abilito il login da root sulla vm da console

```
sed -i s/without-password/yes/g /etc/ssh/sshd_config && systemctl restart ssh
```

Installo il software

Per installare i servizi necessari lanciare il comando

```
apt-get install openvpn autossh -y
```

OPENVPN:

Presupponendo presente sulla vm la cartella Vpn con all'interno le configurazioni openvpn, passo a copiare i file per l'avvio:

```
cp -rv /root/Vpn/openvpn/apv/* /etc/openvpn
cp /root/Vpn/openvpn/apv/client.ovpn /etc/openvpn/apv.conf
systemctl daemon-reload
```

vim /etc/systemd/system/openvpn@apv.service

```
[Unit]
Description=OpenVPN connection to %i
PartOf=openvpn.service
ReloadPropagatedFrom=openvpn.service

[Service]
Type=forking
ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openvpn/%i.status 10 --cd /etc/openvpn
--config /etc/openvpn/%i.conf
ExecReload=/bin/kill -HUP $MAINPID
WorkingDirectory=/etc/openvpn

[Install]
WantedBy=multi-user.target
```

Abilito il servizio all'avvio:

```
systemctl enable openvpn@apv.service
```

AUTOSSH:

aggiungo l'utente:

```
useradd -m -s /bin/false autossh
```

*** creo il file config di ssh (esempio preso da apv):** *

```
Host autportven-prod
HostName 10.0.20.30
Port 22
User extraway
Localforward 8080 localhost:8080
Localforward 5432 localhost:5432
Localforward 19080 10.0.20.31:8080
Localforward 13306 10.0.20.31:3306
```

creo le chiavi:

```
su -s /bin/bash autossh
ssh-keygen -t rsa
```

copio le chiavi sul server prod del cliente:

scp id_rsa.pub extraway@10.0.20.30:/tmp

aggiungo in coda la chiave fra quelle autorizzate:

cat /tmp/id_rsa.pub » /home/extraway/.ssh/authorized_keys

cancello la chiave copiata:

rm -f /tmp/id_rsa.pub

configuro il mapping delle porte ssh:

su -s /bin/bash autossh vim .ssh/config

```
Host autportven-prod
HostName 10.0.20.30
Port 22
User extraway
Localforward 8080 localhost:8080
Localforward 5432 localhost:5432
Localforward 19080 10.0.20.31:8080
Localforward 13306 10.0.20.31:3306
```

controllo che il collegamento funzioni e mappi le porte regolarmente:

```
su -s /bin/bash autossh
ssh -g extraway@autportven-prod
```

```
root@VPN-APV:~# netstat -an |egrep '8080|5432|19080|13306'|egrep -v tcp6
tcp        0      0 0.0.0.0:9080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
```

creo il file di avvio di autossh in systemd:

root@VPN-APV:/etc/systemd/system# vim /etc/systemd/system/3dautossh.service (root deve avere la sua chiave presso il cliente)

```
[Unit]
Description=AutoSSH service
Wants=sys-devices-virtual-net-tun0.device
After=sys-devices-virtual-net-tun0.device

[Service]
ExecStart=/usr/bin/autossh -M 0 -v -q -N -o "ServerAliveInterval 60" -o "ServerAliveCountMax 3"
extraway@autportven-prod -i /home/autossh/.ssh/id_rsa -g -F /home/autossh/.ssh/config

[Install]
WantedBy=multi-user.target
```

Questo il significato delle opzioni scelte per lo start di autossh:

-M port[echo:port]

specifies the base monitoring port to use. Without the echo port, this port and the port immediately above it (port + 1) should be something nothing else is using. autossh will send test data on the base monitoring port, and receive it back on the port above. For example, if you specify “-M 20000”, autossh will set up forwards so that it can send data on port 20000 and receive it back on 20001. Setting the monitor port to 0 turns the monitoring function off, and autossh will only restart ssh upon ssh's exit. **In pratica è più consono disabilitare la funzione e usare altri strumenti come ServerAliveInterval e ServerAliveCountMax per controllare se il tunnel è up.**

-v [verbose]

Causes ssh to print debugging messages about its progress. This is helpful in debugging connection, authentication, and configuration problems.Multiple -v options increase the verbosity.The maximum is 3. **Ho scoperto che in mancanza di questa opzione il tunnel si avviava solo da cli e non da systemd.**

-q [quiet]

Causes most warning and diagnostic messages to be suppressed. **Consigliato nel readme e inserito nonostante la precedente opzione -v sia inserita.**

-o [ServerAliveInterval] -o [ServerAliveCountMax]

Opzioni consigliate nel readme che permettono il restart del tunnel nel caso in cui la connessione ssh non sia funzionante controllando il **TTL** con **ServerAliveInterval 60** (dove 60 sono secondi) e dopo 3 tentativi nel caso in cui **ServerAliveCountMax** sia impostato a **3**.

-i [identity file]

Selects a file from which the identity (private key) for public key authentication is read. The default is ~/.ssh/identity for protocol version 1, and ~/.ssh/id_dsa, ~/.ssh/id_ecdsa, ~/.ssh/id_ed25519 and ~/.ssh/id_rsa for protocol version 2. Identity files may also be specified on a per-host basis in the configuration file. It is possible to have multiple -i options (and multiple identities specified in configuration files). **In mancanza di questa opzione autossh avviato da systemd non riesce a collegarsi**.

-g [global]

Allows remote hosts to connect to local forwarded ports. If used on a multiplexed connection, then this option must be specified on the master process. **In mancanza di queste opzioni tutte le porte forwardate sono bindate solo su localhost.**

-N [no execute]

Do not execute a remote command. This is useful for just forwarding ports (protocol version 2 only).

-F [configfile]

Specifies an alternative per-user configuration file. If a configuration file is given on the command line, the system-wide configuration file (/etc/ssh/ssh_config) will be ignored. The default for the per-user con figuration file is ~/.ssh/config. **In pratica nel comando systemd è stato necessario affinché autossh prendesse le porte mappate dal file corretto.**

testo lo script prima di abilitarlo:

```
root@VPN-APV:/etc/openvpn# systemctl start 3dautossh.service
root@VPN-APV:/etc/openvpn# systemctl status 3dautossh.service -l
● 3dautossh.service - AutoSSH service
   Loaded: loaded (/etc/systemd/system/3dautossh.service; enabled)
   Active: active (running) since gio 2016-03-31 15:25:50 CEST; 12s ago
 Main PID: 778 (autossh)
   CGroup: /system.slice/3dautossh.service
           ├─778 /usr/lib/autossh/autossh -M 8080 -q -N -o ServerAliveInterval 60 -o
ServerAliveCountMax 3 extraway@autportven-prod -i /home/autossh/.ssh/id_rsa -g
           └─781 /usr/bin/ssh -L 8080:127.0.0.1:8080 -R 8080:127.0.0.1:8081 -q -N -o
ServerAliveInterval 60 -o ServerAliveCountMax 3 -i /home/autossh/.ssh/id_rsa -g
extraway@autportven-prod

mar 31 15:25:50 VPN-APV autossh[778]: starting ssh (count 1)
mar 31 15:25:50 VPN-APV autossh[778]: ssh child pid is 781
```

controllo le porte:

```
 netstat -an |egrep '8080|5432|19080|13306'|egrep -v tcp6
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:13306           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:19080           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
```

abilito il servizio in autostart:

```
systemctl enable 3dautossh
```