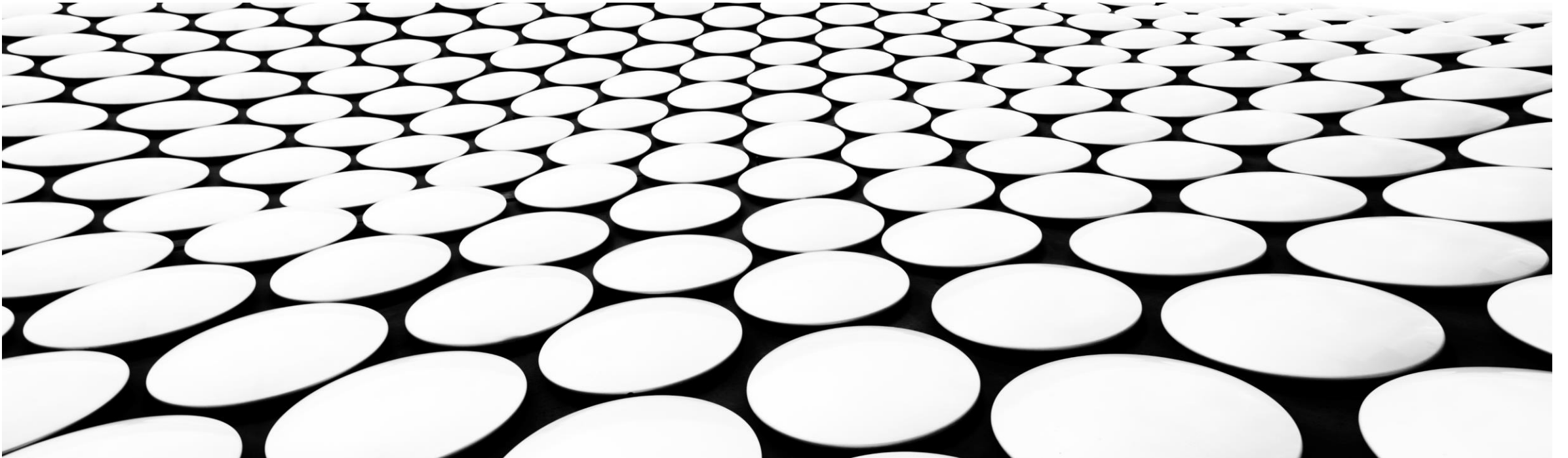


---

# INTRODUCTION TO CLOUD COMPUTING

BY NIRAL PATEL JANUARY 2021





# INTRODUCTION

- In today world we want to access everything from our phone and faster. Cloud computing is one of the best way to do that. Cloud Provide like AWS they do provide good amount of security and alert. In amazon alert we have custom option that we can choose from. In this class I learn
- How to set up my cloud computing
- How to access them remotely
- Setup security and alert setting



# AMAZON WEB SERVICE ACCOUNT

- Creat AWS service account.
- Creating an IAM user
- Set permissions : Administrator Access
- How to download .csv file with credentials of newly created user.



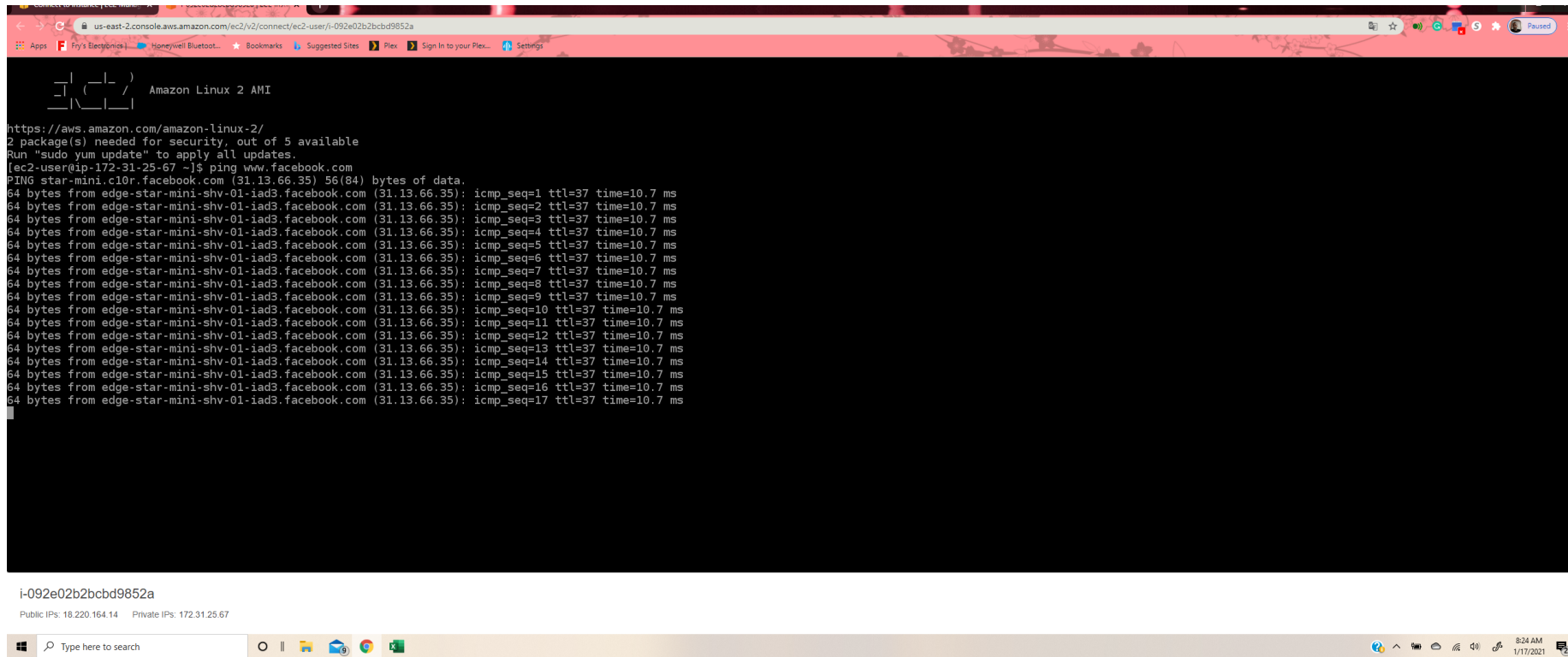
# VIRTUAL MACHINE (VM) INSTANCES

- Launching an EC2 instance
- Connecting to the instance
- Terminating the instance

# LAUNCHING AN EC2 INSTANCE

Details	Security	Networking	Storage	Monitoring	Tags
<b>▼ Instance details</b> <a href="#">Info</a>					
Platform Amazon Linux (Inferred)	AMI ID ami-0a0ad6b70e61be944	Monitoring disabled			
Platform details Linux/UNIX	AMI name amzn2-ami-hvm-2.0.20201218.1-x86_64-gp2	Termination protection Enabled			
Launch time Sun Jan 24 2021 18:07:44 GMT-0600 (Central Standard Time) (less than a minute)	AMI location amazon/amzn2-ami-hvm-2.0.20201218.1-x86_64-gp2	Lifecycle normal			
Stop-hibernate behavior disabled	AMI Launch index 0	Key pair name -			
State transition reason -	Credit specification standard	Kernel ID -			
State transition message -	Usage operation RunInstances	RAM disk ID -			
Owner 441096058823	Enclaves Support -				
<b>▼ Host and placement group</b> <a href="#">Info</a>					
Host ID -	Affinity -	Placement group -			
Host resource group name -	Tenancy default	Partition number -			
Virtualization type hvm	Reservation r-0629c44c3afd6a607	Number of vCPUs 1			
<b>▼ Capacity reservation</b> <a href="#">Info</a>					
Capacity Reservation ID -	Capacity Reservation setting open				
<b>▼ Accelerators</b> <a href="#">Info</a>					
Elastic Graphics ID -	Elastic inference accelerator ID -				

# CONNECTING TO THE INSTANCE



The screenshot shows a terminal window within the AWS Management Console. The terminal displays the following text:

```
Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 5 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-25-67 ~]$ ping www.facebook.com
PING star-mini.c10r.facebook.com (31.13.66.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=1 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=2 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=3 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=4 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=5 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=6 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=7 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=8 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=9 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=10 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=11 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=12 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=13 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=14 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=15 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=16 ttl=37 time=10.7 ms
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=17 ttl=37 time=10.7 ms
```

Below the terminal output, the instance ID `i-092e02b2bccbd9852a` is visible, along with public and private IP addresses: `Public IPs: 18.220.164.14 Private IPs: 172.31.25.67`. The bottom of the screenshot shows the Windows taskbar with the search bar and system tray.

# TERMINATING THE INSTANCE

The screenshot shows the AWS Management Console interface for EC2 instances. A notification banner at the top reads: "Welcome to the new instances experience! We're redesigning the EC2 console to make it easier to use. To switch between the old console and the new console, use the New EC2 Experience toggle above the navigation panel. We'll release updates continuously based on customer feedback." Below the banner, the "Instances (1)" section is active, displaying a table with one instance. The instance is in a "Terminated" state. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4..., Elastic IP, IPv6 IPs, Monitoring, Security group name, and Key name. Below the table, there is a prompt: "Select an instance above".

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name
-	i-092e02b2bcd9852a	Terminated	t2.micro	-	No alarms +	us-east-2b	-	18.220.164.14	-	-	disabled	-	-



# VIRTUAL PRIVATE CLOUD

- In this project I Learn about Virtual Private Cloud. This service allows customer to provision a logically isolated section of the AWS cloud, and launch AWS resources into a virtual network.
- Task completed in this projects
  - Launching VPC with a single subnet
  - Viewing subnets and route tables
  - Adding another subnet



# LAUNCHING VPC WITH A SINGLE SUBNET

The screenshot displays the AWS IAM console interface for managing Virtual Private Clouds (VPCs). At the top, there's a header 'Your VPCs (1/2)' with a search bar and a 'Create VPC' button. Below this is a table listing VPCs. The first VPC, 'Netw211-VPC', is selected and its details are shown in a panel below. The details panel includes tabs for 'Details', 'CIDRs', 'Flow logs', and 'Tags'. The 'Details' tab is active, showing various configuration parameters for the VPC.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool
Netw211-VPC	vpc-07fe6fb12362d7648	Available	192.168.0.0/24	-	-
-	vpc-fd398396	Available	172.31.0.0/16	-	-

**vpc-07fe6fb12362d7648 / Netw211-VPC**

**Details**

VPC ID vpc-07fe6fb12362d7648	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-8bb32ce0	Route table rtb-041a5642f4a600512	Network ACL acl-034c400b21a2e892e
Default VPC No	IPv4 CIDR 192.168.0.0/24	IPv6 pool -	IPv6 CIDR -
Owner ID 441096058823			

# QUESTIONS

- 1. With a /26 network prefix, how many usable IPv4 addresses are there? Why is the number of available IPv4 addresses HERE shown as 59?
- Answer here: total available IPv4 is 62 out of that 3 reserved by AWS.
- 1 for AWS for the VPC ROUTER.
- 2. FOR DNS server
- 3. For the future use.
- 2. What's the role of an Internet Gateway?
- Answer here: it serves 2 purpose.
- 1. It perform network address translation
- 2. Provide a target in your vpc rout tables for internet-routable traffic
- References:
- 1. [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Subnets.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)
- 2. [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

# ADDING ANOTHER SUBNET

The screenshot shows the AWS Management Console interface for Subnets in the us-east-2 region. The left sidebar contains navigation options for VPC, Security, Reachability, and Transit. The main content area displays a list of subnets, with 'Public Subnet 2' selected. Below the list, the details for 'Public Subnet 2' are shown, including its route table 'rtb-0c3ca68ab9390974e' and its routes.

**Subnets (1/5)**

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
-	subnet-3b743777	Available	vpc-fd398396	172.31.32.0/20	-
-	subnet-0f10b264	Available	vpc-fd398396	172.31.0.0/20	-
Public Subnet 2	subnet-05b92c68343015940	Available	vpc-07fe6fb12362d7648   Net...	192.168.0.64/26	-
-	subnet-e37e6599	Available	vpc-fd398396	172.31.16.0/20	-
Public subnet 1	subnet-0f2c2828eccc9d0a0	Available	vpc-07fe6fb12362d7648   Net...	192.168.0.0/26	-

**subnet-05b92c68343015940 / Public Subnet 2**

Details | Flow logs | **Route table** | Network ACL | Tags | Sharing

Route table: **rtb-0c3ca68ab9390974e** [Edit route table association](#)

**Routes (2)**

Destination	Target
192.168.0.0/24	local
0.0.0.0/0	igw-0835ef2206be14ab4

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use



# VM INSTANCE SECURITY

- In this I explore 2 techniques used to secure AWS EC2 instances: setting up security group to control inbound and outbound traffic of an instance.
- Tasks to be completed:
  - Launching an EC2 instance
  - Connecting to the instance using a key pair
  - Setting up a security group

# LAUNCHING AN EC2 INSTANCE

The screenshot displays the AWS Management Console interface for an EC2 instance. The top navigation bar includes the AWS logo, a search bar, and user information. The left sidebar contains a navigation menu with categories like 'New EC2 Experience', 'Instances', 'Images', 'Elastic Block Store', 'Network & Security', 'Load Balancing', and 'Auto Scaling'. The main content area shows the 'Instance summary for i-04b84e0b7ba0b47ec', which is currently in a 'Running' state. Below the summary, there are tabs for 'Details', 'Security', 'Networking', 'Storage', 'Monitoring', and 'Tags'. The 'Details' tab is active, showing a grid of instance attributes such as Platform (Amazon Linux), AMI ID, Launch time, and Instance type (t2.micro).

**Instance summary for i-04b84e0b7ba0b47ec** Info  
Updated less than a minute ago

Instance ID i-04b84e0b7ba0b47ec	Public IPv4 address 18.216.177.188   <a href="#">open address</a>	Private IPv4 addresses 192.168.0.12
Instance state Running	Public IPv4 DNS ec2-18-216-177-188.us-east-2.compute.amazonaws.com   <a href="#">open address</a>	Private IPv4 DNS ip-192-168-0-12.us-east-2.compute.internal
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-07fe6fb12362d7648 (Netw211-VPC)
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.   <a href="#">Learn more</a>	IAM Role -	Subnet ID subnet-0f2c2828e0e9d0a0 (Public subnet 1)

**Instance details** Info

Platform Amazon Linux (Inferred)	AMI ID ami-01aab85a5e4a5a0fe	Monitoring disabled
Platform details Linux/UNIX	AMI name amzn2-ami-hvm-2.0.20210126.0-x86_64-gp2	Termination protection Disabled
Launch time Sat Jan 30 2021 18:32:23 GMT-0600 (Central Standard Time) (6 minutes)	AMI location amazon/amzn2-ami-hvm-2.0.20210126.0-x86_64-gp2	Lifecycle normal
Stop-hibernate behavior disabled	AMI Launch index 0	Key pair name netw211- project-ec2
State transition reason -	Credit specification standard	Kernel ID -
State transition message -	Usage operation RunInstances	RAM disk ID -

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

# CONNECTING TO THE INSTANCE USING A KEY PAIR

```
ec2-user@ip-192-168-0-12:~  
└─$ Using username "ec2-user".  
└─$ Authenticating with public key "imported-openssh-key"  
  
_ | _ | )  
_ | ( _ | /  Amazon Linux 2 AMI  
_ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-192-168-0-12 ~]$ ipconfig  
-bash: ipconfig: command not found  
[ec2-user@ip-192-168-0-12 ~]$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001  
    inet 192.168.0.12 netmask 255.255.255.192 broadcast 192.168.0.63  
    inet6 fe80::45a:b5ff:fe6e:9408 prefixlen 64 scopeid 0x20<link>  
    ether 06:5a:b5:6e:94:08 txqueuelen 1000 (Ethernet)  
    RX packets 36792 bytes 53094716 (50.6 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 9653 bytes 583246 (569.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 648 (648.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 648 (648.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[ec2-user@ip-192-168-0-12 ~]$ ping -c 4 www.facebook.com  
PING star-mini.cl0r.facebook.com (31.13.66.35) 56(84) bytes of data.  
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=1  
ttl=37 time=10.8 ms  
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=2  
ttl=37 time=11.0 ms  
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=3  
ttl=37 time=10.9 ms  
64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp_seq=4  
ttl=37 time=11.0 ms  
  
--- star-mini.cl0r.facebook.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 10.893/10.989/11.047/0.096 ms  
[ec2-user@ip-192-168-0-12 ~]$
```

# SETTING UP A SECURITY GROUP

- The local computer to the instance in the cloud.

```
CA. Command Prompt
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\niral>PING 18.216.177.188

Pinging 18.216.177.188 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 18.216.177.188:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\niral>PING 18.216.177.188

Pinging 18.216.177.188 with 32 bytes of data:
Reply from 18.216.177.188: bytes=32 time=43ms TTL=221
Reply from 18.216.177.188: bytes=32 time=69ms TTL=221
Reply from 18.216.177.188: bytes=32 time=38ms TTL=221
Reply from 18.216.177.188: bytes=32 time=35ms TTL=221

Ping statistics for 18.216.177.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 69ms, Average = 46ms

C:\Users\niral>
```



# CLOUD STORAGE

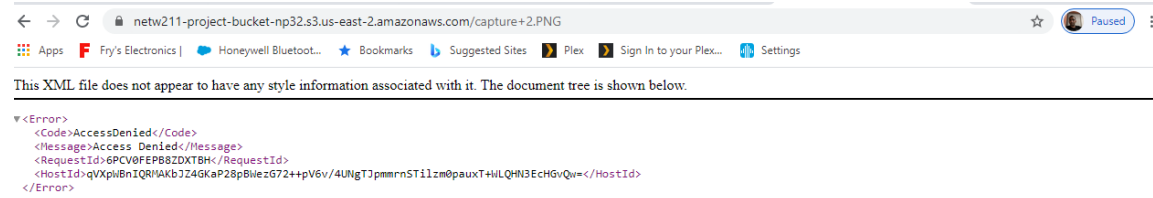
- I explore Amazon's simple storage service (S3). S3 is an object storage service used to store and protect data for use cases such as mobile applications, websites, Backups, IoT device, and big data analytics.
- Task I did
  - Creating an S3 bucket
  - Uploading a file
  - Changing file and bucket permissions
  - Removing the file



# QUESTION

- What does the default encryption do?
- Answer here: encryption Encrypt the file. It's type of data security. it will make harder to read content of the file or data.
- Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket
- References:
- 1. <https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html>

# UPLOADING A FILE



The screenshot shows a web browser window with the address bar containing the URL `netw211-project-bucket-np32.s3.us-east-2.amazonaws.com/capture+2.PNG`. The browser's address bar includes navigation icons (back, forward, refresh) and a star icon for bookmarks. Below the address bar, there are several tabs: 'Apps', 'Fry's Electronics', 'Honeywell Bluetooth...', 'Bookmarks', 'Suggested Sites', 'Plex', 'Sign In to your Plex...', and 'Settings'. The main content area of the browser displays an error message: 'This XML file does not appear to have any style information associated with it. The document tree is shown below.' Below this message, the XML document tree is displayed in a collapsed state, showing the following structure:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>6PCV0FEPB8ZXTBH</RequestId>
  <HostId>qVXpIhBnIQRhAKbJZ4GKaP28pBilezG72++pV6v/4UNgTJpmmrnSTilzm0pauXT+ILQHNECHGvQw</HostId>
</Error>
```

# CHANGING PERMISSIONS

The screenshot shows the AWS S3 console interface. The browser address bar indicates the URL: `s3.console.aws.amazon.com/s3/object/netw211-project-bucket-np32?region=us-east-2&prefix=capture+2.PNG&tab=permissions`. The AWS navigation bar is visible at the top, and a sidebar on the left lists various S3 services. A notification banner at the top of the console area states: "We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose **Provide feedback**."

The main content area displays the object "capture 2.PNG" with a breadcrumb path: "Amazon S3 > netw211-project-bucket-np32 > capture 2.PNG". There are buttons for "Copy S3 URI" and "Object actions". Below this, there are tabs for "Properties", "Permissions", and "Versions", with "Permissions" selected.

The "Access control list (ACL)" section is expanded, showing a table of permissions. The table has columns for "Grantee", "Object", and "Object ACL".

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: <code>ca5b80f1043f0b649a217c3254b8afc5cf53aad53351f22f9720cbe8d8aa1eb1</code>	Read	Read, Write
Everyone (public access) Group: <code>http://acs.amazonaws.com/groups/global/AllUsers</code>	<span style="color: red;">⚠ Read</span>	-
Authenticated users group (anyone with an AWS account) Group: <code>http://acs.amazonaws.com/groups/global/AuthenticatedUsers</code>	-	-

At the bottom of the console, there is a footer with "Feedback", "English (US)", and copyright information: "© 2008 - 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".



# CLOUD MONITORING

- I learn Amazon SNS( simple Notification Service ), managed pub/sub message service, and amazon cloudwatch, a monitoring and management service.
- Task to need to completed
  - Launching an EC2 instance
  - Setting up SNS notification and subscription
  - Setting up a cloudwatch alarm
  - Deleting cloud resources

# LAUNCHING AN EC2 INSTANCE

**Instance summary for i-06fdc97f684c7b9d2** [Info](#)  
Updated less than a minute ago

[Refresh](#) [Connect](#) [Instance state ▼](#)

Instance ID i-06fdc97f684c7b9d2	Public IPv4 address 52.15.185.125   <a href="#">open address</a>	Private IPv4 addresses 172.31.45.33
Instance state Running	Public IPv4 DNS ec2-52-15-185-125.us-east-2.compute.amazonaws.com	Private IPv4 DNS ip-172-31-45-33.us-east-2.compute.internal

```
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

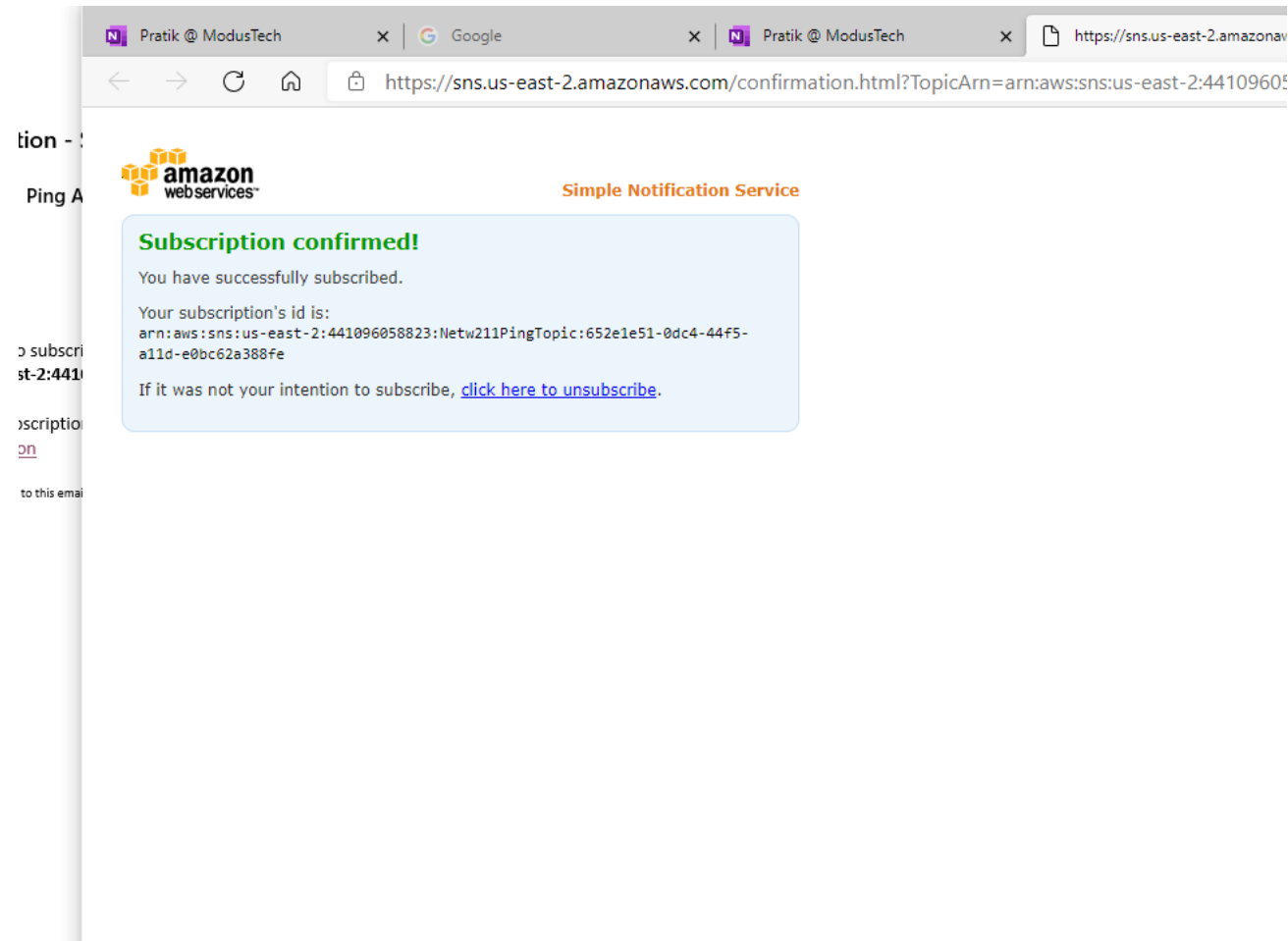
C:\Users\niral>ping 52.15.185.125

Pinging 52.15.185.125 with 32 bytes of data:
Reply from 52.15.185.125: bytes=32 time=51ms TTL=223
Reply from 52.15.185.125: bytes=32 time=45ms TTL=223
Reply from 52.15.185.125: bytes=32 time=36ms TTL=223
Reply from 52.15.185.125: bytes=32 time=51ms TTL=223

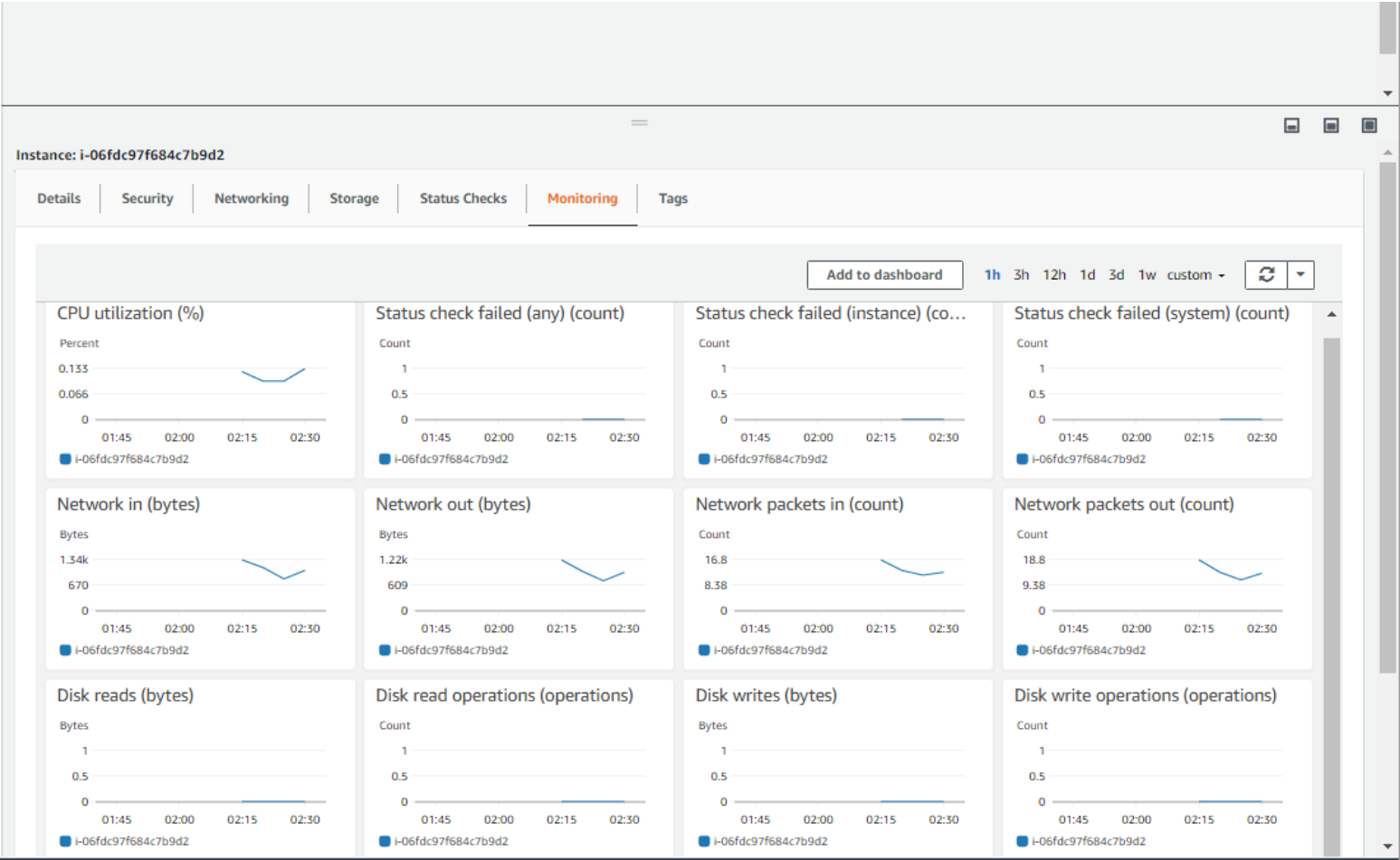
Ping statistics for 52.15.185.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 51ms, Average = 45ms

C:\Users\niral>
```

# SETTING UP SNS NOTIFICATION AND SUBSCRIPTION



# SETTING UP A CLOUDWATCH ALARM AND MONITORING





## CHALLENGES/ SKILLS

- In class I had some challenges when AWS change some interface.
- Some time remotely accessing the cloud using ping
  
- I learn how to set up cloud
- I learn how to setup remote access cloud.
- How to cancel the cloud
- How to encrypted the data file
- How to setup alerts on important data.





# CONCLUSION

- In this class I learn, I learn how to create amazon account, launching an EC2 instance connect to it. Adding another subnet and viewing subnets, connecting to instance using a key par and setting up key pair. Now I can create my storage cloud and keep data safe. And how to make it secure and keep it safe. Create a Bucket and upload my personal files. Change permissions who can get access to it. And setup an monitor and setup email alert for as soon as some one get access to my data.