

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

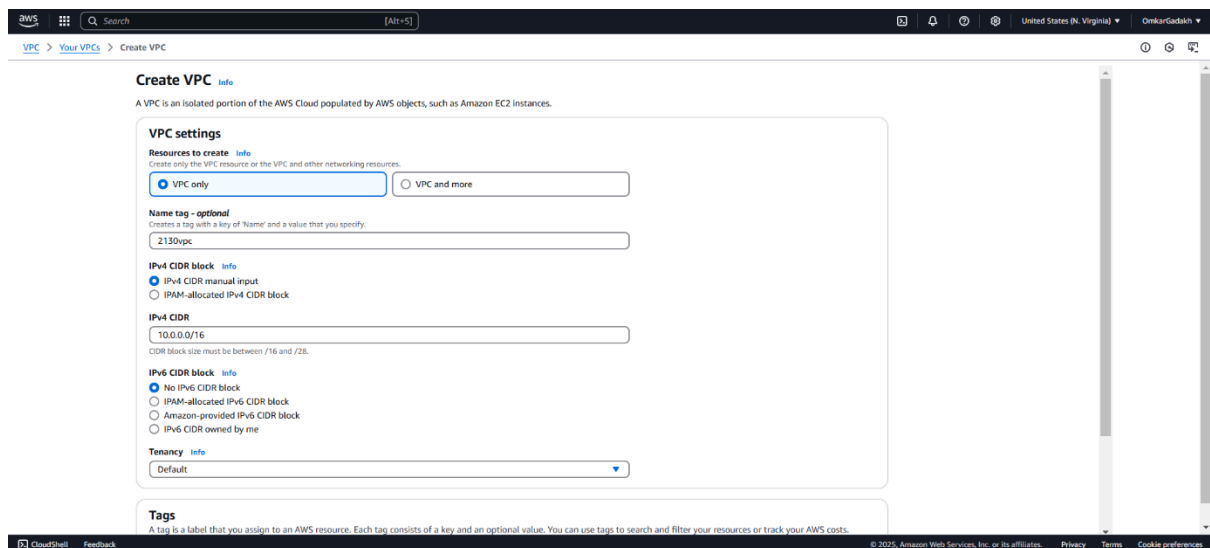
Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

Step 1: Create a VPC and attach an Internet Gateway

- Go to the Amazon Console and search for “VPC”.
- Select the VPC option.
- In the VPC settings, select the VPC only and assign an appropriate name to VPC as “2130VPC”.
- Choose IPV4 CIDR **manual input** and enter the CIDR block for VPC as “10.0.0.0/16”.
- Click on “No IPV6 CIDR block”.



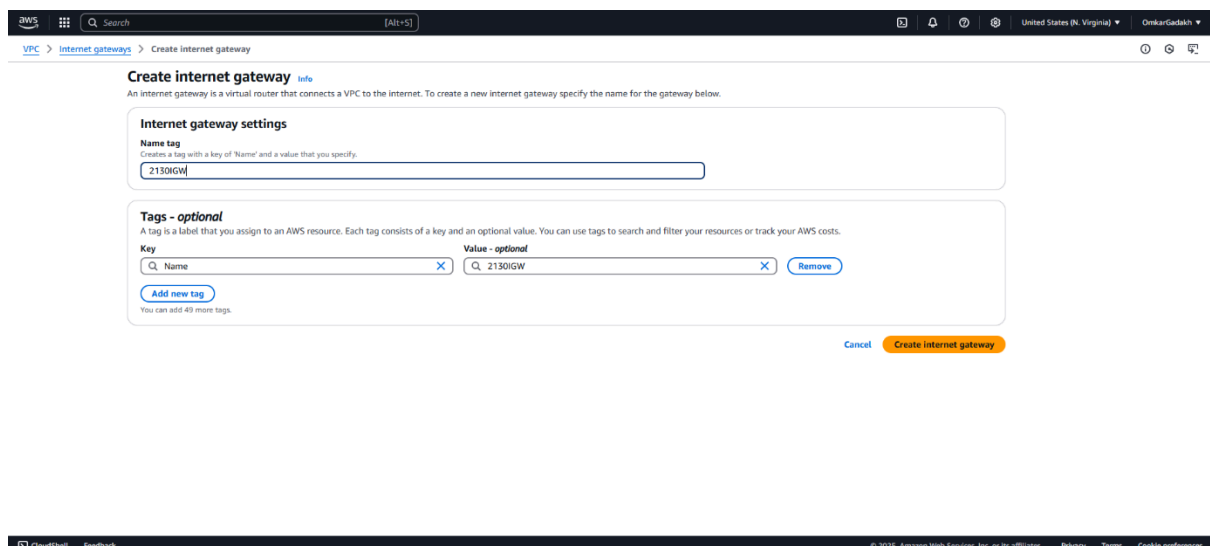
The screenshot displays the AWS Management Console interface for creating a new VPC. The 'VPC settings' section is active, showing options for 'Resources to create' (VPC only), 'Name tag - optional' (2130vpc), 'IPv4 CIDR block' (IPv4 CIDR manual input, 10.0.0.0/16), and 'IPv6 CIDR block' (No IPv6 CIDR block). The 'Tenancy' is set to 'Default'.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh **PRN:** 20220802130
Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

STEP 2: Now, go to Internet Gateways in VPC panel and click on “Create Internet Gateway”.

- Provide the name for the Internet Gateway as “2130IGW”



The screenshot shows the AWS Management Console interface for creating an internet gateway. The breadcrumb navigation indicates the path: VPC > Internet gateways > Create internet gateway. The main heading is 'Create internet gateway' with an information icon. A descriptive text states: 'An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.' The 'Internet gateway settings' section contains a 'Name tag' field with the value '2130IGW' and a description: 'Creates a tag with a key of 'Name' and a value that you specify.' Below this is the 'Tags - optional' section, which explains that a tag is a label for an AWS resource. It shows a table with one tag: Key 'Name' and Value '2130IGW'. There are buttons for 'Add new tag', 'Cancel', and 'Create internet gateway'.

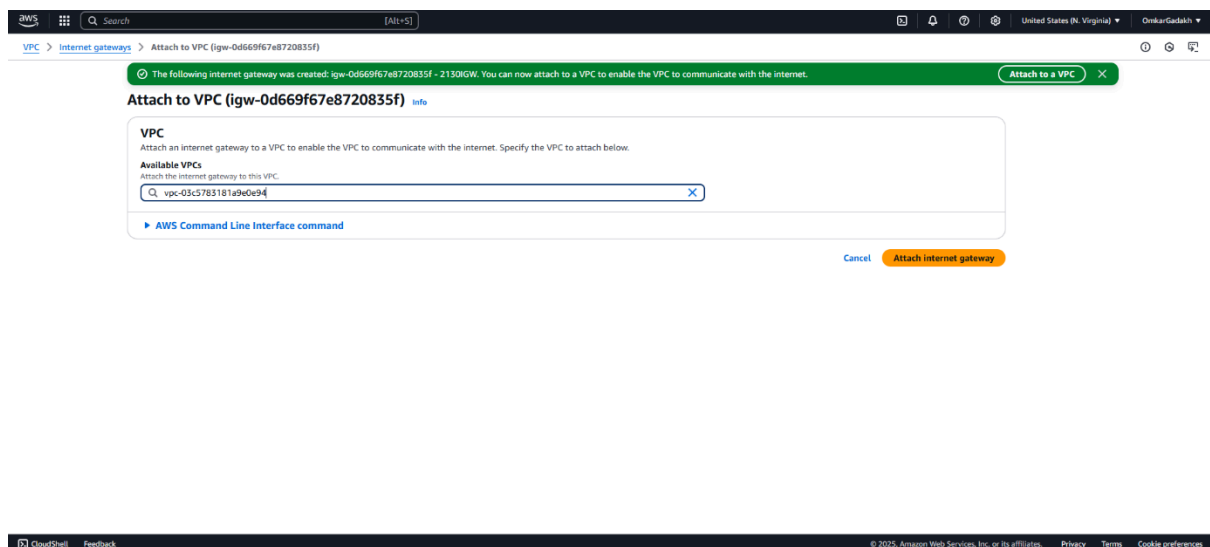
- After creation, click “Attach to VPC” and select the VPC you created.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

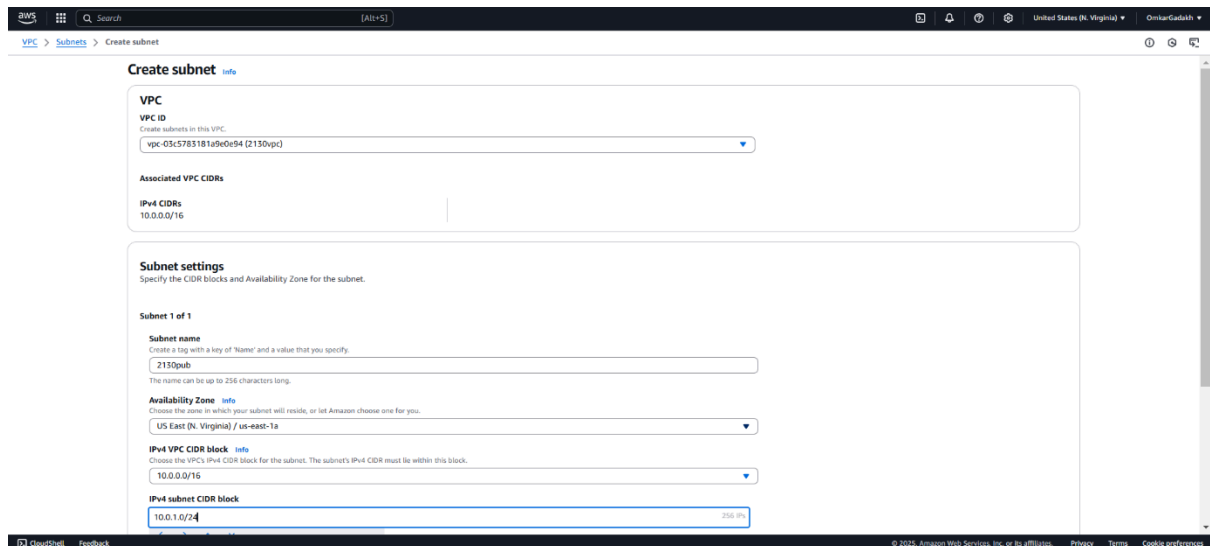
PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS



STEP 3: CREATE A SUBNET.

- In the VPC panel, navigate to **Subnets** and click **Create Subnet**.
- In subnet settings, name the subnet as **"2130PUB"**.
- Enter the IPv4 CIDR block IP as **"10.0.1.0/24"**.



School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

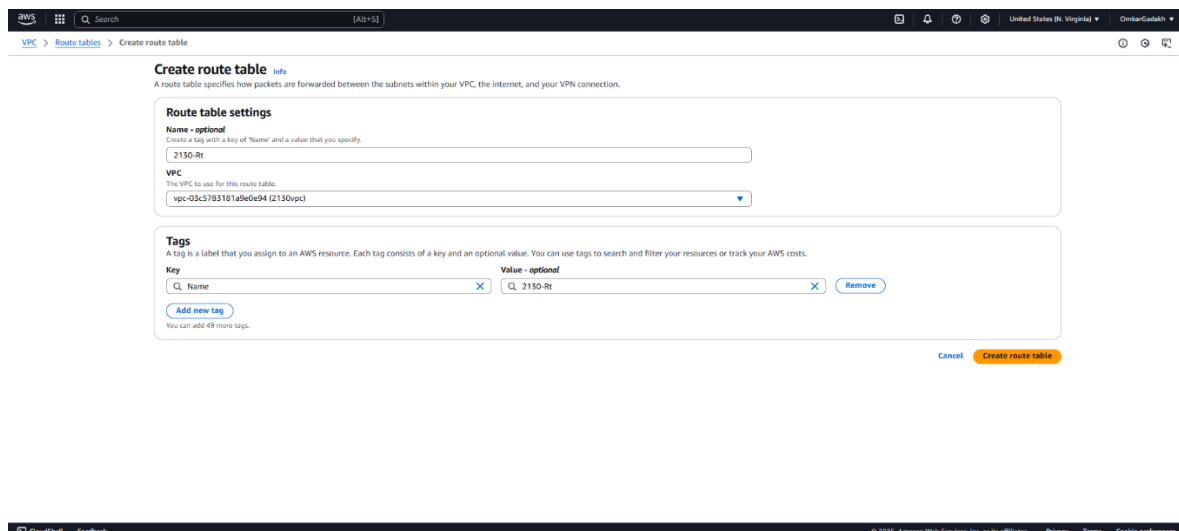
PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

=

STEP 4:CREATE ROUTE TABLE AND ASSOCIATE IT WITH SUBNET AND EDIT ROUTS.

- Navigate to Route tables in VPC panel and click “Create Route Table”.
- In Route Table settings enter “2130RT”.
- Attach the created VPC to it.



- To associate it with a subnet, click “Edit Subnet Associations” and select the subnet name “2130PUB”
- Attaching the created subnet to route table.



School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecting VPC Flow Logs For Efficient Network Monitoring In AWS

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
2130pub	subnet-0a89919021b6a0fae	10.0.1.0/24	-	Main (rtb-06a169c4310b01b51)

- After this, visit the Routes section, click on **“Edit Routes”** and add a new route.
- In the **“Destination Field”** enter **“0.0.0.0/0”** and in the Target field, select the **“Internet Gateway”** that was previously created.

Destination	Target	Status	Propagated
0.0.0.0/0	Internet Gateway	Active	No

STEP 5: CREATE A NETWORK ACCESS CONTROL LIST (NACL) AND EDIT INBOUND RULES AND EDIT SUBNET ASSOCIATION.

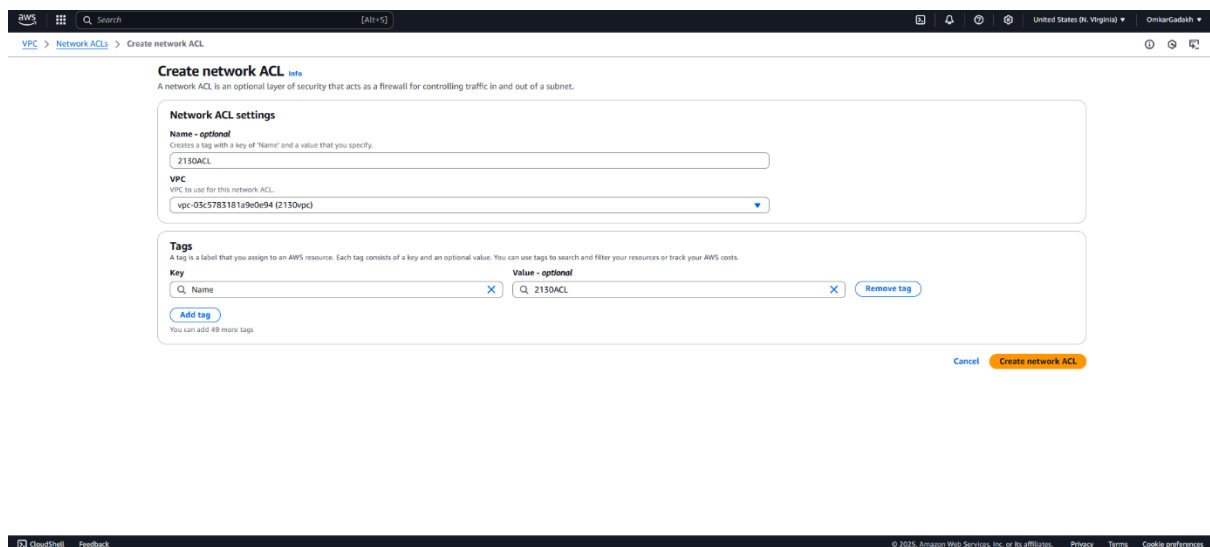
- Go to the Network ACLs in the VPC panel.
- And create **“NACL”** name **“2130NACL”** and select vpc and create network ACL.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

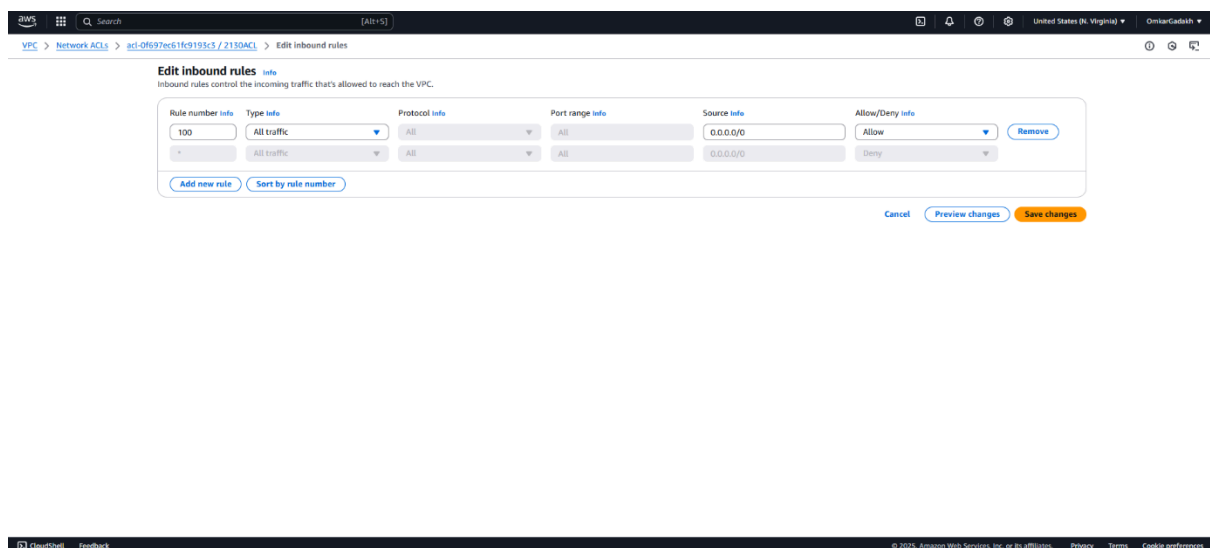
PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS



The screenshot shows the 'Create network ACL' page in the AWS Management Console. The page title is 'Create network ACL' with an 'info' link. Below the title is a description: 'A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.' The 'Network ACL settings' section includes a 'Name - optional' field with the value '2130ACL' and a 'VPC' dropdown menu showing 'vpc-05c5783181a9e0b94 (2130vpc)'. The 'Tags' section has a table with one row: Key 'Name', Value '2130ACL'. At the bottom right are 'Cancel' and 'Create network ACL' buttons.

- The Inbound and Outbound Rules will be updated to allow All traffic under
- rule number 100 for both inbound and outbound rules.



The screenshot shows the 'Edit inbound rules' page in the AWS Management Console. The page title is 'Edit inbound rules' with an 'info' link. Below the title is a description: 'Inbound rules control the incoming traffic that's allowed to reach the VPC.' The page displays a table of rules. The first rule has Rule number '100', Type 'All traffic', Protocol 'All', Port range 'All', Source '0.0.0.0/0', and Allow/Deny 'Allow'. There is a 'Remove' button next to it. At the bottom right are 'Cancel', 'Preview changes', and 'Save changes' buttons.

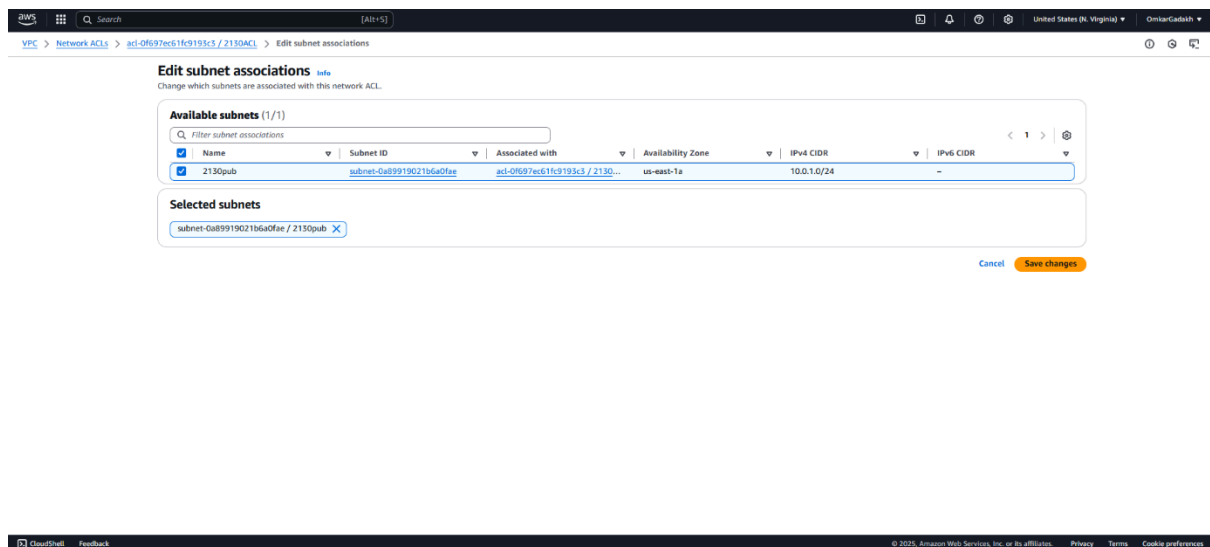
School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

- And go to **"EDIT SUBNET ASSOCIATION"** and click on created subnet **"2130PUB"** and save changes.



STEP6:CREATE SECURITY GROUP.

- Create **"security group"** name **"2130SG"** and select created vpc and create security group.



**D Y PATIL
INTERNATIONAL
UNIVERSITY**
AKURDI PUNE

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

The screenshot shows the AWS Management Console interface for creating a new security group. The 'Basic details' section includes a text input for the security group name (2130SG), a text input for the description (allow), and a dropdown menu for the VPC (vpc-03c5783181a9e0e94 (2130vpc)). The 'Inbound rules' section is partially visible, showing a table with columns for Type, Protocol, Port range, Source, and Description - optional. The table currently has one row with 'All traffic' as the type, 'All' as the protocol, 'All' as the port range, and 'Anywhere...' as the source. There is an 'Add rule' button at the bottom of the table.

STEP 7: CREATE A CLOUDWATCH LOG GROUP.

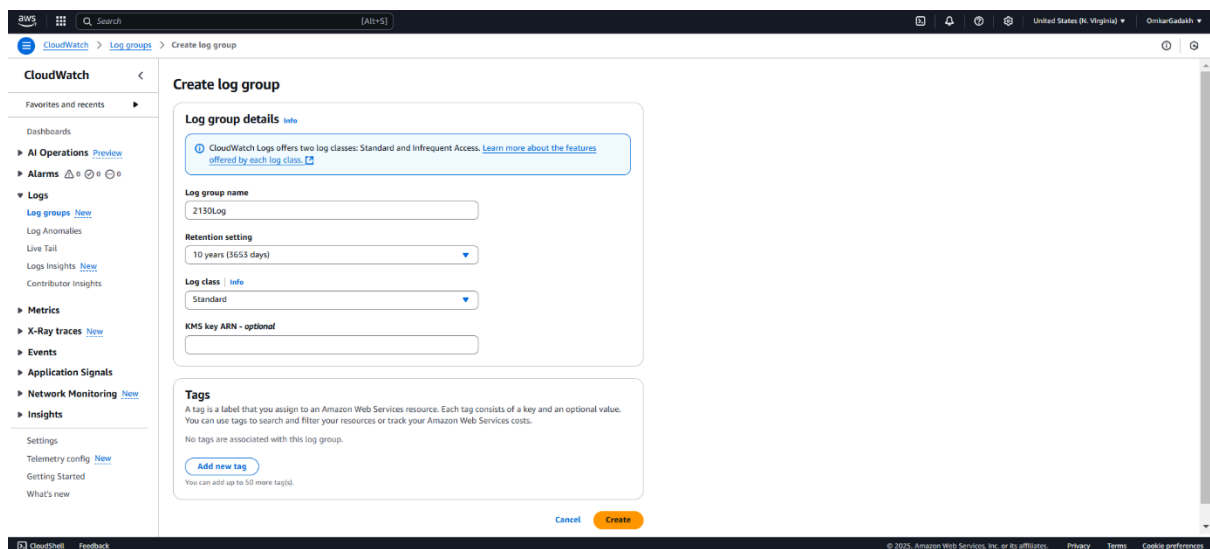
- Search for “CloudWatch” in the search bar and select it.
- In the CloudWatch console, go to Log Groups and click Create Flow Log Below.
- Assign a relevant name to the log group as “2130log”.
- Keep the Retention Settings as “Never Expire”.
- Keep the log class as “Standard”.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS



STEP 8: CREATE FLOWLOG.

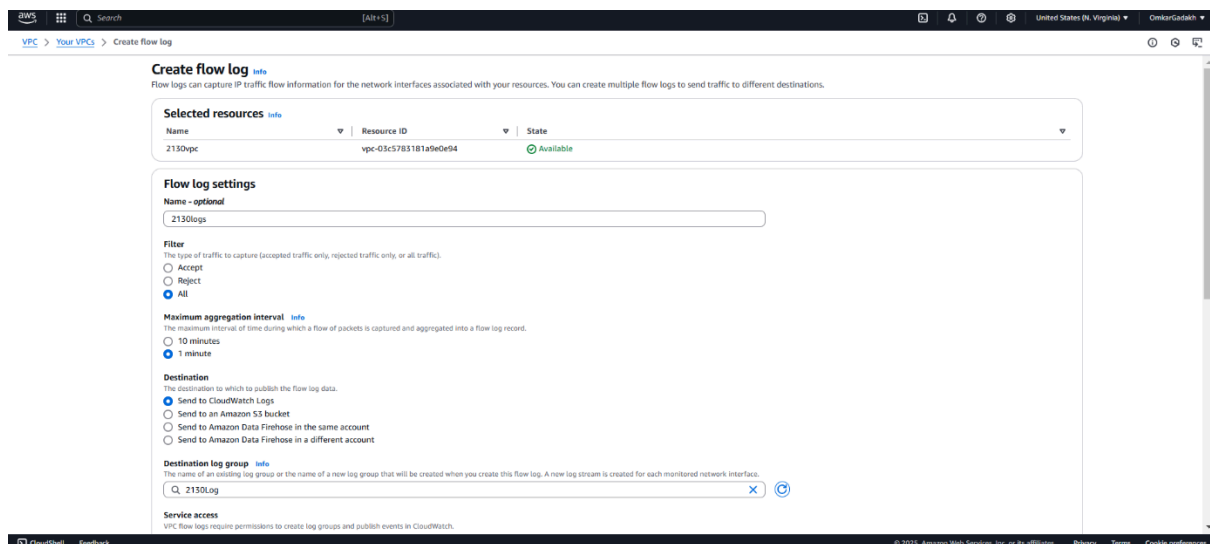
- Select the VPC and click **"Flow Logs"**.
- Click on **"Create Flow Log"**.
- Provide the name for the Flow Log as **"2130FLOW"**
- Select the **Filter** option to **"All"**.
- Keep the **Maximum Aggregation Interval** as **"1 minute"**.
- Set the **Destination** to **"Send to Cloud Logs"**.
- Select the CloudWatch log Group you created earlier.
- Create a **new role** to grant **Service Access**.
- Choose the **Default Format** for the log record format.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS



- The Log Group is now **linked** to your VPC

STEP 9: LAUNCH AN EC2 INSTANCE.

- Give an appropriate name to the EC2 instance as **"2130EC2"**.
- Select the AMI as **"Ubuntu"**.
- Select the created **"VPC"** in Network Settings.
- Select the associated **"subnet"**.
- Select security group **"2130SG"** that we already have created.



School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: 2130EC2

Application and OS Images (Amazon Machine Image)

Search our full catalog including 1000s of application and OS images

Recently: Quick Start

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), 550 Volume Type

ami-04a4f1d8c54c110d (aa-64-bit) / ami-04a4f1d8c54c110d (aa-64-bit)

Virtualization: true, ENA: enabled, true, Root device type: ebs

Free tier eligible

Description

Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Summary

Number of instances: 1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64, read more

ami-04a4f1d8c54c110d

Virtual server type (instance type)

t2.micro

Firewall (security group)

2130SG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 80 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the Internet.

Cancel Launch instance Preview code

Key pair (login)

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

2130newkey

Create new key pair

Network settings

VPC - required

vpc-03c5783181a9e0e94 (2130vpc)

Subnet

subnet-0a89919021b6a0f0e (2130pub)

Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

Create security group Select existing security group

Common security groups

Select security groups

2130SG sg-08c3f69f52f89c344

Compare security group rules

Summary

Number of instances: 1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64, read more

ami-04a4f1d8c54c110d

Virtual server type (instance type)

t2.micro

Firewall (security group)

2130SG

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 80 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the Internet.

Cancel Launch instance Preview code

STEP10: CREATE IAM ROLE.

- Click on IAM and then on roles and create role.
- STEP 1: Select trusted entity type "AWS SERVICE".
- Select use case "EC2".



School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

- **STEP 2:**Add permissions policies “VPCFullAccess”.
- **STEP 3:** Add role details name “2130ROLE” and create role.
- And “role” is created.

Step 2: Add permissions

Select trusted entity

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allow users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.

Use case

- ☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- ☐ **EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot instances on your behalf.
- ☐ **EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- ☐ **EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- ☐ **EC2 - Spot Instances**
Allows EC2 Spot instances to launch and manage spot instances on your behalf.

Step 3: Name, review, and create

Choose one or more policies to attach to your new role.

Filter by Type
All types 17 matches

Policy name	Type	Description
<input type="checkbox"/> AmazonDMSVPCManagementRole	AWS managed	Provides access to manage VPC setting...
<input type="checkbox"/> AmazonDRSVPCManagement	AWS managed	Provides access to manage VPC setting...
<input type="checkbox"/> AmazonEC2InfrastructureRolePolicyForVpcLattice	AWS managed	Provides access to other AWS service r...
<input type="checkbox"/> AmazonEKSVPCResourceController	AWS managed	Policy used by VPC Resource Controlle...
<input type="checkbox"/> AmazonVPCCrossAccountNetworkInterfaceOperations	AWS managed	Provides access to create network inter...
<input checked="" type="checkbox"/> AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via...

AmazonVPCFullAccess
Provides full access to Amazon VPC via the AWS Management Console.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "AmazonVPCFullAccess",
6-       "Effect": "Allow",
7-       "Action": [
8-         "ec2:AcceptVpcPeeringConnections",
9-         "ec2:AcceptVpcEndpointConnections",
10-        "ec2:AllocateAddress",
11-        "ec2:AssignPrivateAddresses",
12-        "ec2:AssignPrivateIpAddresses",
13-        "ec2:AssociateAddress",
14-        "ec2:AssociateRouteOptions",
15-        "ec2:AssociateRouteTable",
16-        "ec2:AssociateSecurityGroupVpc",
17-        "ec2:AssociateSubnetCidrBlock",
18-        "ec2:AssociateVpcCidrBlock",
19-        "ec2:AttachClassicLinkVpc",
20-        "ec2:AttachInternetGateway",

```

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

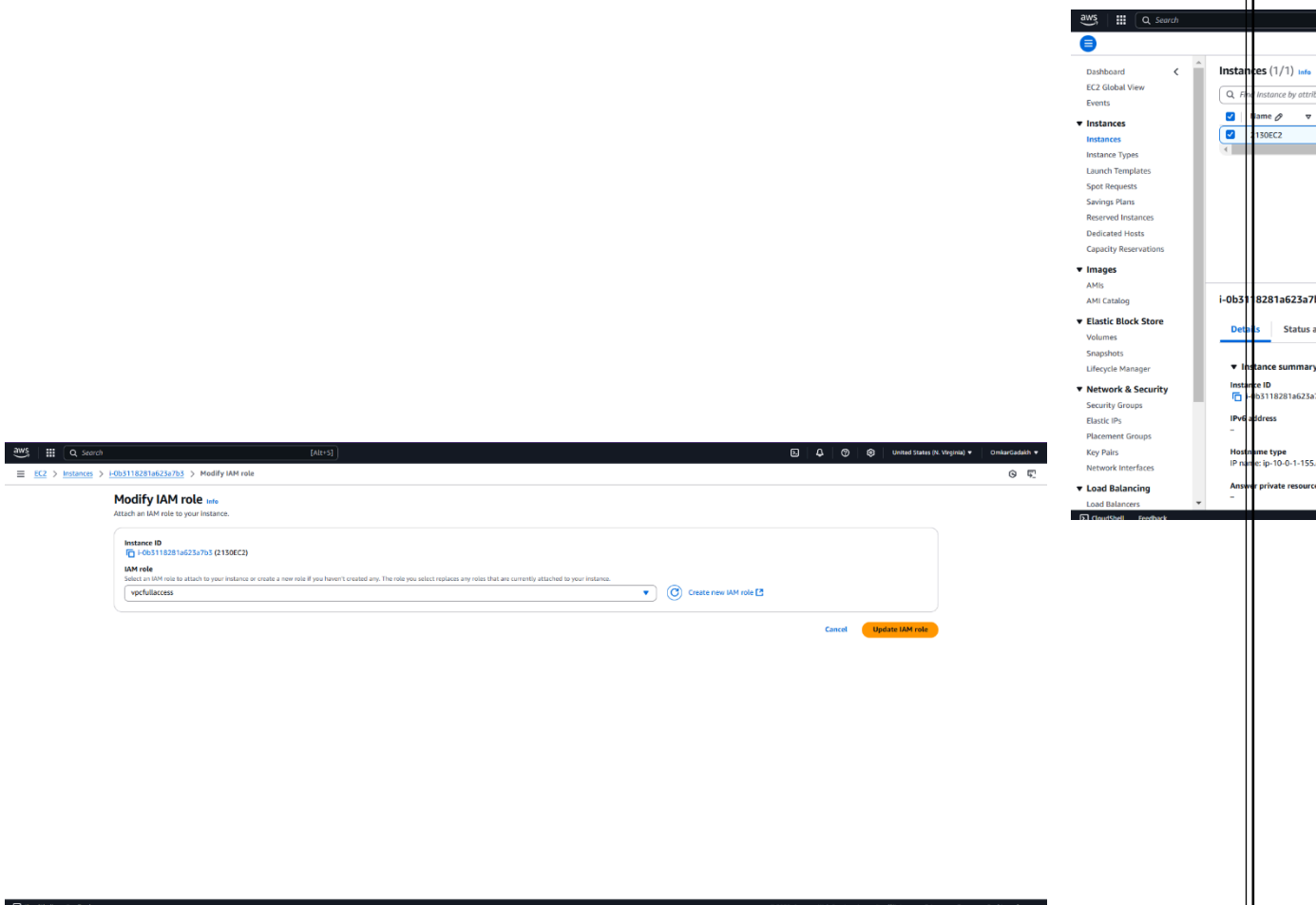
Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

STEP11: select the instance and go to its security and select “Modify IAM Role”.

- Update the “IAM Role”.



The screenshot displays the AWS IAM console interface. The main content area shows the 'Modify IAM role' page for the instance 'i-0b3118281a623a795'. The page includes a dropdown menu for selecting an IAM role, currently set to 'vpcfullaccess'. A 'Create new IAM role' link is visible next to the dropdown. The 'Update IAM role' button is highlighted in orange. The left sidebar shows the navigation menu with 'Instances' selected. The right sidebar shows the 'Instance summary' for the selected instance, including its ID, name, and IP address.

School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

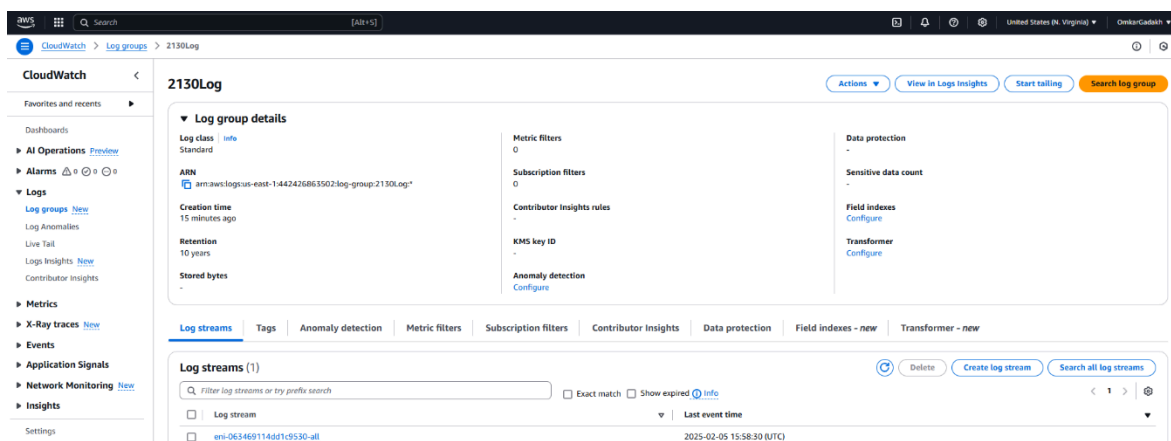
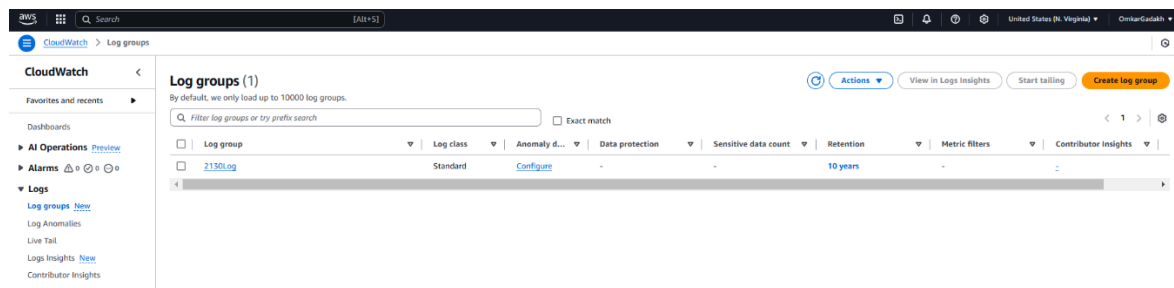
Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS

STEP 12: GO TO CLOUD WATCH TO CHECK THE FLOW LOGS ARE GENERATED OR NOT.

- Go to cloud watch and in log groups.
- Click on created log "2130LOGS".
- Click on the log stream you can see all the logs are generated.

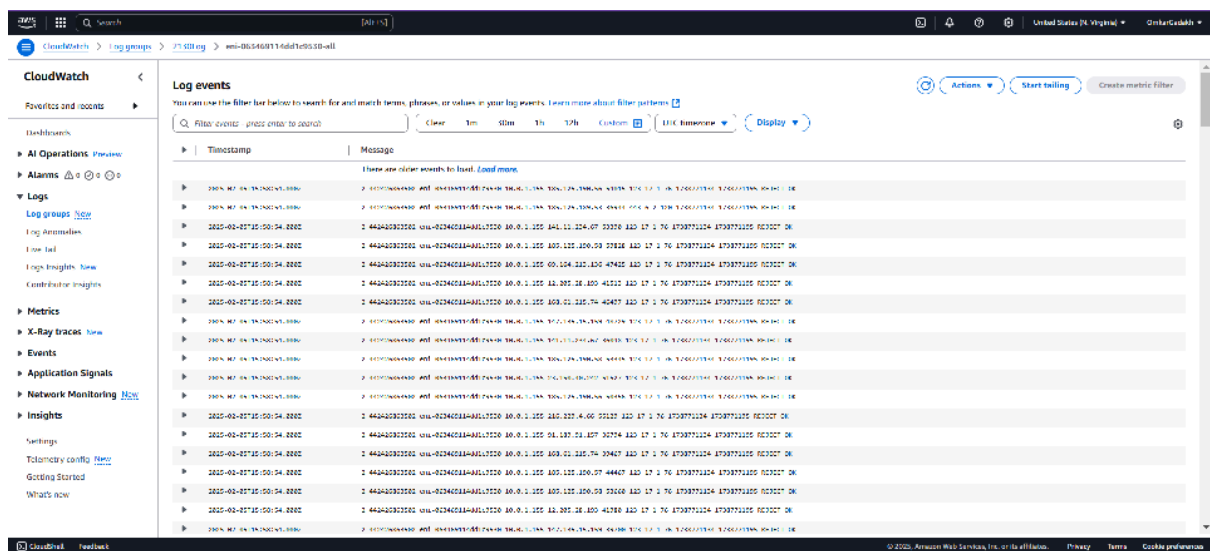


School of Computer Science, Engineering and Applications (SCSEA)
B Tech TY (CCSA)
Subject: Cloud Architecture and Protocol

Name of the Student: Omkar Gadakh

PRN: 20220802130

Title of Practical: Architecturing VPC Flow Logs For Efficient Network Monitoring In AWS



The screenshot displays the AWS CloudWatch console interface. The left-hand navigation pane shows various monitoring tools, with 'Logs' selected. The main area is titled 'Log events' and shows a list of log entries. The first entry is expanded, revealing a detailed message. The message is a VPC flow log record, which includes a timestamp, an interface ID, an action type (e.g., 'accept'), a source IP address, a destination IP address, a protocol number, and a port range. The log entries are filtered by a specific pattern, and the console provides options to clear, filter, or display the logs.