

Week5-HW-2

1. In EC2 instance page I launched ubuntu machine with below arrangements.

The screenshot shows the 'Launch an instance' wizard. Step 1: Name and tags. A name 'patika-odev-vpn' is entered. Step 2: Application and OS Images (Amazon Machine Image). It shows a search bar and a 'Quick Start' section with logos for Amazon Linux, Ubuntu, Windows, Red Hat, SUSE Linux, and a placeholder for more. A 'Browse more AMIs' link is available. Step 3: Amazon Machine Image (AMI) selection. It lists 'Ubuntu Server 22.04 LTS (HVM), SSD Volume Type' as the selected AMI, which is 'Free tier eligible'. Other details shown include ami-015c25ad8763b2f11 (64-bit (x86)) / ami-0641bed8c0ce71686 (64-bit (Arm)), Virtualization: hvm, ENA enabled: true, Root device type: ebs.

I created Key Pair which is named 'patika-odev-vpn' from Security Groups.

Key pairs (1)							Actions	Create key pair
<input type="text"/> Filter key pairs							Filter	Reset
<input type="checkbox"/>	Name	Type	Created	Fingerprint		ID		
<input type="checkbox"/>	patika-odev-vpn	rsa	2022/06/03 21:16 GMT+3	1f:8a:50:37:c0:f6:58:40:68:7c:b4:ef:aa:...		key-028443c2c1cd09126		

With this patika-odev-vpn the pem file is created and downloaded to host machine, and it is used for connection to EC2 instance.

▼ Instance type [Info](#)

Instance type

t2.micro	Free tier eligible	
Family: t2	1 vCPU	1 GiB Memory
On-Demand Linux pricing: 0.0134 USD per Hour		
On-Demand Windows pricing: 0.018 USD per Hour		

Compare instance types

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

 [Create new key pair](#)

In first selection VPC create default VPC connection.

▼ Network settings

VPC - *required* [Info](#)

vpc-0641da7178ca7dd3f	(default)	
172.31.0.0/16		

Subnet [Info](#)

subnet-0f82df36819ab9519	
VPC: vpc-0641da7178ca7dd3f	Owner: 422442723856
Availability Zone: eu-central-1a	IP addresses available: 4091

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable	
--------	------------------

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

<input checked="" type="radio"/> Create security group	<input type="radio"/> Select existing security group
--	--

Security group name - *required*

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;\$!*

Description - *required* [Info](#)

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - <i>optional</i> Info
Anywhere	<input type="text" value="Add CIDR, prefix list or security"/> 	e.g. SSH for admin desktop
		<input type="text" value="0.0.0.0/0"/>

The created VPC connection which is named 'vpn-server'.

The screenshot shows the AWS VPC console. At the top, there's a header with 'Your VPCs (1/1)' and a 'Create VPC' button. Below the header is a search bar labeled 'Filter VPCs'. The main table has columns: Name, VPC ID, State, IPv4 CIDR, and IPv6 CIDR. A single row is selected, showing 'vpn-server' as the name, 'vpc-0641da7178ca7dd3f' as the VPC ID, 'Available' as the state, '172.31.0.0/16' as the IPv4 CIDR, and '-' as the IPv6 CIDR. Below the table, the VPC ID 'vpc-0641da7178ca7dd3f / vpn-server' is displayed. Underneath, there are tabs for 'Details', 'CIDRs', 'Flow logs', and 'Tags', with 'Details' being the active tab. The 'Details' section contains several key-value pairs:

VPC ID	vpc-0641da7178ca7dd3f	State	Available	DNS hostnames	Enabled	DNS resolution	Enabled
Tenancy	Default	DHCP options set	dopt-03745509368590a17	Main route table	rtb-0ae30d42a171c21de	Main network ACL	acl-089bdc92cd0634626
Default VPC	Yes	IPv4 CIDR	172.31.0.0/16	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Route 53 Resolver DNS Firewall		Owner ID					

Storage is selected as 40 GB.

The screenshot shows the 'Configure storage' section of an EC2 instance setup. It includes a summary table for the root volume and a note about free tier storage. There are also buttons for adding new volumes and viewing file systems.

1x	40	GiB	gp2	Root volume
----	----	-----	-----	-------------

Advanced

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems **Edit**

2. After configured the instance settings I launched the instance as below.

Instances (1/1) [Info](#)

Search [Clear filters](#)

Instance state = running	X	Clear filters						
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Pu...
patika-odev-vpn	i-07f2e059b23cd52ca	Running	t2.micro	2/2 checks passed	No alarms	eu-central-1a	ec2-3-65-0-178.eu-cent...	3.6

Instance: i-07f2e059b23cd52ca (patika-odev-vpn)

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

Instance summary [Info](#)

Instance ID i-07f2e059b23cd52ca (patika-odev-vpn)	Public IPv4 address 3.65.0.178 open address	Private IPv4 addresses 172.31.20.82
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-65-0-178.eu-central-1.compute.amazonaws.com open address
Hostname type IP name: ip-172-31-20-82.eu-central-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-20-82.eu-central-1.compute.internal	Answer private resource DNS name IPv4 (A)
Instance type t2.micro	Elastic IP addresses -	Auto-assigned IP address 3.65.0.178 [Public IP]
VPC ID vpc-0641da7178ca7dd3f (vin-server)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	IAM Role -

Public IPv4 Address :3.68.247.170

Private IPv4 Address :172.31.20.82

When we shutdown the machine we lost Public IPv4 Address. In order not to loose this ip address, we need to apply the Elastic IP address Allocation.

Success Elastic IP address associated successfully.
Elastic IP address 3.68.247.170 has been associated with instance i-07f2e059b23cd52ca

Elastic IP addresses (1/1)

Filter Elastic IP addresses [Clear filters](#)

Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record	Associated instance ID
vin-server-elp	3.68.247.170	Public IP	eipalloc-08aff37d2ba344d0a	-	i-07f2e059b23cd52ca

Summary

Allocated IPv4 address 3.68.247.170	Type Public IP	Allocation ID eipalloc-08aff37d2ba344d0a	Reverse DNS record -
Association ID eipassoc-05908157dba69368d	Scope VPC	Associated instance ID i-07f2e059b23cd52ca	Private IP address 172.31.20.82
Network interface ID eni-0d06c0a2ba567c17f	Network interface owner account ID 422442723856	Public DNS ec2-3-68-247-170.eu-central-1.compute.amazonaws.com	NAT Gateway ID -

Final result of our instance is like below:

The screenshot shows the AWS EC2 Instances page. At the top, there's a search bar and several filter and action buttons. Below the header, a table lists one instance: 'patika-odev-vpn' (instance ID i-07f2e059b23cd52ca), which is 'Running' and has an 't2.micro' instance type. It has 2/2 checks passed and no alarms. The instance is located in 'eu-central-1a' and has a public IPv4 address of 'ec2-3-68-247-170.eu-c...'.

Below the table, a detailed view for the instance 'i-07f2e059b23cd52ca (patika-odev-vpn)' is shown. The 'Details' tab is selected, followed by tabs for Security, Networking, Storage, Status checks, Monitoring, and Tags. Under 'Instance summary', the following details are listed:

Detail	Value	Detail	Value
Instance ID	i-07f2e059b23cd52ca (patika-odev-vpn)	Public IPv4 address	3.68.247.170 open address
IPv6 address	-	Instance state	Running
Hostname type	IP name: ip-172-31-20-82.eu-central-1.compute.internal	Private IP DNS name (IPv4 only)	ip-172-31-20-82.eu-central-1.compute.internal
Instance type	t2.micro	Elastic IP addresses	3.68.247.170 (vin-server-elp) [Public IP]
		Private IPv4 addresses	172.31.20.82
		Public IPv4 DNS	ec2-3-68-247-170.eu-central-1.compute.amazonaws.com open address
		Answer private resource DNS name	IPv4 (A)
		Auto-assigned IP address	-

At the bottom of the page, there are links for Feedback, Unified Settings, Copyright notice, Privacy, Terms, and Cookie preferences.

3. To connect with SSH client from host:

I changed the permission of the downloaded pem file .

The screenshot shows the 'Connect to instance' dialog for the instance 'i-07f2e059b23cd52ca (patika-odev-vpn)'. The 'SSH client' tab is selected. The dialog provides instructions for connecting:

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is 'patika-odev-vpn.pem'.
- Run this command, if necessary, to ensure your key is not publicly viewable:
chmod 400 patika-odev-vpn.pem
- Connect to your instance using its Public DNS:
ec2-3-68-247-170.eu-central-1.compute.amazonaws.com

Example command:
ssh -i "patika-odev-vpn.pem" ubuntu@ec2-3-68-247-170.eu-central-1.compute.amazonaws.com

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

At the bottom right, there's a 'Cancel' button.

At the very bottom, there are links for Feedback, Unified Settings, Copyright notice, Privacy, Terms, and Cookie preferences.

We connected the ubuntu machine with this command:

```
ubuntu@ip-172-31-20-82: ~
> ssh -i "patika-odev-vpn.pem" ubuntu@ec2-3-68-247-170.eu-central-1.compute.amazonaws.com
```

```
ubuntu@ip-172-31-20-82: ~
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-1004-aws x86_64)

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

 System information as of Fri Jun  3 19:03:21 UTC 2022

 System load:  0.0           Processes:      98
 Usage of /:   3.7% of 38.60GB  Users logged in:  0
 Memory usage: 20%
 Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-20-82:~$
```

4. After connection is succeeded, in ubuntu machine I downloaded Open VPN Tool from GitHub.

```
ubuntu@ip-172-31-20-82: ~
ubuntu@ip-172-31-20-82:~$ wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh
--2022-06-03 19:05:40--  https://git.io/vpn
Resolving git.io (git.io)... 140.82.113.21
Connecting to git.io (git.io)|140.82.113.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.github.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-06-03 19:05:40--  https://raw.github.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.github.com (raw.github.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.github.com (raw.github.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2022-06-03 19:05:40--  https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23501 (23K) [text/plain]
Saving to: 'openvpn-install.sh'

openvpn-install.sh          100%[=====]  22.95K --.-KB/s    in 0s

2022-06-03 19:05:40 (89.1 MB/s) - 'openvpn-install.sh' saved [23501/23501]

This installer needs to be run with superuser privileges.
ubuntu@ip-172-31-20-82:~$
```

```
ubuntu@ip-172-31-20-82:~  
Welcome to this OpenVPN road warrior installer!  
This server is behind NAT. What is the public IPv4 address or hostname?  
Public IPv4 address / hostname [3.68.247.170]:  
Which protocol should OpenVPN use?  
 1) UDP (recommended)  
 2) TCP  
Protocol [1]: 1  
What port should OpenVPN listen to?  
Port [1194]:  
Select a DNS server for the clients:  
 1) Current system resolvers  
 2) Google  
 3) 1.1.1.1  
 4) OpenDNS  
 5) Quad9  
 6) AdGuard  
DNS server [1]: 1  
Enter a name for the first client:  
Name [client]: elif-client
```

```
root@ip-172-31-20-82:~  
* Notice:  
An updated CRL has been created.  
CRL file: /etc/openvpn/server/easy-rsa/pki/crl.pem  
2022-06-03 19:12:35 WARNING: Using --genkey --secret filename is DEPRECATED. Use --genkey secret filename instead.  
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-iptables.service → /etc/systemd/system/openvpn-iptables.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /lib/systemd/system/openvpn-server@.service.  
Finished!  
The client configuration is available in: /root/elif-client.ovpn  
New clients can be added by running this script again.  
ubuntu@ip-172-31-20-82:~$ cd /root  
-bash: cd: /root: Permission denied  
ubuntu@ip-172-31-20-82:~$ sudo su  
root@ip-172-31-20-82:/home/ubuntu# cd /root  
root@ip-172-31-20-82:~/# ll  
total 36  
drwx----- 4 root root 4096 Jun  3 19:12 ./  
drwxr-xr-x 19 root root 4096 Jun  3 18:42 ../  
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc  
-rw-r--r--  1 root root 161 Jul  9  2019 .profile  
drwx-----  2 root root 4096 Jun  3 18:42 .ssh/  
-rw-r--r--  1 root root 165 Jun  3 19:12 .wget-hsts  
-rw-r--r--  1 root root 5020 Jun  3 19:12 elif-client.ovpn  
drwx-----  4 root root 4096 Jun  3 18:42 snap/
```

The VPN client makes a connection with 1194 UDP port and we should edit inbound rules for EC2 instance.

EC2 > Security Groups > sg-0682aa1b440976bd0 - patika-odev-vpn-sg > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules <small>Info</small>						
Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sgr-0ece050cb81f47d2f	SSH	TCP	22	Custom ▾	<input type="text"/> 0.0.0.0/0 X	<input type="button"/> Delete
-	Custom UDP	UDP	1194	Anywh... ▾	<input type="text"/> 0.0.0.0/0 X	<input type="button"/> allow access to VPN port <input type="button"/> Delete

Add rule

Cancel Preview changes Save rules

Details

Security group name <input type="button"/> patika-odev-vpn-sg	Security group ID <input type="button"/> sg-0682aa1b440976bd0	Description <input type="button"/> launch-wizard-1 created 2022-06-03T18:10:10.535Z	VPC ID <input type="button"/> vpc-0641da7178ca7dd3f <input checked="" type="checkbox"/>
Owner <input type="button"/> 422442723856	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

ⓘ You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X

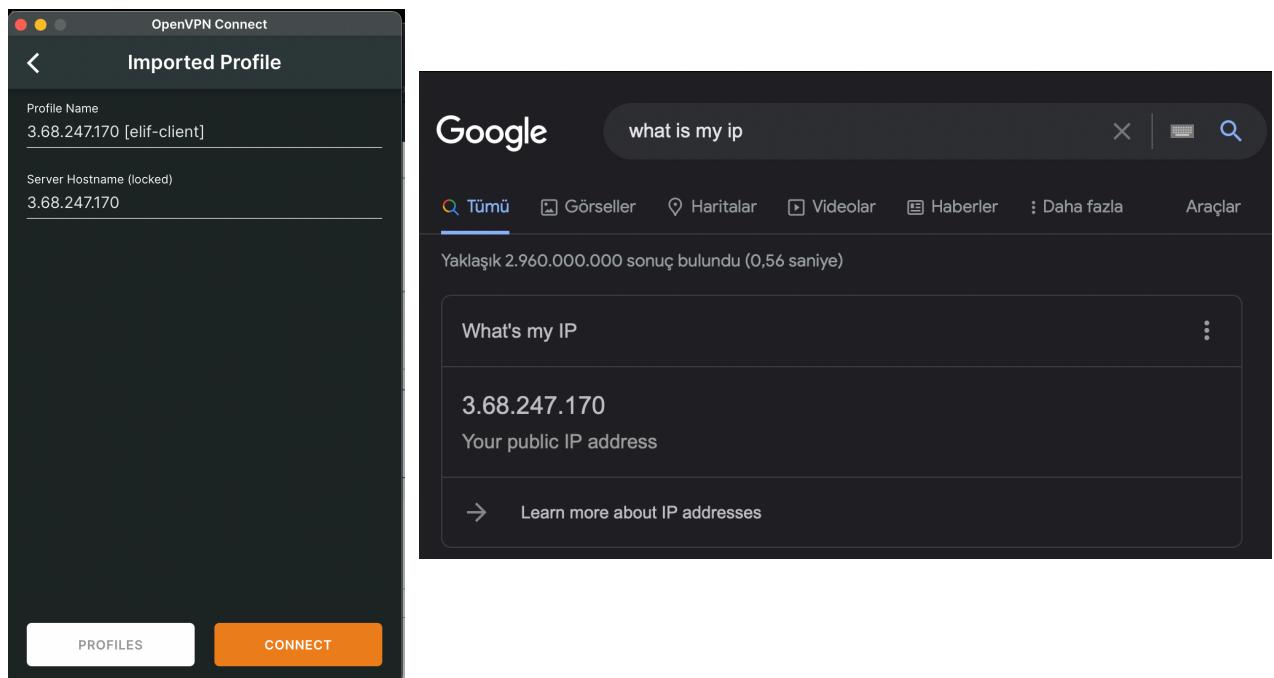
Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-0147019a1c659c4cd	IPv4	Custom UDP	UDP
<input type="checkbox"/>	-	sgr-0ece050cb81f47d2f	IPv4	SSH	TCP

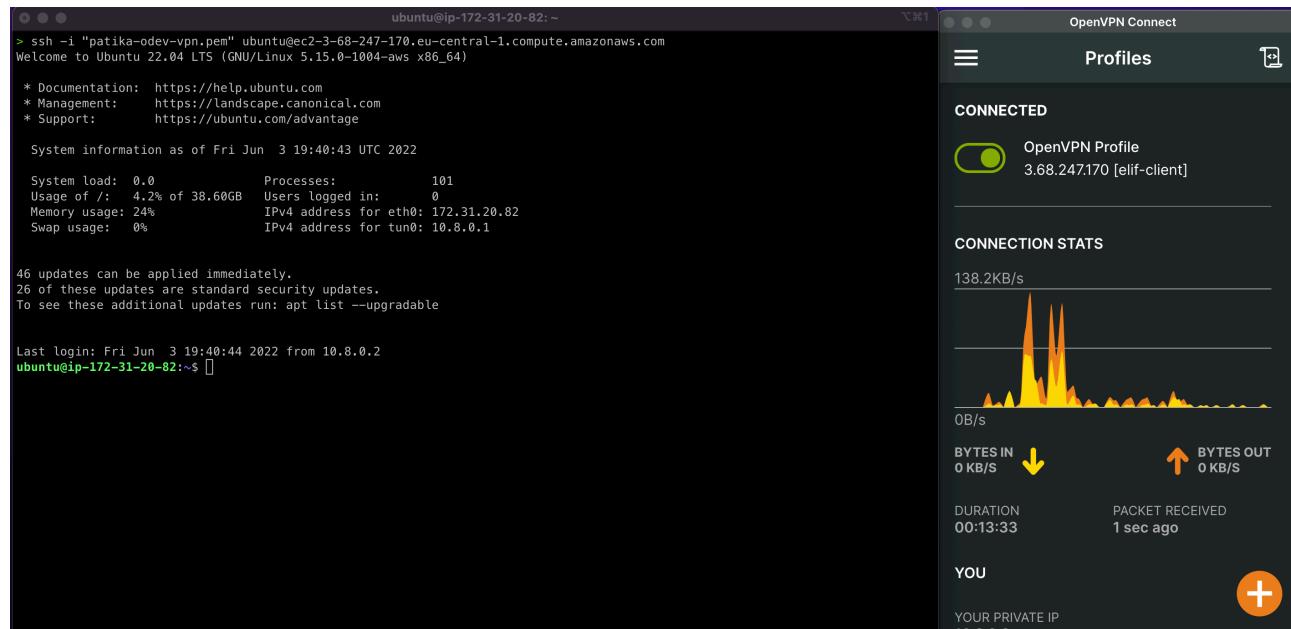
The 'elif-client.ovpn' file is in ubuntu machine and I moved it to host machine with scp connection:

```
> scp -i "patika-odev-vpn.pem" ubuntu@ec2-3-68-247-170.eu-central-1.compute.amazonaws.com:/home/ubuntu/elif-client.ovpn .
elif-client.ovpn                                         100% 5020     79.7KB/s   00:00
> ll
total 24
-rw-r--r--  1 elif  staff   4,9K  3 Haz 22:18 elif-client.ovpn
-r-----@ 1 elif  staff   1,6K  3 Haz 21:19 patika-odev-vpn.pem
~/Desktop/aws/personal >
```

I downloaded OpenVPN Connect in host machine and drop the elif-client.ovpn file for VPN connection.



While VPN connection is open, to connect the ubuntu instance form host:



Ubuntu machine connected with Private IP address which is mean local connection because we are in VPN connection.