheti annak állapotát a következő paranccsal:

```
sudo service ssh status
```

```
tanulo@debian:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-01-11 14:06:14 CET; 8s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1446 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1447 (sshd)
      Tasks: 1 (limit: 1131)
     Memory: 1.0M
        CPU: 16ms
     CGroup: /system.slice/ssh.service
             └─1447 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

jan 11 14:06:14 debian systemd[1]: Starting OpenBSD Secure Shell server...
jan 11 14:06:14 debian sshd[1447]: Server listening on 0.0.0.0 port 22.
jan 11 14:06:14 debian sshd[1447]: Server listening on :: port 22.
jan 11 14:06:14 debian systemd[1]: Started OpenBSD Secure Shell server.
tanulo@debian:~$ _
```

Ha még sincs engedélyezve, akkor adja ki a következő parancssort:

```
sudo systemctl enable ssh
sudo systemctl start ssh
```

Kliens teszt:

Nézzük meg, most mit kaptunk a szerver ssh-n keresztüli elérése esetén:

ssh tanulo@192.168.0.1

```
tanulo@tanulo:~$ ssh tanulo@192.168.0.1
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
ECDSA key fingerprint is SHA256:eNMGmpelOpesLEAKOYqYs3zQ24KRyuGaROI9X3iVGRM.
Are you sure you want to continue connecting (yes/no)? 
```

Ekkor „yes” majd a jelszó megadása után a következőt kapjuk:

```
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.0.1' (ECDSA) to the list of known hosts.
tanulo@192.168.0.1's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic i686)

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

0 csomag frissíthető.
0 frissítés biztonsági frissítés.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Feb  8 17:28:38 2021
tanulo@SERVER:~$ 
```

A promptból látható, hogy sikeresen elértük a szervert. Azonban még nincs minden beállítva, ezért még lépjünk ki az SSH kapcsolatból:

```
logout
```

```
tanulo@SERVER:~$ logout
Connection to 192.168.0.1 closed.
tanulo@tanulo:~$ 
```

FIGYELEM! Néha előfordulhat az ssh tanulo@192.168.0.1 kiadása során az alábbi eset:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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:OPdi/GFalRmLuN9WGIjB3TYdaRwQGPlmhrUd++mpMwk.
Please contact your system administrator.
Add correct host key in /home/tanulo/.ssh/known_hosts to get rid of this messag
e.
Offending ECDSA key in /home/tanulo/.ssh/known_hosts:1
  remove with:
  ssh-keygen -f "/home/tanulo/.ssh/known_hosts" -R "192.168.0.1"
ECDSA host key for 192.168.0.1 has changed and you have requested strict checki
ng.
Host key verification failed.
tanulo@tanulo-VirtualBox:~$
```

Ekkor adja ki a következő parancssort:

```
tanulo@tanulo-VirtualBox:~$ ssh-keygen -f "/home/tanulo/.ssh/known_hosts" -R "1
92.168.0.1"
# Host 192.168.0.1 found: line 1
/home/tanulo/.ssh/known_hosts updated.
Original contents retained as /home/tanulo/.ssh/known_hosts.old
```

II. SSH kulcspár (public/private) létrehozása és elhelyezése

Figyelem! A elérési utakban pirossal szereplő részek átalános megadások, azaz oda kell mindig behelyettesíteni az aktuális értéket!

1. A kliens Terminálban adja ki a következő parancsot:
   `ssh-keygen`

- Elérési út és kulcsnév megadása:
  /home/*felhasznalonev*/.ssh/*kulcsNev*

- Jelszó nem kötelező

Az alábbi esetben mindenhol az alapértelmezettet állítjuk be, azaz mindenhova ENTER nyomunk és nem írunk be semmit!

```
tanulo@tanulo:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/tanulo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tanulo/.ssh/id_rsa.
Your public key has been saved in /home/tanulo/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:vOc0VEkkY3R05QaSSEvOE2xrNZUShrmy09YPWV/6JBo tanulo@tanulo
The key's randomart image is:
+---[RSA 2048]----+
|         +O*O++o.|
|         =*O=+.o |
|         .=+oo  o|
|       .. +o  ...|
|        S=.. o o.|
|        ooo E o o|
|        .o+  = + |
|         + .. . .|
|          .      |
+----[SHA256]-----+
tanulo@tanulo:~$
```

- Létrejön:
  privát kulcs: **/home/*felhasznalonev*/.ssh/*kulcsNev***
  publikus kulcs: **/home/*felhasznalonev*/.ssh/*kulcsNev*.pub**

FIGYELEM! A .ssh mappa rejtett, ha az alábbi ls -l parancsok nem jelenítik meg, akkor használja az ls -la parancsot!

Ez a két sor a fenti nagyobb szövegben látható:

```
Your identification has been saved in /home/tanulo/.ssh/id_rsa
Your public key has been saved in /home/tanulo/.ssh/id_rsa.pub
```

- Ellenőrizzük le, hogy tényleg léteznek ezek az állományok!

```
tanulo@tanulo-VirtualBox:~$ ls -l /home/tanulo/.ssh/id_rsa
-rw------- 1 tanulo tanulo 1671 márc   4 08:27 /home/tanulo/.ssh/id_rsa
tanulo@tanulo-VirtualBox:~$ ls -l /home/tanulo/.ssh/id_rsa.pub
-rw-r--r-- 1 tanulo tanulo 406 márc   4 08:27 /home/tanulo/.ssh/id_rsa.pub
tanulo@tanulo-VirtualBox:~$
```

2. A szerveren a következő parancsokat adja ki:

mkdir /home/*felhasznalonev*/.ssh
touch /home/*felhasznalonev*/.ssh/authorized_keys

```
tanulo@ubuntu:~$ mkdir /home/tanulo/.ssh
tanulo@ubuntu:~$ touch /home/tanulo/.ssh/authorized_keys
```

- Majd ellenőrizze le:

```
tanulo@server:~$ ls -l /home/tanulo/.ssh
total 4
-rw------- 1 tanulo tanulo 406 márc   4 08:56 authorized_keys
```

3. A publikus kulcsot átmásoljuk a kliensről a szerverre:

ssh-copy-id -i /home/*felhasznalonev*/.ssh/*kulcsNev*.pub felhasznalo_a_szerveren@szerver_nev(vagyIPcím)

```
tanulo@tanulo-VirtualBox:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub tanulo@192.168.0.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/tanulo/.ss
h/id_rsa.pub"
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
ECDSA key fingerprint is SHA256:OPdi/GFalRmLuN9WGIjB3TYdaRwQGPlmhrUd++mpMwk.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are promp
ted now it is to install the new keys
tanulo@192.168.0.1's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'tanulo@192.168.0.1'"
and check to make sure that only the key(s) you wanted were added.

tanulo@tanulo-VirtualBox:~$
```

Ekkor a "**~/.ssh/id_rsa.pub**" tartalma átmásolódik a authorized_keys állományba. (Minden kulcs 1 sor.)

- Nézzük meg, hogy megtörtént-e:
  `cat ~/.ssh/authorized_keys`

```
tanulo@ubuntu:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCusEWDVFtlzI7lwa7hj19+TODed8Kelgrsnltqtb1JBXazWooY+sF5iJHiN3Qs
VPEWO/4Vtpd1OHIJyBrEKOdPn6aNoPcd4HV4s/ECIJGQWgiEjj6TuejIPys+/VR7RLrm/tNFSqGOoKwbVNJgg/FDZxgRmPZjJu1q
GEFMUKwOViZyg7B4FKEO7q9aQnimdNosGZOv5bvJiiEfrpze149/+OspGhyamoBIe/5YzpucZKd1Oy2BN8ISjSCiKMTT3uMbWwPB
hnNFXaVywqel54rhTu3S8BZDt+zgzQCAOSMyzjMfBRMbblCd9kXbAkigYLYJDzLOfYePgJLKth5DP6Td tanulo@tanulo-Virtu
alBox
tanulo@ubuntu:~$
```

4. Végezzük még el az alábbi műveleteket a szerveren:

chown *felhasznalonev*:*felhasznalonev* /home/*felhasznalonev*/.ssh
chown *felhasznalonev*:*felhasznalonev* /home/*felhasznalonev*/.ssh/authorized_keys

```
tanulo@ubuntu:~$ chown tanulo:tanulo /home/tanulo/.ssh
tanulo@ubuntu:~$ chown tanulo:tanulo /home/tanulo/.ssh/authorized_keys
tanulo@ubuntu:~$ _
```

chmod 700 /home/*felhasznalonev*/.ssh
chmod 644 /home/*felhasznalonev*/.ssh/authorized_keys

```
tanulo@ubuntu:~$ chmod 700 /home/tanulo/.ssh
tanulo@ubuntu:~$ chmod 644 /home/tanulo/.ssh/authorized_keys
tanulo@ubuntu:~$
```

sudo nano /etc/ssh/sshd_config

Keressük meg az alábbi sort:
#PasswordAuthentication yes

Majd cseréljük le erre:
PasswordAuthentication no

```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no
```

Ha szeretnénk megváltoztatni az SSH 22—es portját megváltoztatni, akkor ugyan ebben a fájlban, keressünk rá az alábbi sorra:

```
#Port 22
```

Majd írjuk át és aktíváljuk:

```
Port 2222
```

III. A szerver SSH-n keresztül való elérése

1. Nézzük meg, hogy a kliensen keresztül elérjük-e a szervert:
   ssh *felhasznalonev*@*szerverIP* -i ~/.ssh/*kulcsNev*

```
tanulo@tanulo-VirtualBox:~$ ssh tanulo@192.168.0.1 -i ~/.ssh/id_rsa.pub
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic i686)

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

0 csomag frissíthető.
0 frissítés biztonsági frissítés.


Last login: Wed Mar 11 07:04:34 2020 from 192.168.0.2
tanulo@ubuntu:~$
```

Sikerült! Figyeljük meg, hogy a prompt megváltozott a szerver promptjára. Innentől kezdve a szerver erőforrásait és fájljait tudjuk használni.

1. Jelenítsük meg a szerver hálózati kártyáit és beállításait!

   ip a

```
tanulo@ubuntu:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:9d:b6:af
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9d:b6af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:334 errors:0 dropped:0 overruns:0 frame:0
          TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50744 (50.7 KB)  TX bytes:43362 (43.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:34578 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34578 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:2558996 (2.5 MB)  TX bytes:2558996 (2.5 MB)

tanulo@ubuntu:~$
```

2. Hozzunk létre egy „vegyes.txt” fájlt az aktuális felhasználó home könyvtárába!

```
tanulo@ubuntu:~$ touch ~/vegyes.txt
tanulo@ubuntu:~$ ls -l ~
total 0
-rw-rw-r-- 1 tanulo tanulo 0 márc  10 11:57 vegyes.txt
tanulo@ubuntu:~$
```

3. Majd lépjünk át a szerverre és ellenőrizzük le, hogy ott van-e a „vegyes.txt” fájl!

```
tanulo@ubuntu:~$ ls -l ~/
total 0
-rw-rw-r-- 1 tanulo tanulo 0 márc  10 11:57 vegyes.txt
tanulo@ubuntu:~$
```

IV. Kilépés az SSH kapcsolatból

Menjünk vissza kliensre és lépjünk ki az SSH kapcsolatból:

`logout`

```
tanulo@ubuntu:~$ logout
Connection to 192.168.0.1 closed.
tanulo@tanulo-VirtualBox:~$
```