Department of Computer Science, Electrical and Space Engineering

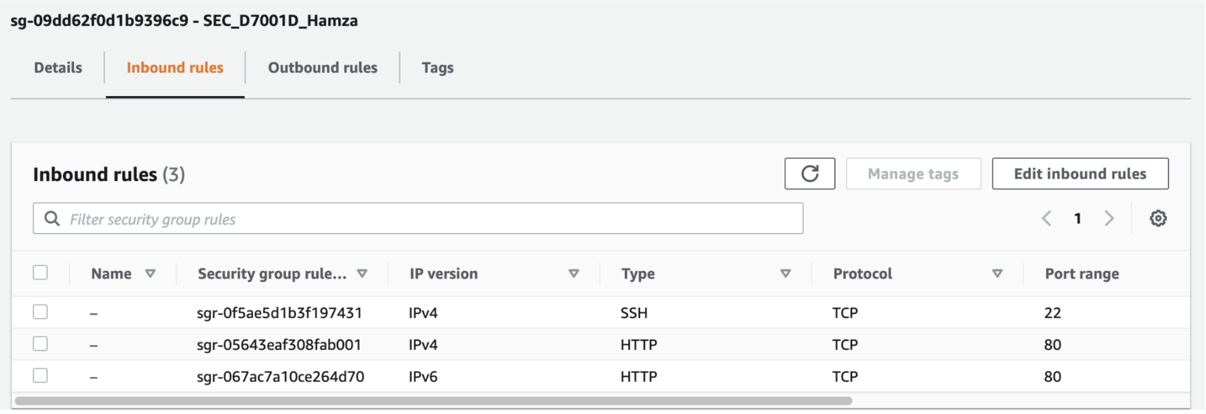
Network Programming and Distributed Applications

Lab 1 - Networking Fundamentals

Ameer Hamza, Otabek Sobirov

10th September 2021

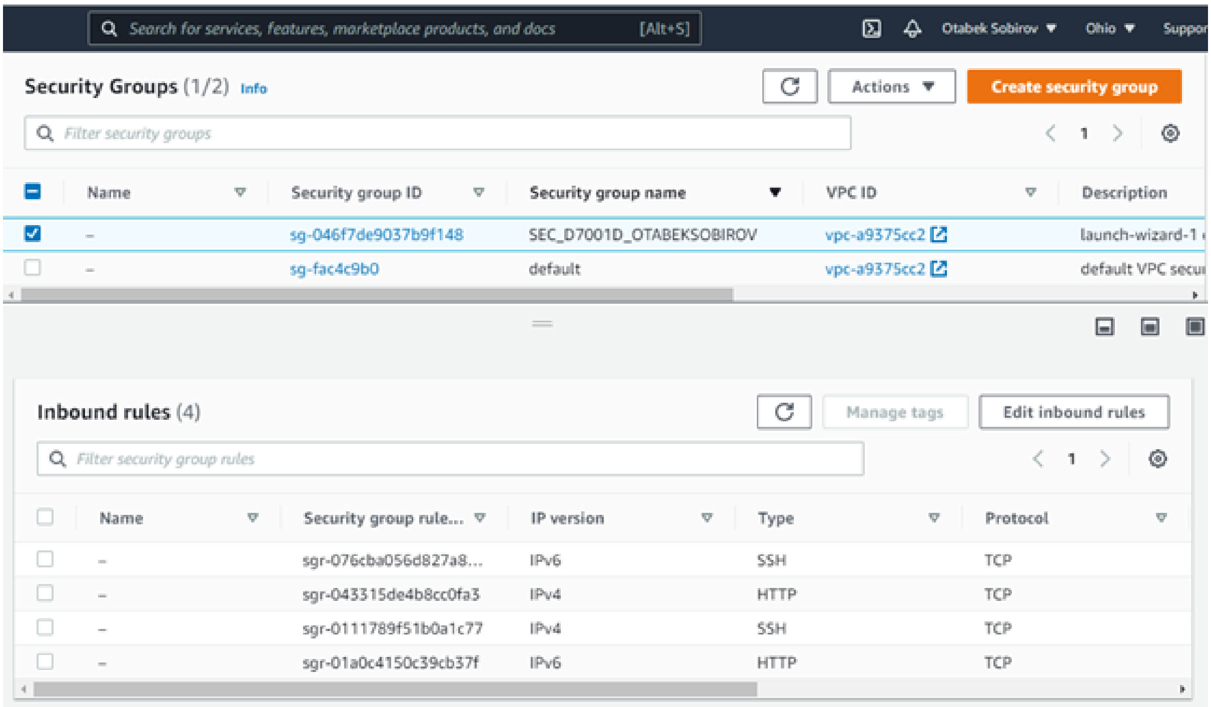
1. Create a security group: SEC_D7001D_YOURLOGINNAME. Configure it to allow SSH and HTTP.



sg-09dd62f0d1b9396c9 - SEC_D7001D_Hamza

Inbound rules (3)

□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-0f5ae5d1b3f197431	IPv4	SSH	TCP	22
□	–	sgr-05643eaf308fab001	IPv4	HTTP	TCP	80
□	–	sgr-067ac7a10ce264d70	IPv6	HTTP	TCP	80



Security Groups (1/2)

☑	Name	Security group ID	Security group name	VPC ID	Description
☑	–	sg-046f7de9037b9f148	SEC_D7001D_OTABEKSOBIROV	vpc-a9375cc2	launch-wizard-1
□	–	sg-fac4c9b0	default	vpc-a9375cc2	default VPC secu

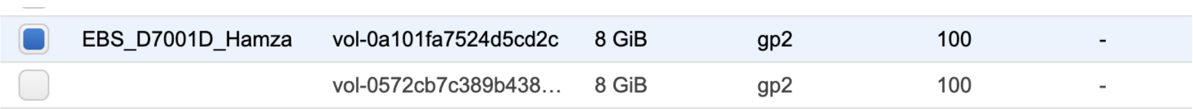
Inbound rules (4)

□	Name	Security group rule...	IP version	Type	Protocol
□	–	sgr-076cba056d827a8...	IPv6	SSH	TCP
□	–	sgr-043315de4b8cc0fa3	IPv4	HTTP	TCP
□	–	sgr-0111789f51b0a1c77	IPv4	SSH	TCP
□	–	sgr-01a0c4150c39cb37f	IPv6	HTTP	TCP

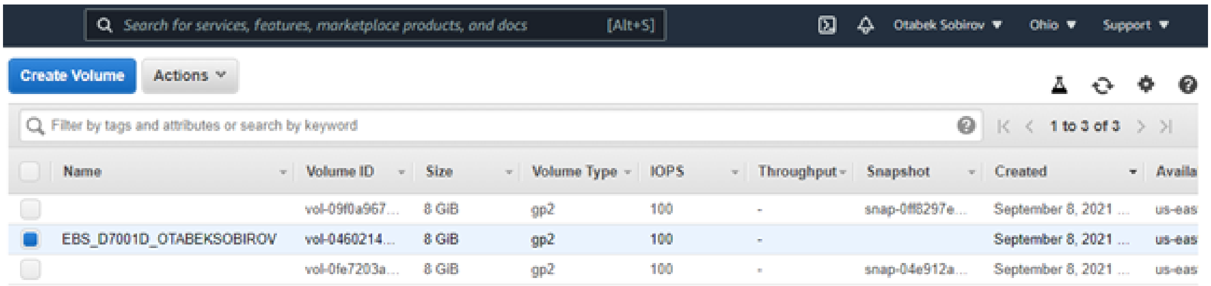
a. QUESTION 1: What is the purpose of security groups in AWS cloud?

Security groups are used to create a group of rules for controlling the inbound and outbound traffic flows to EC2 instances. Groups act as the virtual network firewall. We specify a set of rules based on the protocol and port number used to access EC2 instances.

2. Create an EBS volume with the name EBS_D7001D_YOURUSERNAME.

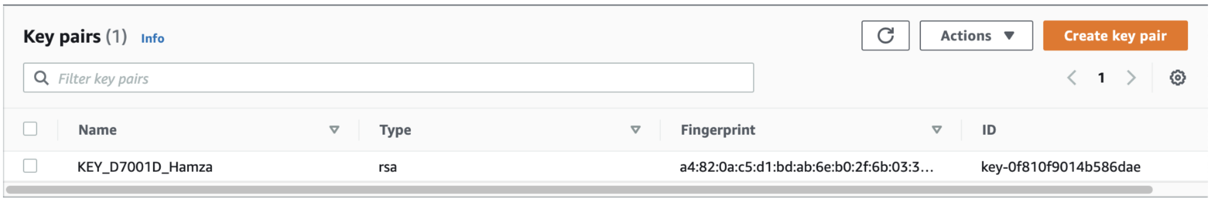


■	EBS_D7001D_Hamza	vol-0a101fa7524d5cd2c	8 GiB	gp2	100	-
□		vol-0572cb7c389b438...	8 GiB	gp2	100	-

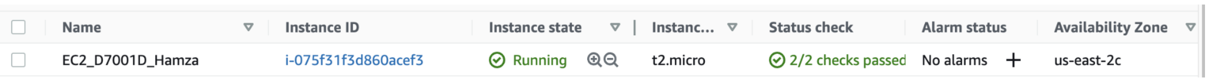

Search for services, features, marketplace products, and docs [Alt+S]
Otabek Sobirov ▼
Ohio ▼
Support ▼
Create Volume
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3

□	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot	Created	Availa
□		vol-09f0a967...	8 GiB	gp2	100	-	snap-0ff8297e...	September 8, 2021 ...	us-eas
☑	EBS_D7001D_OTABEKSOBIROV	vol-0460214...	8 GiB	gp2	100	-		September 8, 2021 ...	us-eas
□		vol-0fe7203a...	8 GiB	gp2	100	-	snap-04e912a...	September 8, 2021 ...	us-eas

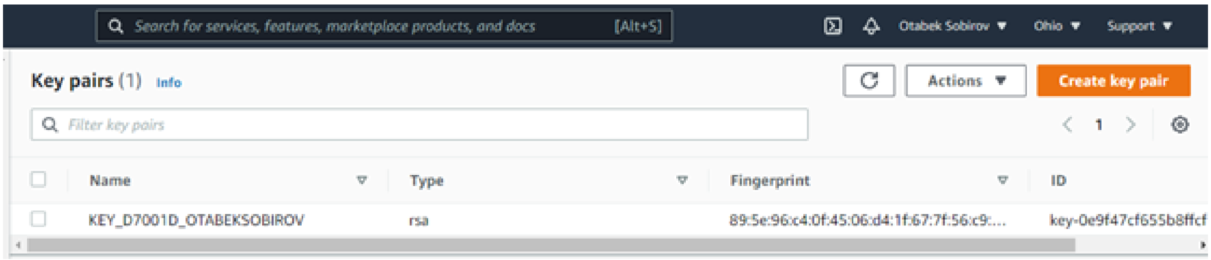
3. Create and launch AWS Instance with the name EC2_D7001D_YOURUSERNAME. Note that the key pair MUST be tagged as KEY_D7001D_YOURUSERNAME and be associated with YOUR security group.



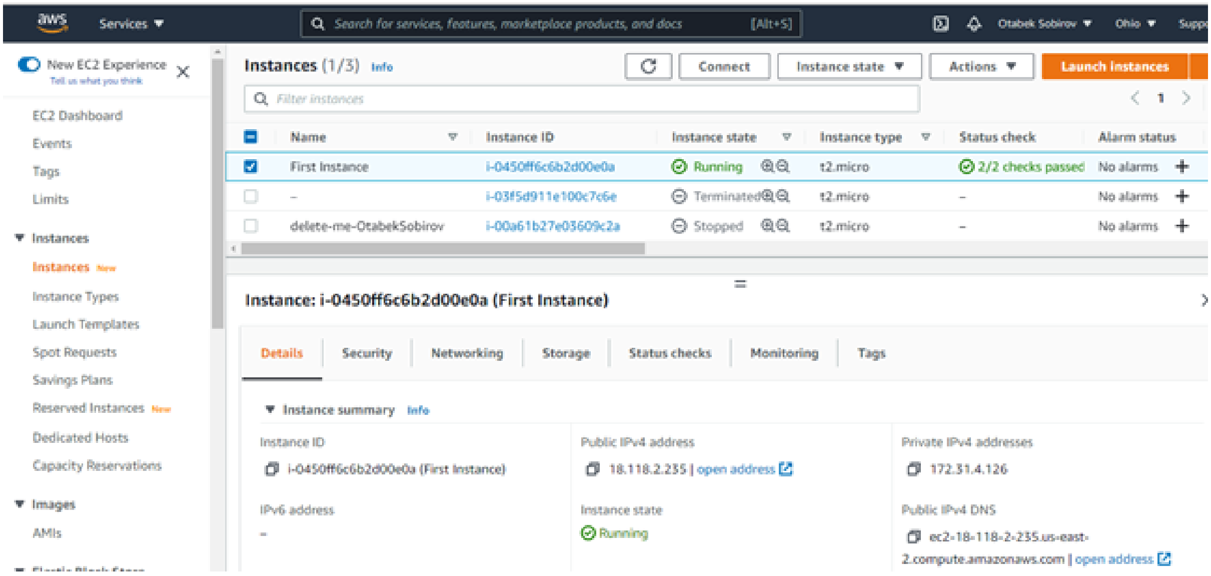
□	Name	Type	Fingerprint	ID
□	KEY_D7001D_Hamza	rsa	a4:82:0a:c5:d1:bd:ab:6e:b0:2f:6b:03:3...	key-0f810f9014b586dae



□	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability Zone
□	EC2_D7001D_Hamza	i-075f31f3d860acef3	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	us-east-2c



□	Name	Type	Fingerprint	ID
□	KEY_D7001D_OTABEKSOBIROV	rsa	89:5e:96:c4:0f:45:06:d4:1f:67:7f:56:c9:...	key-0e9f47cf655b8ffcf



☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	First Instance	i-0450ff6c6b2d00e0a	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +
□	–	i-03f5d911e100c7c6e	⊖ Terminated	t2.micro	–	No alarms +
□	delete-me-OtabekSobirov	i-00a61b27e03609c2a	⊖ Stopped	t2.micro	–	No alarms +

Instance: i-0450ff6c6b2d00e0a (First Instance)

Instance ID: i-0450ff6c6b2d00e0a (First Instance)

Public IPv4 address: 18.118.2.235 | open address

Private IPv4 addresses: 172.31.4.126

IPv6 address: –

Instance state: ✓ Running

Public IPv4 DNS: ec2-18-118-2-235.us-east-2.compute.amazonaws.com | open address

a. QUESTION 2. What type of instance did you create?

t2.micro instance was created. It provides 1 vCPU and 1 GiB of RAM. T2 instances are Burstable Performance Instances that can provide baseline computation power.

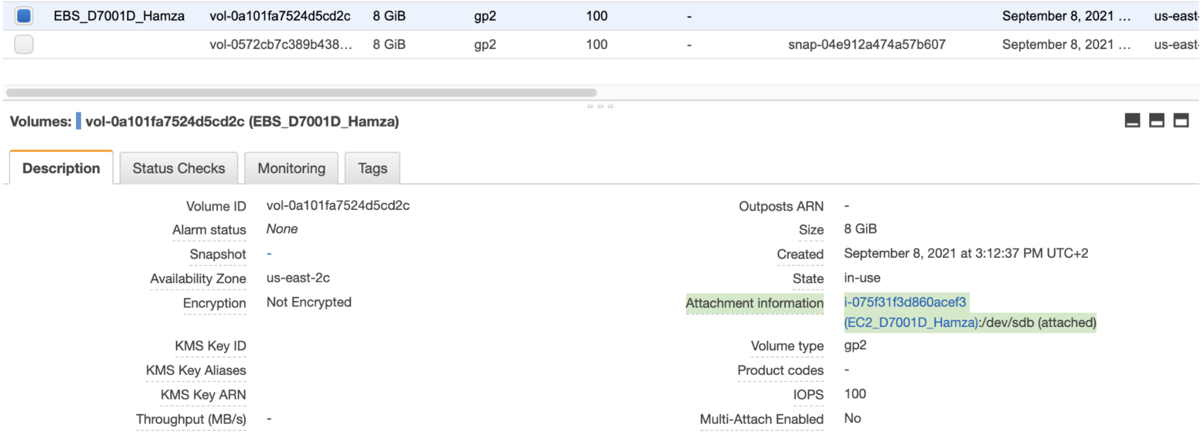
However, they can jump over this baseline if more requests are generated from users (yet fees apply for these extra requests even though it is in the Free Tier plan).

b. QUESTION 3. Which AMI you selected, what motivated your choice.

Ubuntu Server 20.04 LTS (HVM), SSD AMI was used. This AMI is based on Ubuntu for 64-bit (x86) architecture. Three main reasons for using this are:

1. It is in Free Tier Plan
2. Easy to manage
3. Preferred OS for small scale and fast development projects
4. Wide support available for installing packages and troubleshooting.

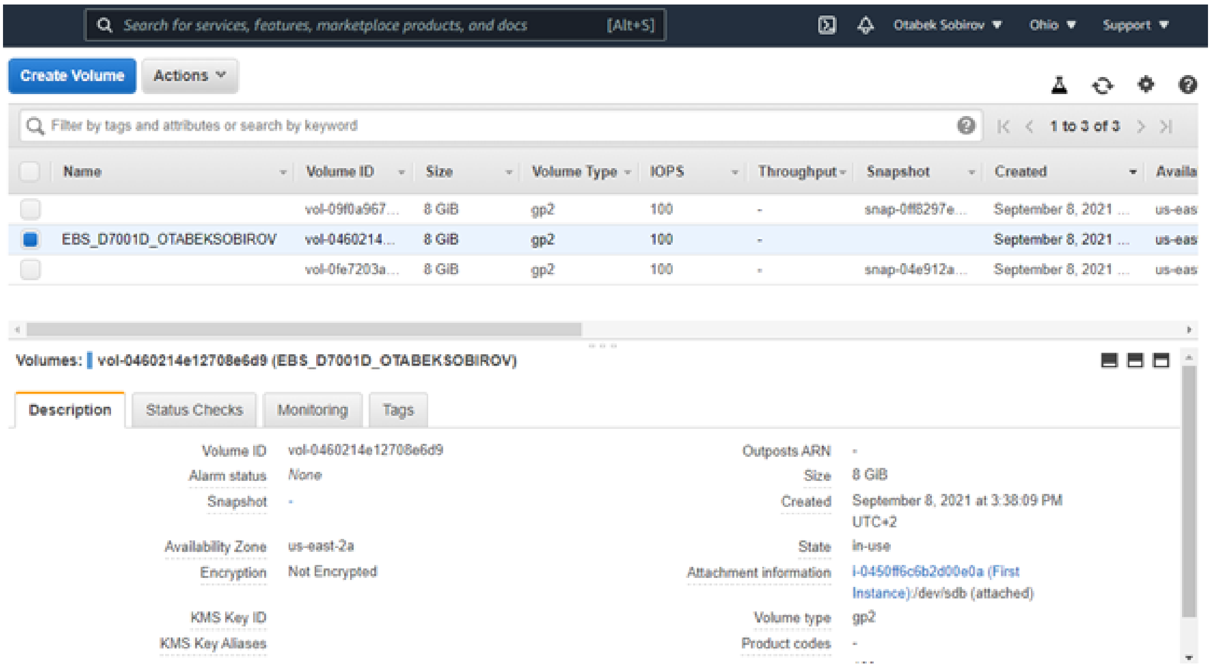
4. Attach your EBS_D7001D_YOURUSERNAME EBS to the instance. Note: store all your working files MUST BE INSIDE THIS EBS. Make sure you have an unchecked "delete on termination" option!



☑	EBS_D7001D_Hamza	vol-0a101fa7524d5cd2c	8 GiB	gp2	100	-		September 8, 2021 ...	us-east
□		vol-0572cb7c389b438...	8 GiB	gp2	100	-	snap-04e912a474a57b607	September 8, 2021 ...	us-east

Volumes: vol-0a101fa7524d5cd2c (EBS_D7001D_Hamza)

Volume ID	vol-0a101fa7524d5cd2c	Outposts ARN	-
Alarm status	*None*	Size	8 GiB
Snapshot	-	Created	September 8, 2021 at 3:12:37 PM UTC+2
Availability Zone	us-east-2c	State	in-use
Encryption	Not Encrypted	Attachment information	i-075f31f3d860acef3 (EC2_D7001D_Hamza):/dev/sdb (attached)
KMS Key ID		Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN		IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No


Search for services, features, marketplace products, and docs
[Alt+S]
Otabek Sobirov
Ohio
Support
Create Volume
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3

	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot	Created	Availa
□		vol-09f0a967...	8 GiB	gp2	100	-	snap-0ff8297e...	September 8, 2021 ...	us-eas
■	EBS_D7001D_OTABEKSOBIROV	vol-0460214...	8 GiB	gp2	100	-		September 8, 2021 ...	us-eas
□		vol-0fe7203a...	8 GiB	gp2	100	-	snap-04e912a...	September 8, 2021 ...	us-eas

Volumes: vol-0460214e12708e6d9 (EBS_D7001D_OTABEKSOBIROV)

Description
Status Checks
Monitoring
Tags

Volume ID vol-0460214e12708e6d9
Alarm status *None*
Snapshot -
Availability Zone us-east-2a
Encryption Not Encrypted
KMS Key ID
KMS Key Aliases

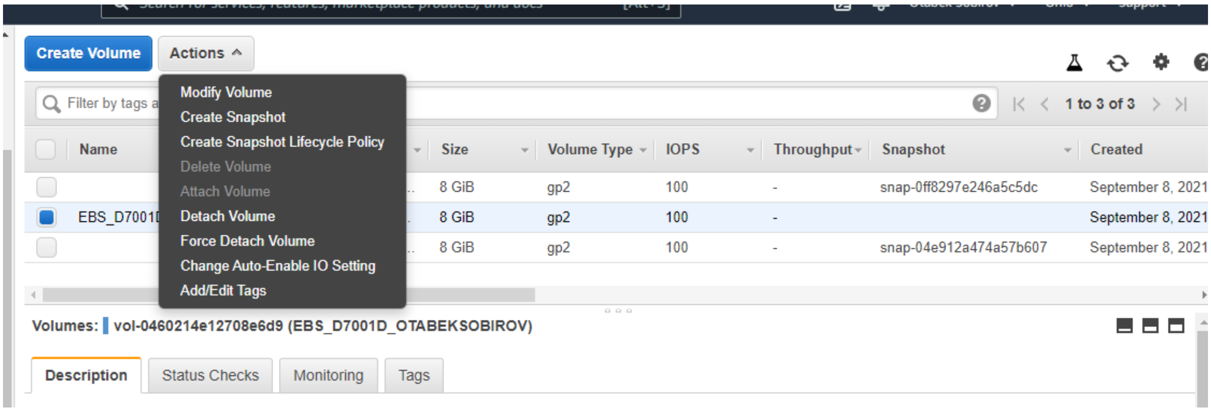
Outposts ARN -
Size 8 GiB
Created September 8, 2021 at 3:38:09 PM UTC+2
State in-use
Attachment information i-0450ff6c6b2d00e0a (First Instance):/dev/sdb (attached)
Volume type gp2
Product codes -

QUESTION 4. Which file system is configured on your volume?

ext4 file system is configured on the instance volume.

b. QUESTION 5. Can you change it?

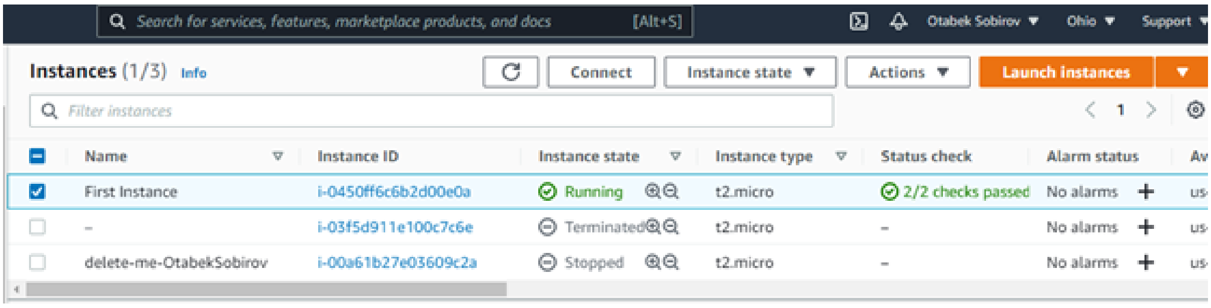
We can change the file system of the attached volume by formatting it. However, it is not possible to change it for the root volume or the volume in which the OS is installed.
This can't be done directly from AWS. For this you need to use the console of the OS.



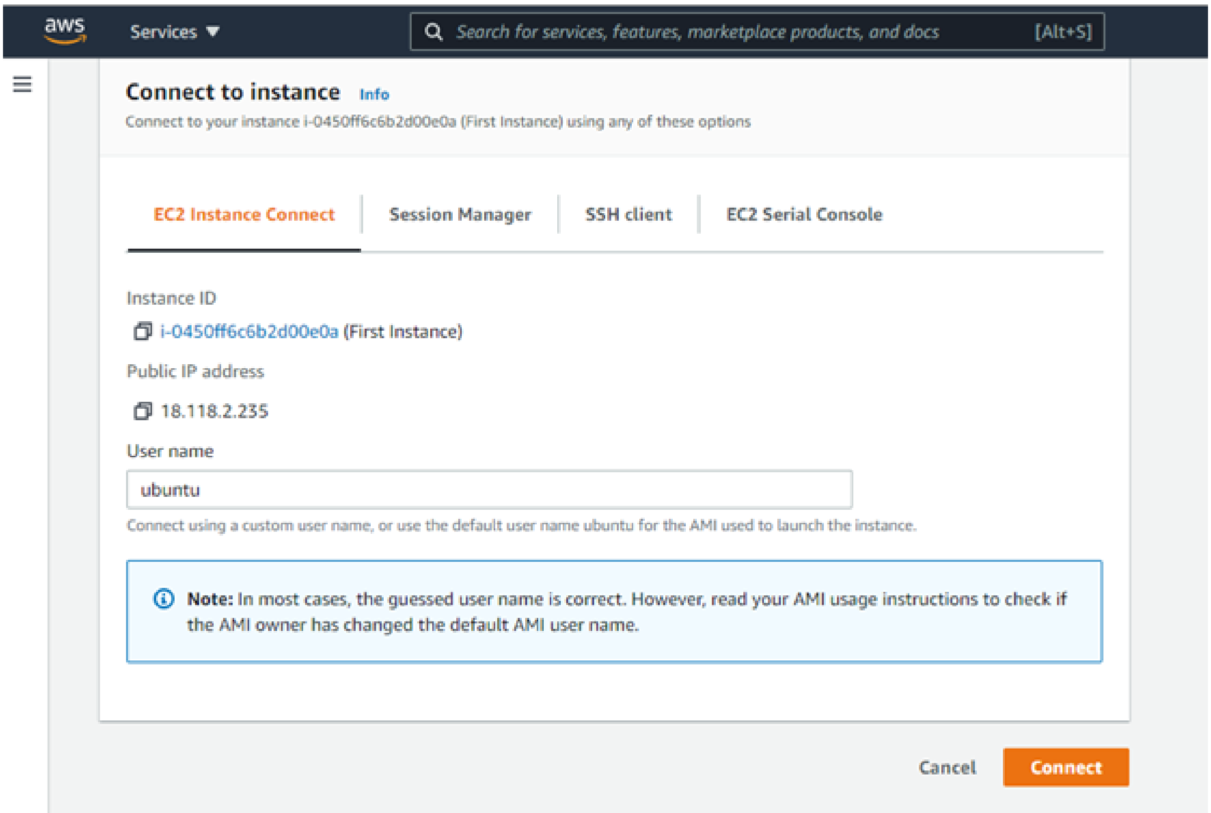
	Name		Size	Volume Type	IOPS	Throughput	Snapshot	Created
□			8 GiB	gp2	100	-	snap-0ff8297e246a5c5dc	September 8, 2021
■	EBS_D7001D		8 GiB	gp2	100	-		September 8, 2021
□			8 GiB	gp2	100	-	snap-04e912a474a57b607	September 8, 2021

Volumes: vol-0460214e12708e6d9 (EBS_D7001D_OTABEKSOBIROV)

5. Log in to your EC2_D7001D_YOURUSERNAME instance.



▬	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Av
☑	First Instance	i-0450ff6c6b2d00e0a	Running	t2.micro	2/2 checks passed	No alarms +	us
□	–	i-03f5d911e100c7c6e	Terminated	t2.micro	–	No alarms +	us
□	delete-me-OtabekSobirov	i-00a61b27e03609c2a	Stopped	t2.micro	–	No alarms +	us



Connect to instance Info

Connect to your instance i-0450ff6c6b2d00e0a (First Instance) using any of these options

Instance ID

i-0450ff6c6b2d00e0a (First Instance)

Public IP address

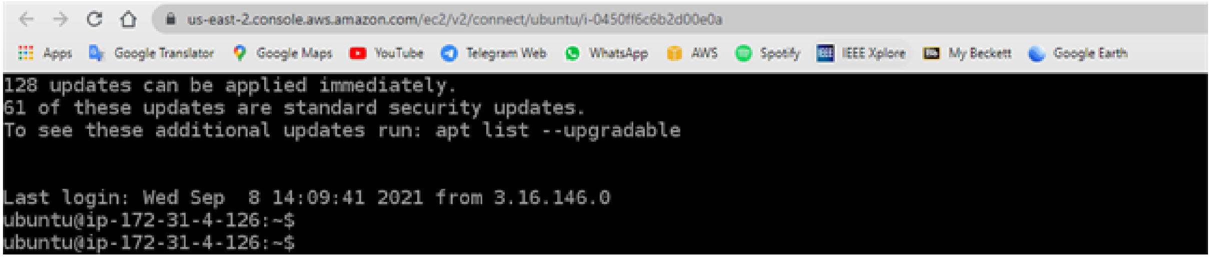
18.118.2.235

User name

ubuntu

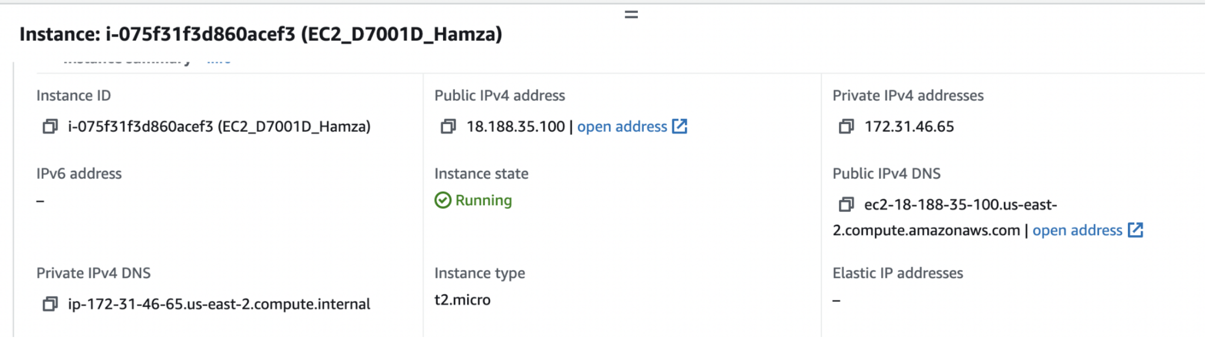
Connect using a custom user name, or use the default user name ubuntu for the AMI used to launch the instance.

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.



```
128 updates can be applied immediately.
61 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Wed Sep  8 14:09:41 2021 from 3.16.146.0
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
```

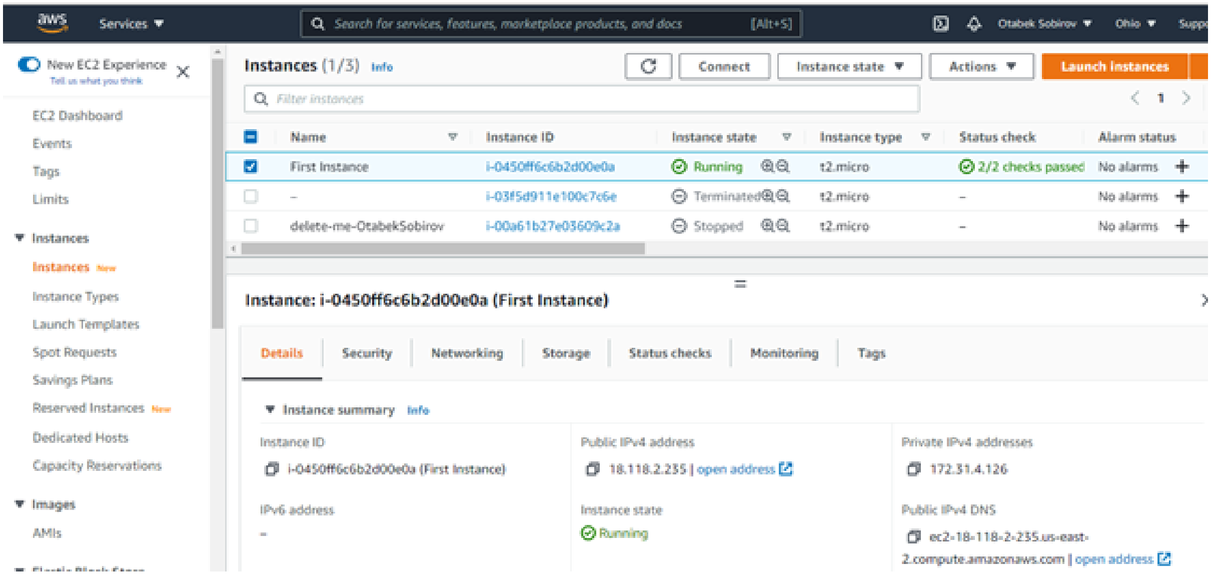


Instance: i-075f31f3d860acef3 (EC2_D7001D_Hamza)

Instance ID	Public IPv4 address	Private IPv4 addresses
i-075f31f3d860acef3 (EC2_D7001D_Hamza)	18.188.35.100 | open address	172.31.46.65

IPv6 address	Instance state	Public IPv4 DNS
–	Running	ec2-18-188-35-100.us-east-2.compute.amazonaws.com | open address

Private IPv4 DNS	Instance type	Elastic IP addresses
ip-172-31-46-65.us-east-2.compute.internal	t2.micro	–



Instances (1/3) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	First Instance	i-0450ff6c6b2d00e0a	Running	t2.micro	2/2 checks passed	No alarms
☐	–	i-03f5d911e100c7c6e	Terminated	t2.micro	–	No alarms
☐	delete-me-OtabekSobirov	i-00a61b27e03609c2a	Stopped	t2.micro	–	No alarms

Instance: i-0450ff6c6b2d00e0a (First Instance)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0450ff6c6b2d00e0a (First Instance)	18.118.2.235 | open address	172.31.4.126

IPv6 address	Instance state	Public IPv4 DNS
–	Running	ec2-18-118-2-235.us-east-2.compute.amazonaws.com | open address

a. QUESTION 6. What is the IP address of your instance?

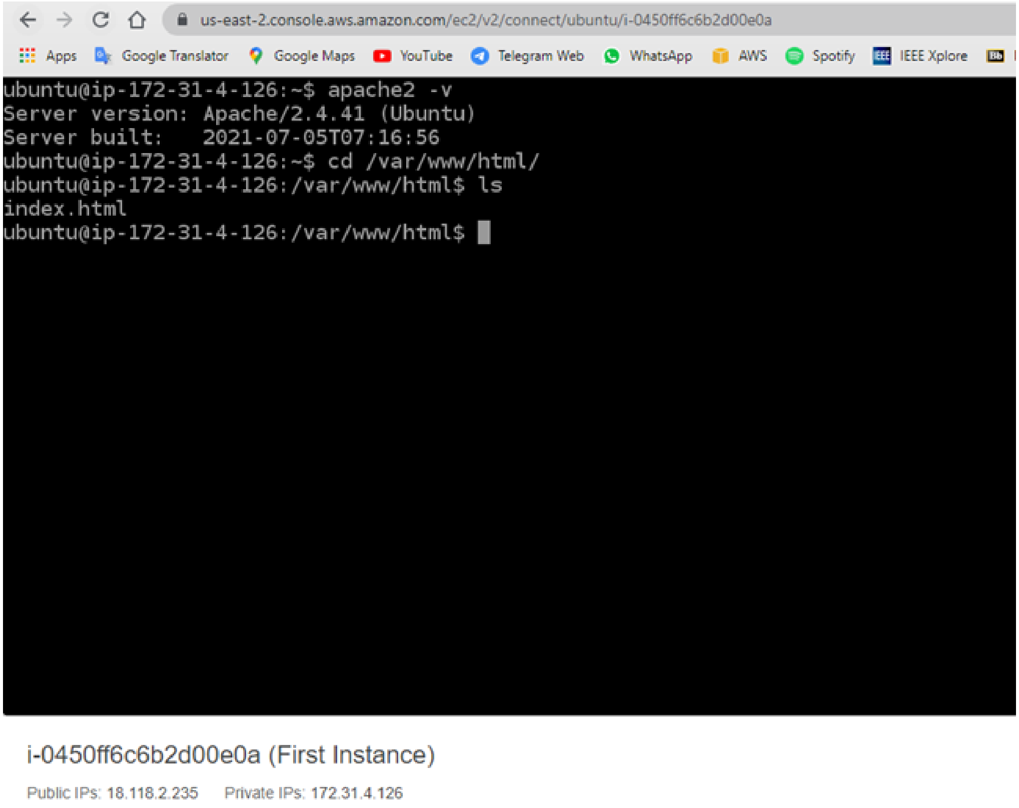
The instance has two IP addresses: Public and Private. Public and the private IP addresses of the instance are shown in the screenshot above.

The private IP address is used in the Cloud local network to communicate with other instances or network devices. The public IP address is for accessing the instance from the internet.

b. QUESTION 7. What is its public and private dns name?

Public and the private DNS addresses of the instances are shown in the screenshot above.

6. Install apache server on your instance (For Ubuntu: sudo apt-get install apache2)



```
ubuntu@ip-172-31-4-126:~$ apache2 -v
Server version: Apache/2.4.41 (Ubuntu)
Server built:   2021-07-05T07:16:56
ubuntu@ip-172-31-4-126:~$ cd /var/www/html/
ubuntu@ip-172-31-4-126:/var/www/html$ ls
index.html
ubuntu@ip-172-31-4-126:/var/www/html$
```

i-0450ff6c6b2d00e0a (First Instance)

Public IPs: 18.118.2.235   Private IPs: 172.31.4.126

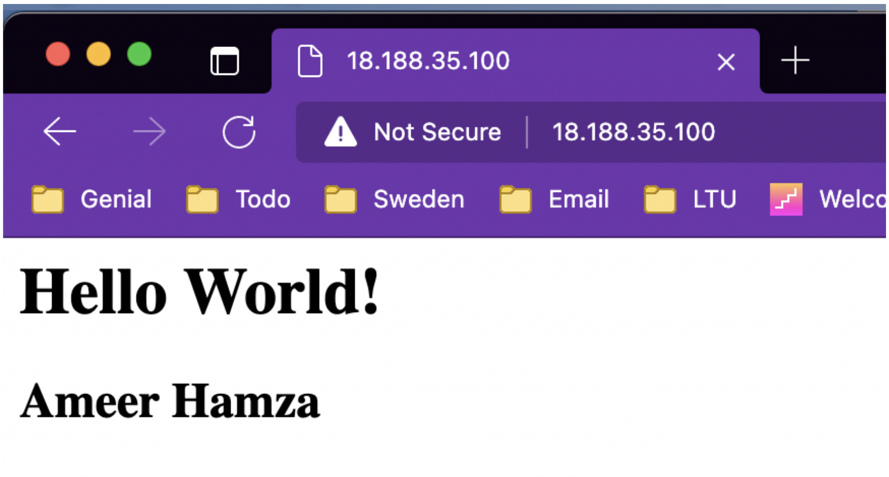
a. QUESTION 8. What is the public address on your server?

IP address: 18.118.2.235

b. QUESTION 9. What text is shown when you open a public dns name in a web browser?

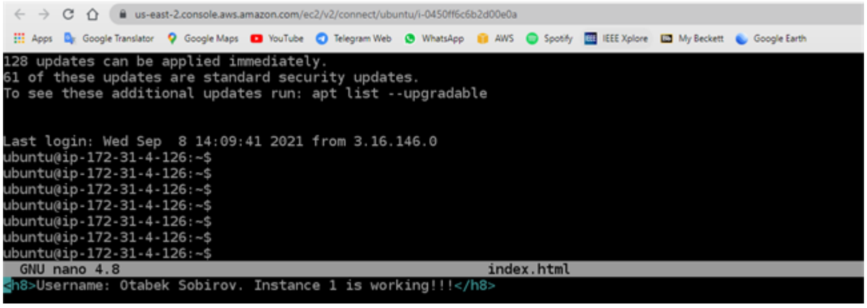
The default page of Apache2 Web Server.

7. Now edit /var/www/index.html and enter text so that you can distinguish this instance from others. When you are done go to the AWS console, select your instance and choose launch more like this.



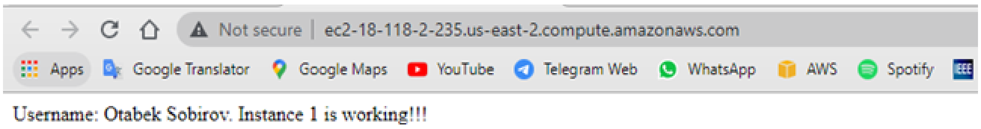
Hello World!

Ameer Hamza



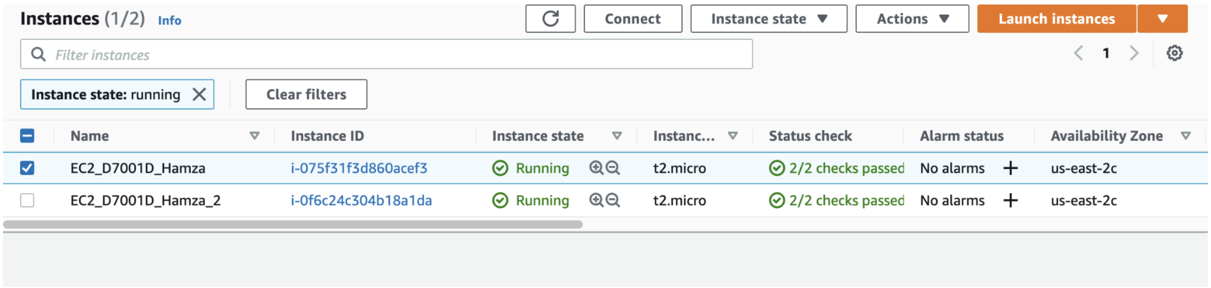
```
128 updates can be applied immediately.
61 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Wed Sep  8 14:09:41 2021 from 3.16.146.0
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
ubuntu@ip-172-31-4-126:~$
  GNU nano 4.8                                 index.html
<h8>Username: Otabek Sobirov. Instance 1 is working!!!</h8>
```

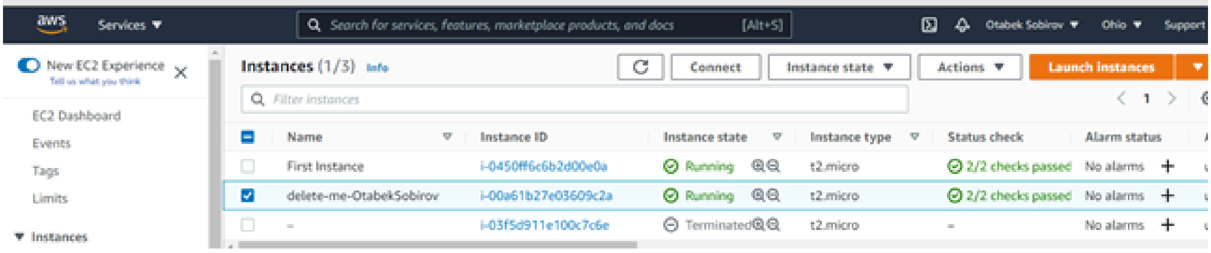


Username: Otabek Sobirov. Instance 1 is working!!!

8. Launch one additional instance. Copy its public dns and paste it to a web browser.



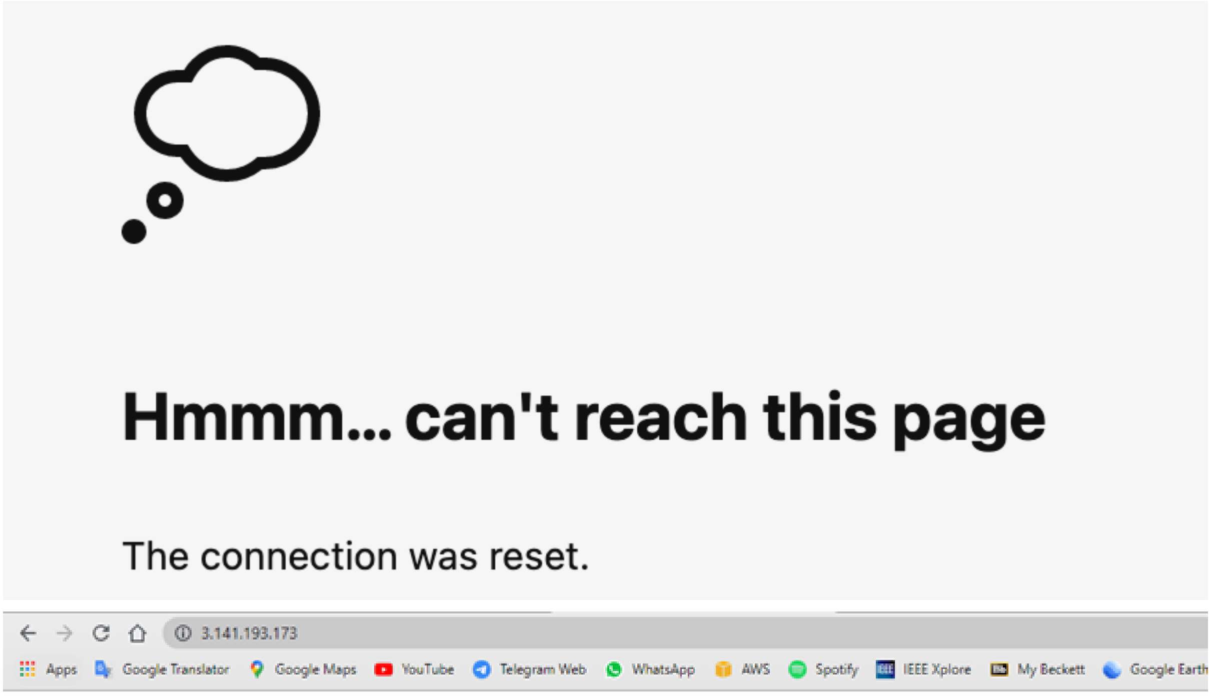
☐	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability Zone
☑	EC2_D7001D_Hamza	i-075f31f3d860acef3	Running	t2.micro	2/2 checks passed	No alarms +	us-east-2c
☐	EC2_D7001D_Hamza_2	i-0f6c24c304b18a1da	Running	t2.micro	2/2 checks passed	No alarms +	us-east-2c



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	First Instance	i-0450ff6c6b2d00e0a	Running	t2.micro	2/2 checks passed	No alarms
☑	delete-me-OtabekSobirov	i-00a61b27e03609c2a	Running	t2.micro	2/2 checks passed	No alarms
□	-	i-03f5d911e100c7c6e	Terminated	t2.micro	-	No alarms

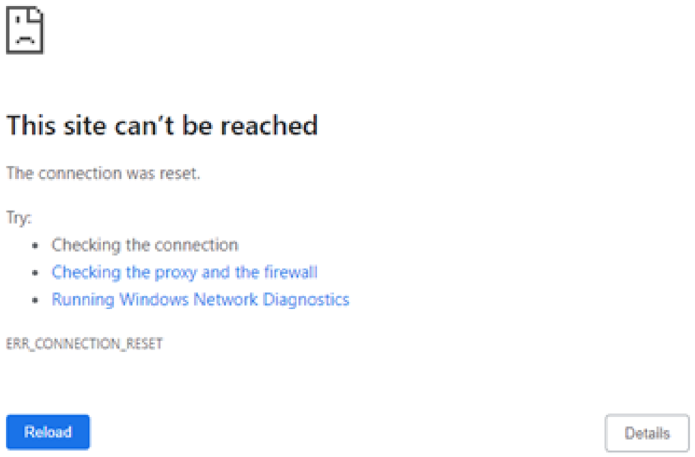
a. QUESTION 10. What was the server response?

This site can’t be reached.



Hmmm... can't reach this page

The connection was reset.



This site can’t be reached

The connection was reset.

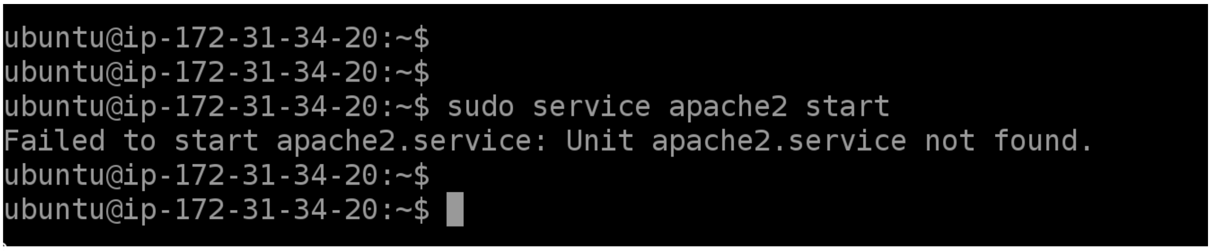
Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

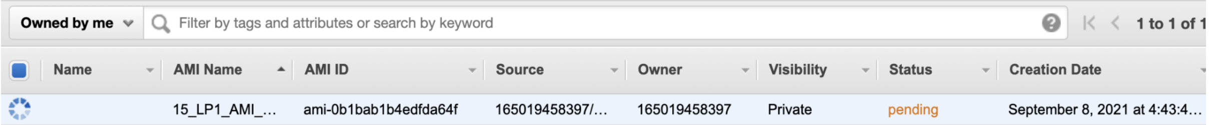
b. QUESTION 11. Explain why.

The new instance was created based on the hardware and platform specifications of the previous instance, but not the services installed in it. As this is not the image copy of the AMI. The previous instance acts like a template.

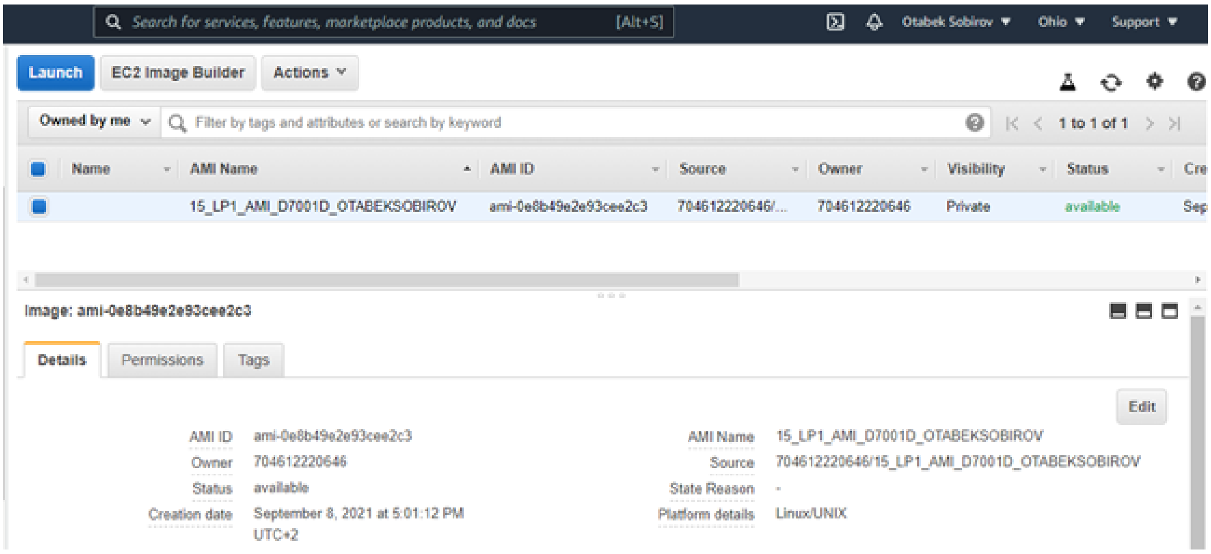


```
ubuntu@ip-172-31-34-20:~$
ubuntu@ip-172-31-34-20:~$
ubuntu@ip-172-31-34-20:~$ sudo service apache2 start
Failed to start apache2.service: Unit apache2.service not found.
ubuntu@ip-172-31-34-20:~$
ubuntu@ip-172-31-34-20:~$ 
```

9. Stop this instance and change the name of the instance to: “delete-me-username”. Now select the instance where your webserver is running and create AMI image 15_LP1_AMI_D7001D_YOURUSERNAME.



Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
	15_LP1_AMI_...	ami-0b1bab1b4edfda64f	165019458397/...	165019458397	Private	pending	September 8, 2021 at 4:43:4...


Search for services, features, marketplace products, and docs
[Alt+S]
Otabek Sobirov
Ohio
Support
Launch
EC2 Image Builder
Actions
Owned by me
Filter by tags and attributes or search by keyword
1 to 1 of 1

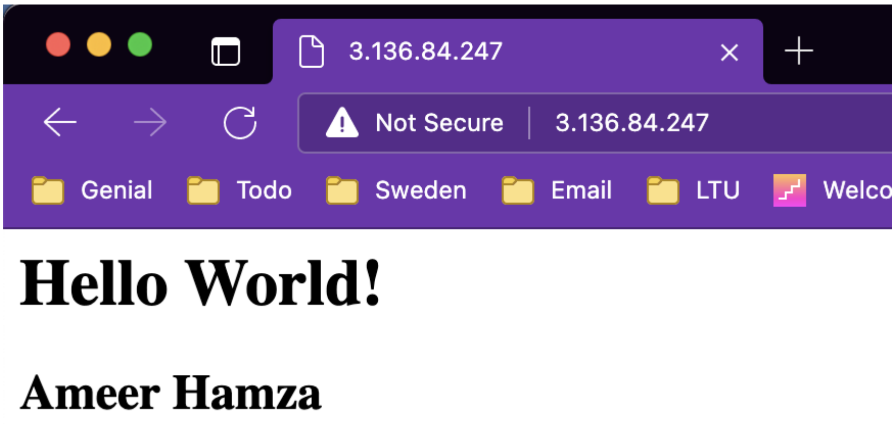
Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Cre
	15_LP1_AMI_D7001D_OTABEKSOBIROV	ami-0e8b49e2e93cee2c3	704612220646/...	704612220646	Private	available	Sep

Image: ami-0e8b49e2e93cee2c3

Details
Permissions
Tags
Edit

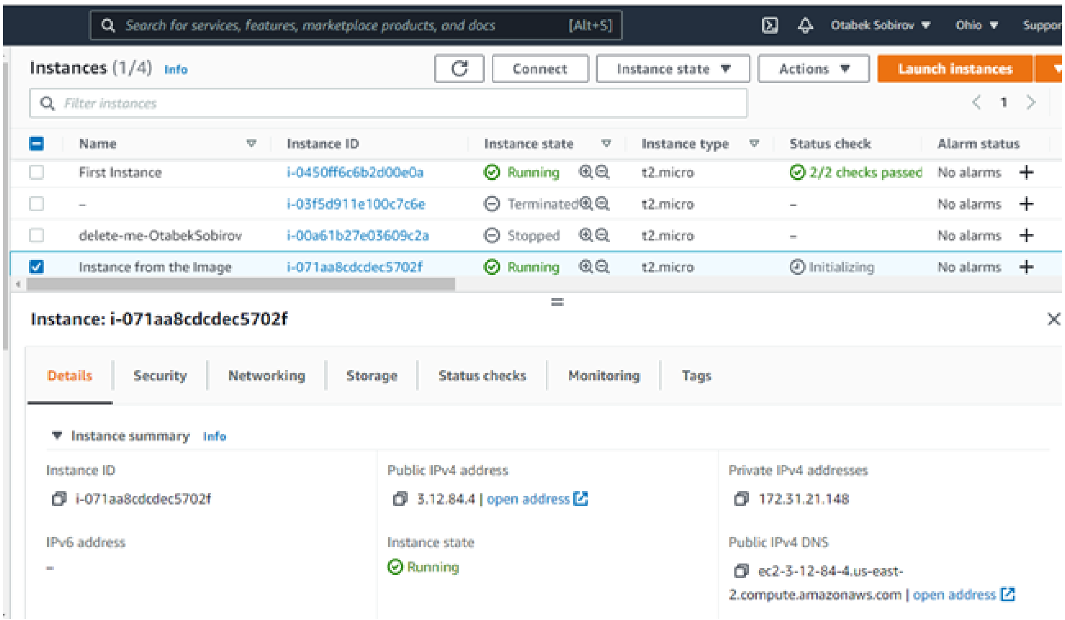
AMI ID	ami-0e8b49e2e93cee2c3	AMI Name	15_LP1_AMI_D7001D_OTABEKSOBIROV
Owner	704612220646	Source	704612220646/15_LP1_AMI_D7001D_OTABEKSOBIROV
Status	available	State Reason	-
Creation date	September 8, 2021 at 5:01:12 PM UTC+2	Platform details	Linux/UNIX

10. Launch a new instance from this image. Copy public dns and paste it to a web browser.



Hello World!

Ameer Hamza



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	First Instance	i-0450ff6c6b2d00e0a	Running	t2.micro	2/2 checks passed	No alarms
□	–	i-03f5d911e100c7c6e	Terminated	t2.micro	–	No alarms
□	delete-me-OtabekSobirov	i-00a61b27e03609c2a	Stopped	t2.micro	–	No alarms
☑	Instance from the Image	i-071aa8cdcdec5702f	Running	t2.micro	Initializing	No alarms

Instance: i-071aa8cdcdec5702f

Instance ID: i-071aa8cdcdec5702f

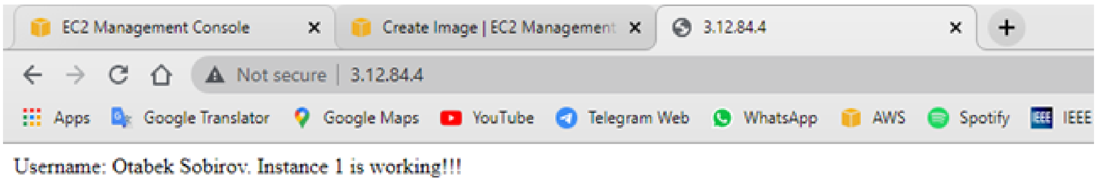
Public IPv4 address: 3.12.84.4 | open address

Private IPv4 addresses: 172.31.21.148

IPv6 address: –

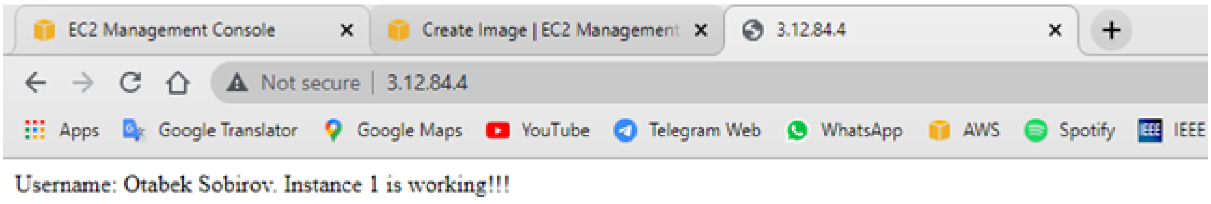
Instance state: Running

Public IPv4 DNS: ec2-3-12-84-4.us-east-2.compute.amazonaws.com | open address



Username: Otabek Sobirov. Instance 1 is working!!!

a. QUESTION 12. What was the server's response?
The web server is in operation. And we have the same webpage as instance 1.

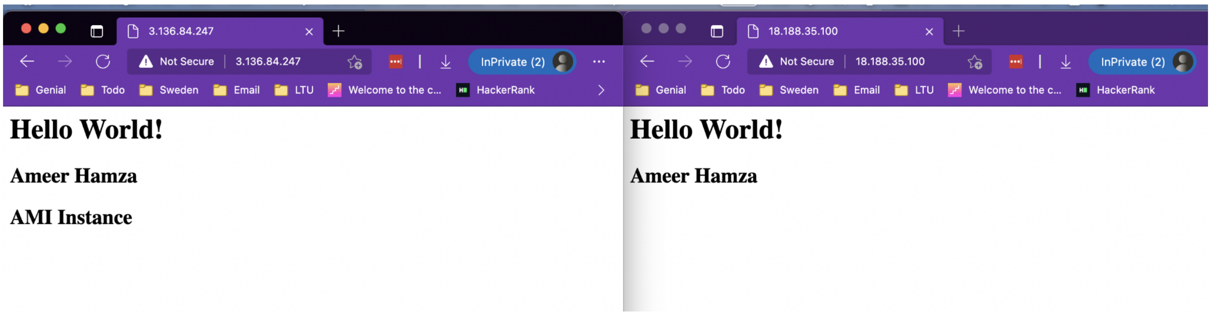


Username: Otabek Sobirov. Instance 1 is working!!!

b. QUESTION 13. Explain why.

Creating an Image(AMI) from the instance is copying a complete image of its disc. Therefore, the OS files and software programs are also stored in that image file.

11. Now edit /var/www/html/index.html and enter text so that you can distinguish this instance from others.



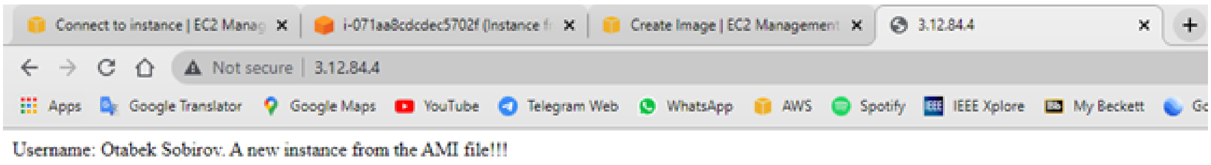
Hello World!

Ameer Hamza

AMI Instance

Hello World!

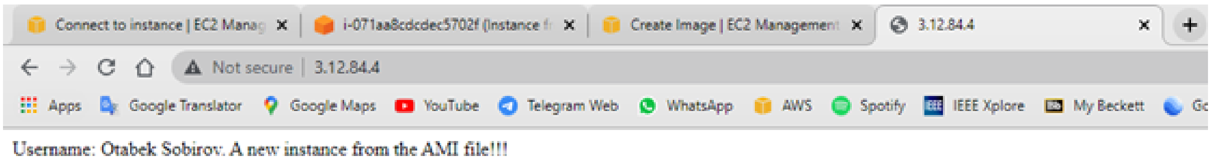
Ameer Hamza



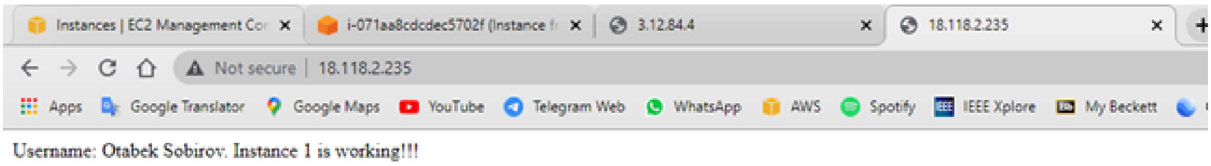
Username: Otabek Sobirov. A new instance from the AMI file!!!

12. Check the main web pages on both servers, where did the text change? Why?

The webpage of the second instance has only changed since it was edited. Webpage of the original instance remained unchanged as both instances are separate devices.



Username: Otabek Sobirov. A new instance from the AMI file!!!



Username: Otabek Sobirov. Instance 1 is working!!!

13. What will be displayed if you launch a new instance from your AMI?

The web page that is stored in the AMI file when the image file was created. (Not the web pages that have been modified in the previous two instances)

Part 3

14. Here is a simple scenario. Suppose you have created a server program to run on TCP port 4032. The remote machine on which you install it is accessible through the name myserv.mydomain.net. Next you install your server program and try to access it from a different computer. Your server is not responding!

a. QUESTION 14. Describe your step-by-step problem searching and troubleshooting approach.

b. QUESTION 15. Demonstrate your approach using appropriate operating system's commands and tools when troubleshooting communications between your local computer and running an AWS instance configured with the web server.

One answer for both questions 14 and 15:

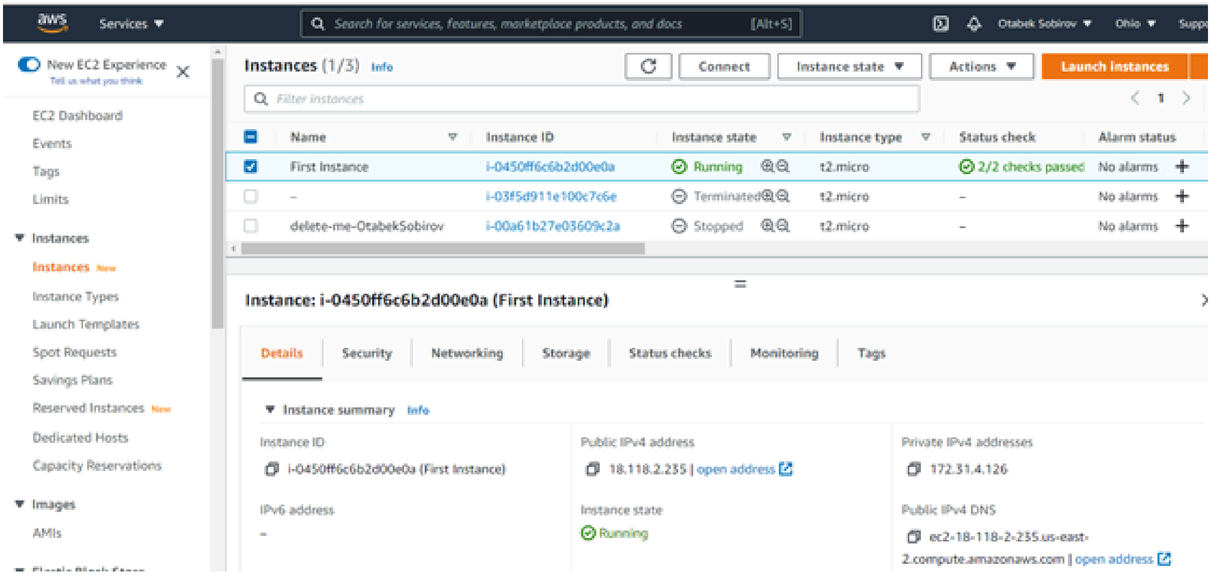
The best troubleshooting approach would be to check from the bottom to the top (OSI model layers: Physical, DataLink, Network and Transport).

1. We need to check if our laptop is connected to the local network properly.
2. Then we need to check the Internet connection of our laptop by trying to reach any web servers on the internet.
3. Then we will ping to our remote server from our laptop. (If pings fail, we use the command "tracert IP_of_remote_server" on Windows or traceroute on Linux-based OS to check how far or till where our pings are going)

4. If pings are successful, it means there is no problem in the first three layers.
5. We should check the security group that our instance belongs to. If there is a rule to block TCP port 4032, we need to change it.
6. If there is no rule, we should use Wireshark software tool to analyze the packet probes exchanged between the web server and our local laptop.
7. We need to check two packets on both sides: Request and Response. Scenarios:
    - a. In our local laptop, the request packet is sent and not received on the server. It means either This port is blocked for **outbound traffic** on the gateway of the local network of our laptop or it is blocked for **inbound traffic** on the firewall of Server.
    - b. Request packet is received on the server and Response packet is sent, but not received on our laptop. It means either the TCP port 4032 is blocked for **inbound traffic** on the gateway of the local network of our laptop or it is blocked for **outbound traffic** on the firewall of Server.

15. Set up wireshark (tshark) on one of the instances and locally on your computer (http://shieldroute.blogspot.se/2012/08/wireshark-on-aws-ec2.html). Start monitoring traffic.

a. QUESTION 16. Be able to interpret and explain the information about different protocols, their fields etc.



Instances (1/3)

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	First Instance	i-0450ff6c6b2d00e0a	Running	t2.micro	2/2 checks passed	No alarms
☐	-	i-03f5d911e100c7c6e	Terminated	t2.micro	-	No alarms
☐	delete-me-OtabekSobirov	i-00a61b27e03609c2a	Stopped	t2.micro	-	No alarms

Instance: i-0450ff6c6b2d00e0a (First Instance)

▼ Instance summary

Instance ID: i-0450ff6c6b2d00e0a (First Instance)

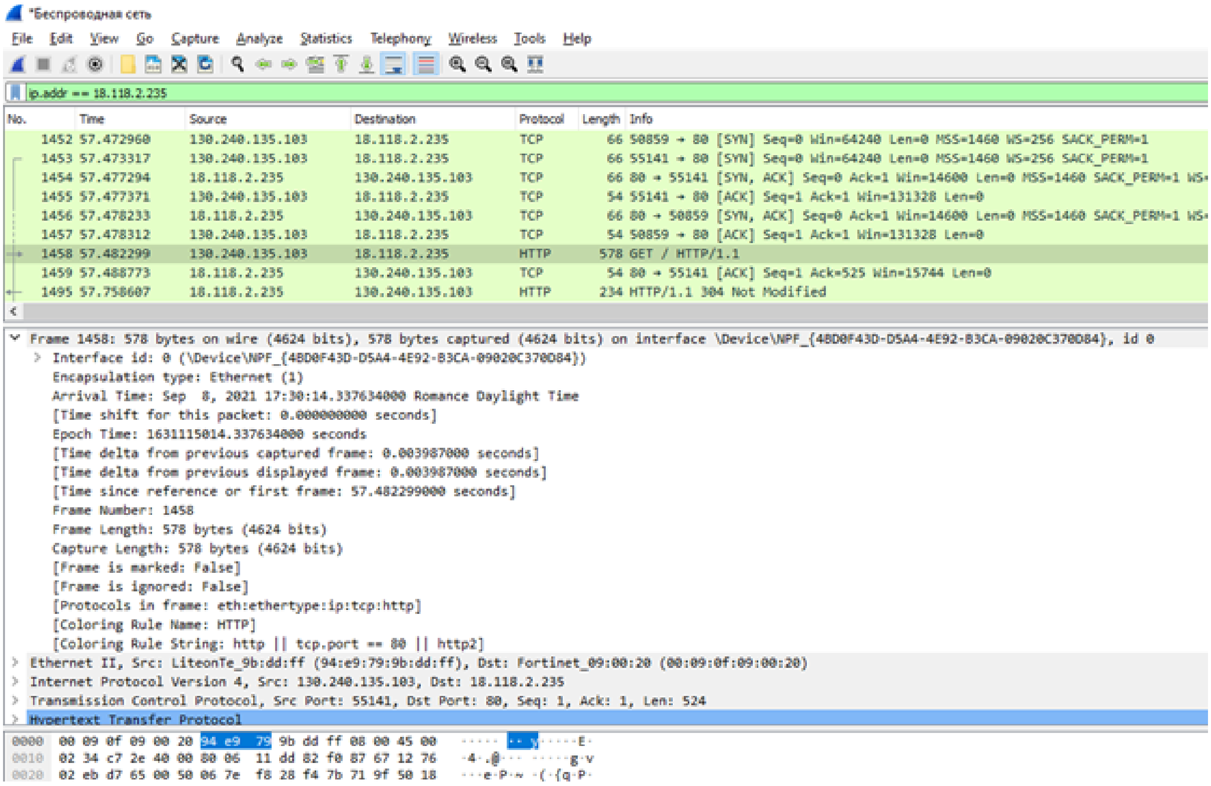
Public IPv4 address: 18.118.2.235 | open address

Private IPv4 addresses: 172.31.4.126

IPv6 address: -

Instance state: Running

Public IPv4 DNS: ec2-18-118-2-235.us-east-2.compute.amazonaws.com | open address



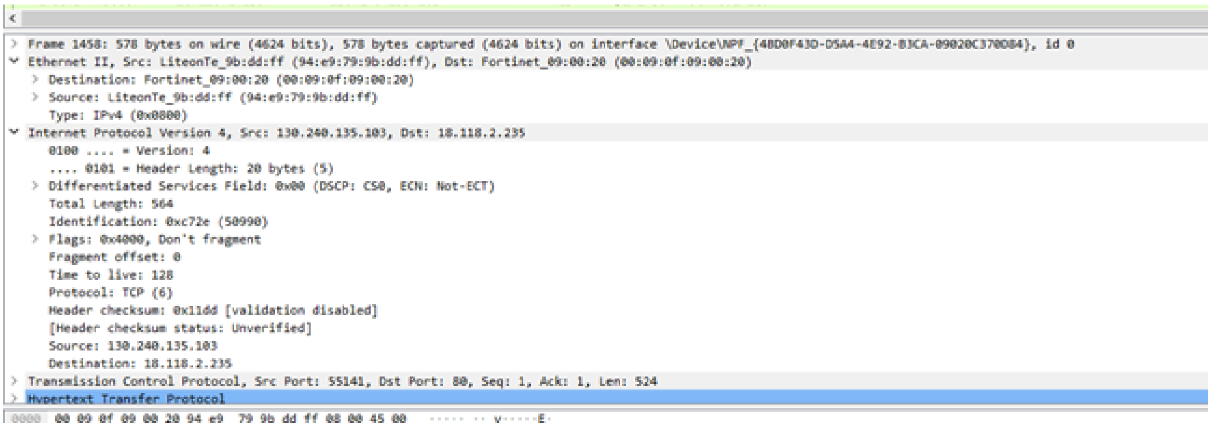
*Беспроводная сеть
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 18.118.2.235
```

```
No.    Time          Source            Destination       Protocol  Length Info
  1452 57.472960     130.240.135.103   18.118.2.235      TCP        66 50859 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  1453 57.473317     130.240.135.103   18.118.2.235      TCP        66 55141 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  1454 57.477294     18.118.2.235      130.240.135.103   TCP        66 80 → 55141 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=
  1455 57.477371     130.240.135.103   18.118.2.235      TCP        54 55141 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  1456 57.478233     18.118.2.235      130.240.135.103   TCP        66 80 → 50859 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=
  1457 57.478312     130.240.135.103   18.118.2.235      TCP        54 50859 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  1458 57.482299     130.240.135.103   18.118.2.235      HTTP      578 GET / HTTP/1.1
  1459 57.488773     18.118.2.235      130.240.135.103   TCP        54 80 → 55141 [ACK] Seq=1 Ack=525 Win=15744 Len=0
  1495 57.758607     18.118.2.235      130.240.135.103   HTTP      234 HTTP/1.1 304 Not Modified
```

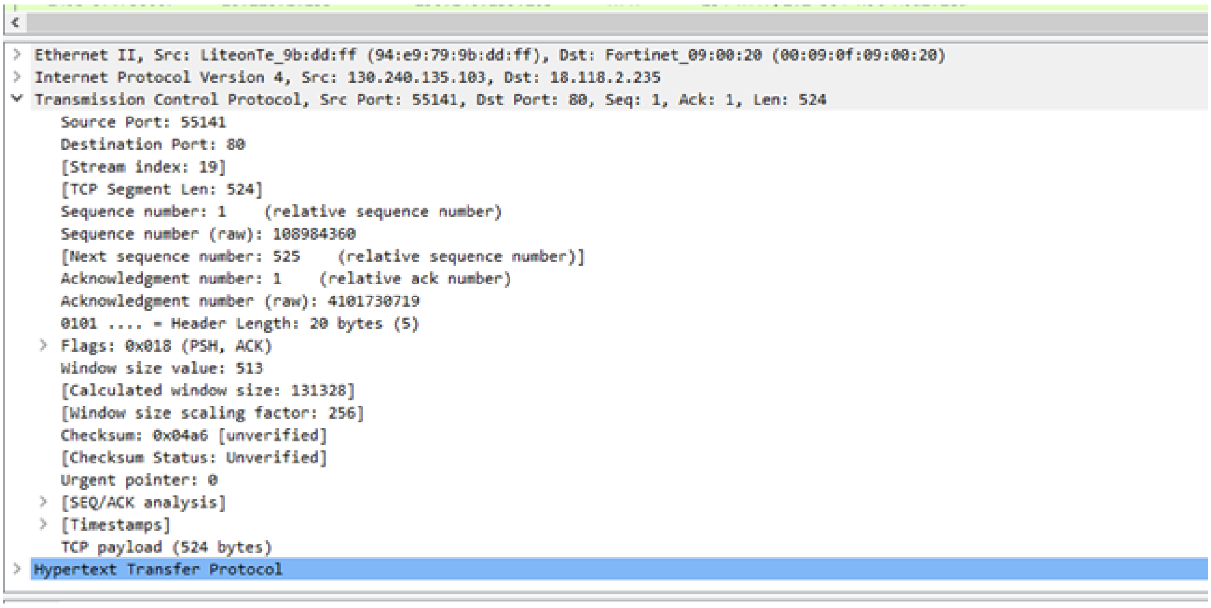
```
v Frame 1458: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{48D0F43D-D5A4-4E92-83CA-09020C370D84}, id 0
  > Interface id: 0 (\Device\NPF_{48D0F43D-D5A4-4E92-83CA-09020C370D84})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  8, 2021 17:30:14.337634000 Romance Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1631115014.337634000 seconds
    [Time delta from previous captured frame: 0.003987000 seconds]
    [Time delta from previous displayed frame: 0.003987000 seconds]
    [Time since reference or first frame: 57.482299000 seconds]
    Frame Number: 1458
    Frame Length: 578 bytes (4624 bits)
    Capture Length: 578 bytes (4624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: LiteonTe_9b:dd:ff (94:e9:79:9b:dd:ff), Dst: Fortinet_09:00:20 (00:09:0f:09:00:20)
> Internet Protocol Version 4, Src: 130.240.135.103, Dst: 18.118.2.235
> Transmission Control Protocol, Src Port: 55141, Dst Port: 80, Seq: 1, Ack: 1, Len: 524
> Hypertext Transfer Protocol
```

```
0000  00 09 0f 09 00 20 94 e9  79 9b dd ff 08 00 45 00   ····· ·· y·····E·
0010  02 34 c7 2e 40 00 80 06  11 dd 82 f0 87 67 12 76   ·4·.@··· ·····g·v
0020  02 eb d7 65 00 50 06 7e  f8 28 f4 7b 71 9f 50 18   ···e·P·~ ·(·{q·P·
```

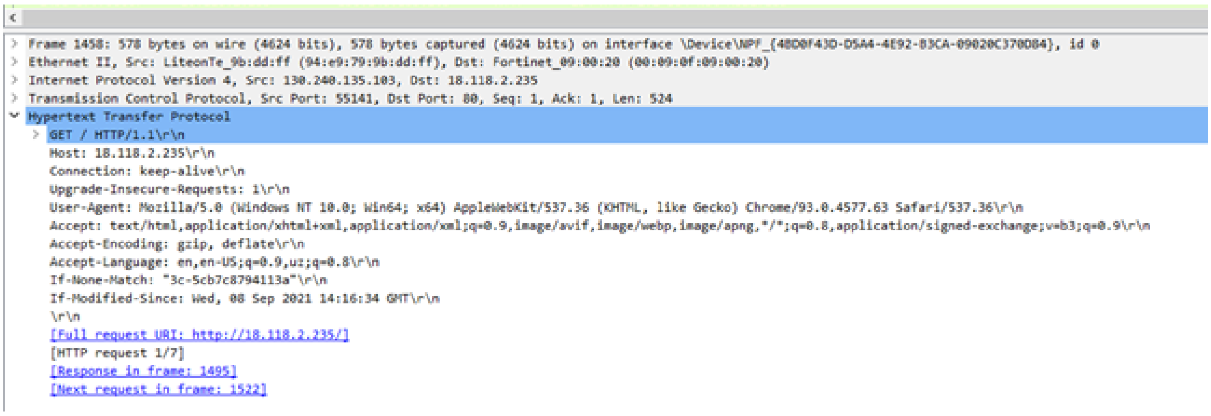


```
> Frame 1458: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{48D0F43D-D5A4-4E92-83CA-09020C370D84}, id 0
v Ethernet II, Src: LiteonTe_9b:dd:ff (94:e9:79:9b:dd:ff), Dst: Fortinet_09:00:20 (00:09:0f:09:00:20)
  > Destination: Fortinet_09:00:20 (00:09:0f:09:00:20)
  > Source: LiteonTe_9b:dd:ff (94:e9:79:9b:dd:ff)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 130.240.135.103, Dst: 18.118.2.235
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 564
    Identification: 0xc72e (50990)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x11dd [validation disabled]
    [Header checksum status: Unverified]
    Source: 130.240.135.103
    Destination: 18.118.2.235
> Transmission Control Protocol, Src Port: 55141, Dst Port: 80, Seq: 1, Ack: 1, Len: 524
> Hypertext Transfer Protocol
```

```
0000  00 09 0f 09 00 20 94 e9  79 9b dd ff 08 00 45 00   ····· ·· y·····E·
```



```
> Ethernet II, Src: LiteonTe_9b:dd:ff (94:e9:79:9b:dd:ff), Dst: Fortinet_09:00:20 (00:09:0f:09:00:20)
> Internet Protocol Version 4, Src: 130.240.135.103, Dst: 18.118.2.235
v Transmission Control Protocol, Src Port: 55141, Dst Port: 80, Seq: 1, Ack: 1, Len: 524
    Source Port: 55141
    Destination Port: 80
    [Stream index: 19]
    [TCP Segment Len: 524]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 108984360
    [Next sequence number: 525    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 4101730719
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x04a6 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (524 bytes)
> Hypertext Transfer Protocol
```



```
> Frame 1458: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{48D0F43D-D5A4-4E92-83CA-09020C370D84}, id 0
> Ethernet II, Src: LiteonTe_9b:dd:ff (94:e9:79:9b:dd:ff), Dst: Fortinet_09:00:20 (00:09:0f:09:00:20)
> Internet Protocol Version 4, Src: 130.240.135.103, Dst: 18.118.2.235
> Transmission Control Protocol, Src Port: 55141, Dst Port: 80, Seq: 1, Ack: 1, Len: 524
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: 18.118.2.235\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en,en-US;q=0.9,uz;q=0.8\r\n
    If-None-Match: "3c-5cb7c8794113a"\r\n
    If-Modified-Since: Wed, 08 Sep 2021 14:16:34 GMT\r\n
    \r\n
    [Full request URI: http://18.118.2.235/]
    [HTTP request 1/7]
    [Response in frame: 1495]
    [Next request in frame: 1522]
```

In order to analyse the different packets and protocols we captured the packets between the remote (aws machine) and our local machine.

We chose one http packet request from the client side and analyzed it based on the OSI model.

Data link layer: It has the mac protocol. Mac protocol header has the following important fields: source and destination mac address, upper layer protocol fields. At this layer all the data from the upper layer will be encapsulated into frames.

Network Layer: At this layer we have the IP protocol and the data is encapsulated into packets: IP protocol header has the following important fields:

1. Source IP Address: 32 bits
2. Destination IP Address: 32 bits
3. Type field: IP version e.g. IPV4.
4. TTL: TIme to live: It defines the lifespan of the packets
5. Length: Size of the packet.

Transport Layer: It defines the transmission protocol such as UDP or TCP. Also it contains the information about source and destination port numbers. Data here is encapsulated into segments.

Application Layer: At this layer we have the user data which is transmitted. For this request packet HTTP protocol was used as shown in the wireshark screenshot.