

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

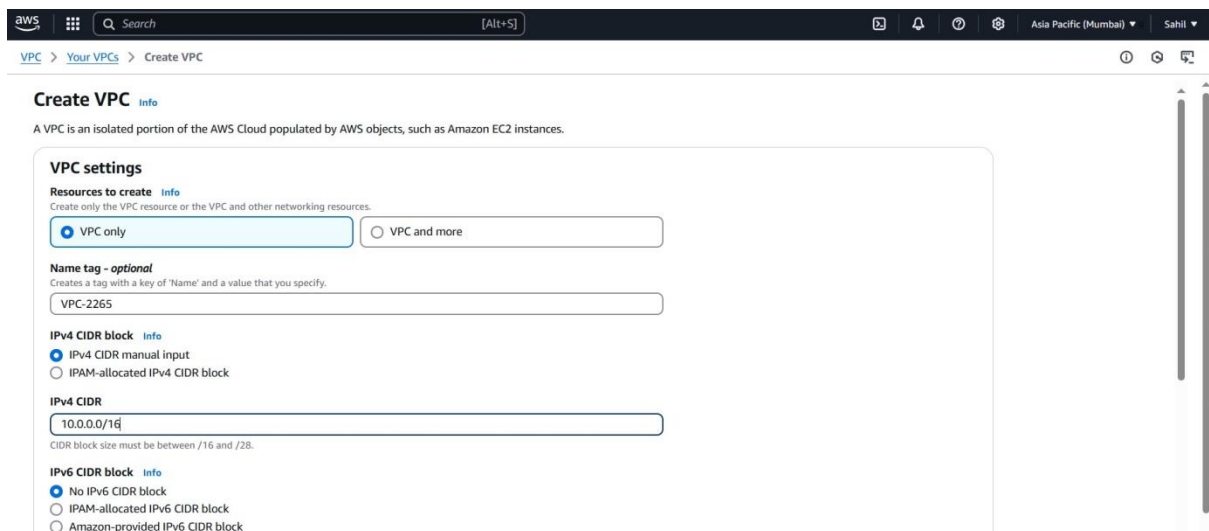
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

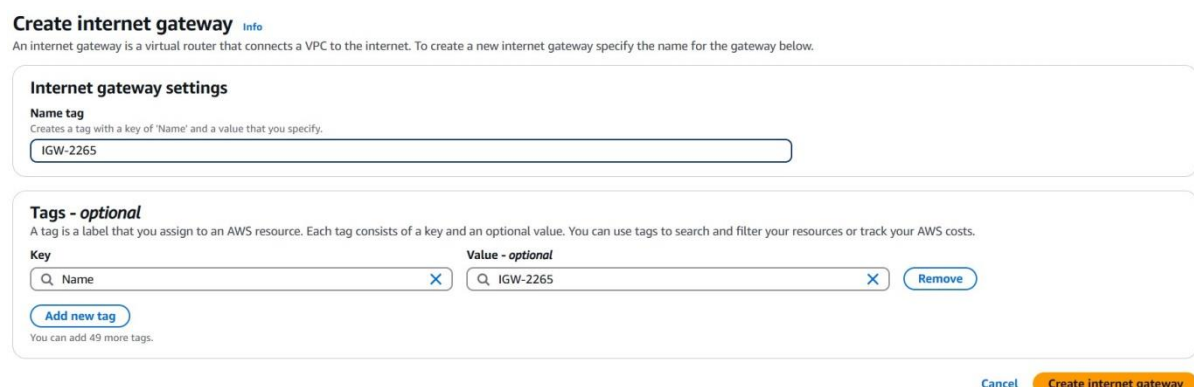
Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

Step 1: Create a VPC and connect Internet Gateway to it.

- Go to AWS console and search for VPC.
- Create VPC by selecting 'VPC Only' with valid name.
- Set IPv4 CIDR range as '10.0.0.0/16'.



- Go to Internet Gateway.
- Create an Internet Gateway.



- Attach the IGW to the VPC.

School of Computer Science, Engineering and Applications (SCSEA)

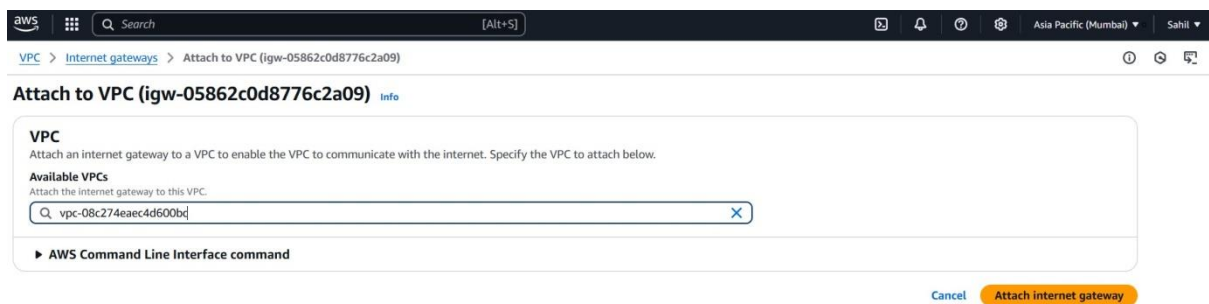
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

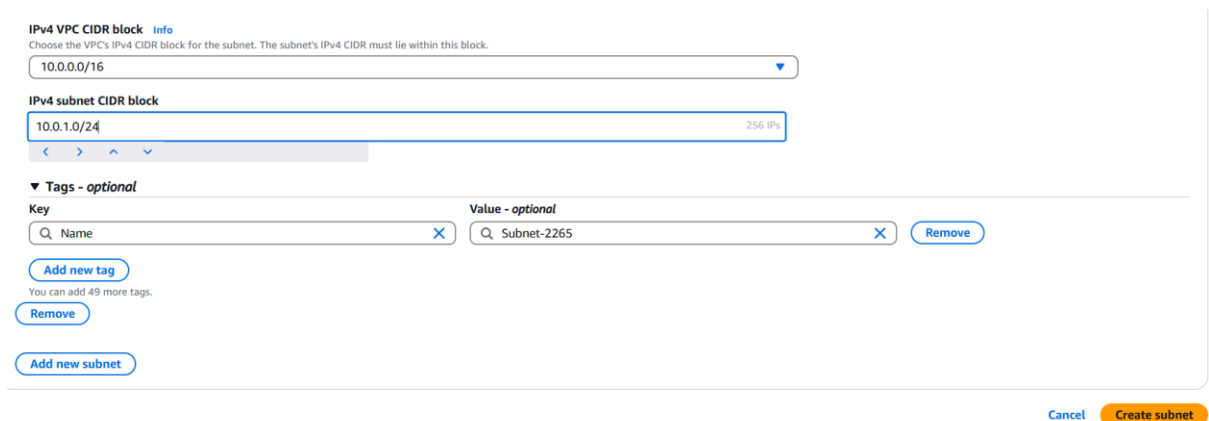
Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.



The screenshot shows the AWS console interface for attaching an internet gateway to a VPC. The breadcrumb trail is 'VPC > Internet gateways > Attach to VPC (igw-05862c0d8776c2a09)'. The main heading is 'Attach to VPC (igw-05862c0d8776c2a09)'. Below this, there's a 'VPC' section with the instruction 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Under 'Available VPCs', there's a search bar with 'vpc-08c274eac4d600b' entered. At the bottom right, there are 'Cancel' and 'Attach internet gateway' buttons.

Step 2: Create a Subnet and Route Table.

- Create a Subnet.
- Enter IPV4 subnet CIDR block as “10.0.1.0/24”, then click on “Create subnet”.



The screenshot shows the AWS console interface for creating a new subnet. The heading is 'IPv4 VPC CIDR block'. Below it, a dropdown menu shows '10.0.0.0/16'. The 'IPv4 subnet CIDR block' field contains '10.0.1.0/24' with a '256 IPs' indicator. There's a 'Tags - optional' section with a table for adding tags. At the bottom right, there are 'Cancel' and 'Create subnet' buttons.

- Create a Route Table and select the VPC we created.
- Associate the Subnet to the Route Table.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

✓ You have successfully updated subnet associations for rtb-0a89ef1004311b96e / RT-2265.

rtb-0a89ef1004311b96e / RT-2265

Actions

Details info

Route table ID

rtb-0a89ef1004311b96e

VPC

vpc-0c684439ec2c35af0 | VPC-2265

Main

No

Owner ID

908027405956

Explicit subnet associations

subnet-0589fe757972c591a / Subnet-2265

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

- Add a Route with Destination as '0.0.0.0/0' and Target as 'Internet Gateway' and select the internet gateway we created i.e. 'IGW-2265'.

Edit routes

Destination 10.0.0.0/16	Target local	Status Active	Propagated No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>	<input type="text" value="Internet Gateway"/>	<input type="text" value="No"/>
<input type="text" value="igw-0f530efa784ea19c8"/>	<input type="text" value="igw-0f530efa784ea19c8"/>	<input type="text" value="Active"/>	<input type="text" value="No"/>

Add route

Cancel Preview Save changes

Step 3: Create a NACL and attach the VPC.

Create network ACL info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - optional

Creates a tag with a key of 'Name' and a value that you specify.

NACL-2265

VPC

VPC to use for this network ACL.

vpc-0c684439ec2c35af0 (VPC-2265)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

NACL-2265

Add tag

You can add 49 more tags.

Cancel Create network ACL

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

- Edit the subnet association and select the subnet 'Subnet-2265'.
- Add Inbound and Outbound rules both with Rule number as '100' and Type as 'All Traffic'.

Edit outbound rules [info](#)

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number info	Type info	Protocol info	Port range info	Destination info	Allow/Deny info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

Step 4: Create a Security Group in EC2 Console.

- Create a Security Group with name 'SG-2265-FL'.
- Set Inbound Rules : SSH – Anywhere IPv4, HTTP – Anywhere IPv4 and HTTPS – Anywhere IPv4.
- Set Description and Click on Create.

✔ Security group (sg-0049138669164f42d | SG-2265-FL) was created successfully

[Details](#)

sg-0049138669164f42d - SG-2265-FL [Actions](#)

Details

Security group name SG-2265-FL	Security group ID sg-0049138669164f42d	Description Allow SSH and HTTP	VPC ID vpc-094225bc64de0682c
Owner 908027405956	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Sharing - new](#) [VPC associations - new](#) [Tags](#)

Inbound rules (3) [Manage tags](#) [Edit inbound rules](#)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0627dc41fae61a062	IPv4	HTTP	TCP	80

Step 5: Create Log Group in AWS CloudWatch.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

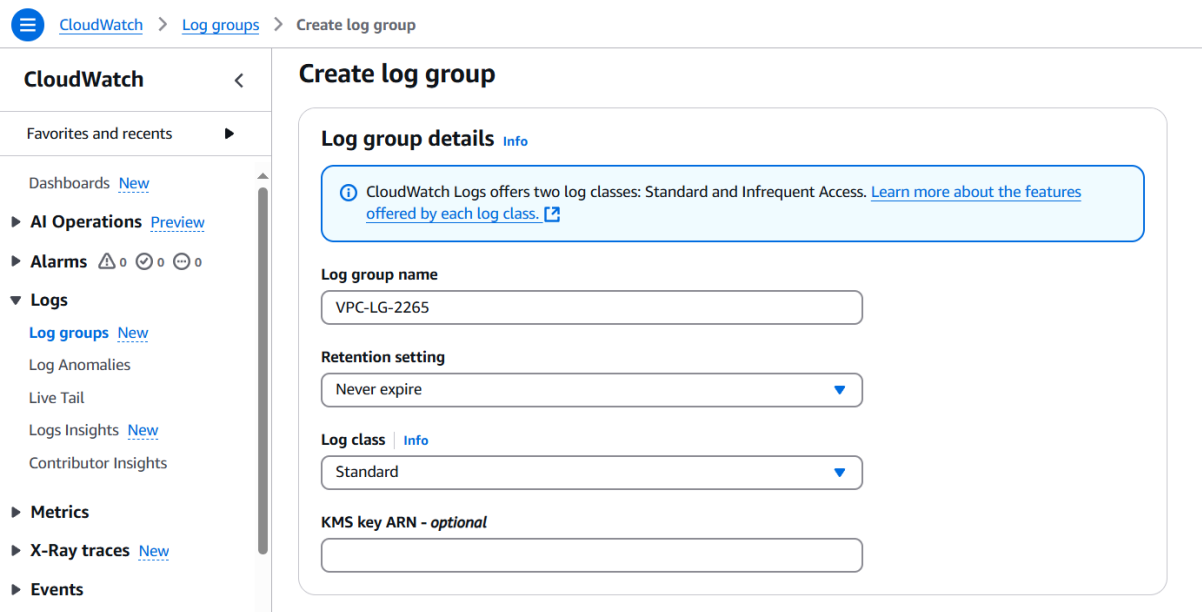
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

- Go to CloudWatch console.
- Go to 'Logs' the 'Log Group's and click on 'Create log group'.
- Name the log group as 'VPC-LG-2265'.
- Keep the Retention setting as 'Never expire'.
- Keep Log class as 'Standard'.
- Click on Create.



CloudWatch > Log groups > Create log group

CloudWatch

Favorites and recents

Dashboards [New](#)

► **AI Operations** [Preview](#)

► **Alarms** [0](#) [0](#) [0](#) [0](#)

▼ **Logs**

Log groups [New](#)

Log Anomalies

Live Tail

Logs Insights [New](#)

Contributor Insights

► **Metrics**

► **X-Ray traces** [New](#)

► **Events**

Create log group

Log group details [Info](#)

CloudWatch Logs offers two log classes: Standard and Infrequent Access. [Learn more about the features offered by each log class.](#)

Log group name

VPC-LG-2265

Retention setting

Never expire

Log class [Info](#)

Standard

KMS key ARN - optional

Step 6: Create a Flow Log.

- Go to VPC console.
- Select the VPC 'VPC-2265'.
- Select Flow logs.
- Click on 'Create flow log'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

vpc-0c684439ec2c35af0 / VPC-2265

Actions

Details Info

VPC ID

vpc-0c684439ec2c35af0

DNS resolution

Enabled

Main network ACL

acl-06467bc31aec0623b

IPv6 CIDR (Network border group)

-

State

Available

Tenancy

default

Default VPC

No

Network Address Usage metrics

Disabled

Block Public Access

Off

DHCP option set

dopt-04032ba0b06b93aa5

IPv4 CIDR

10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups

-

DNS hostnames

Disabled

Main route table

rtb-0aa45e26dc0649d7b

IPv6 pool

-

Owner ID

908027405956

Resource map

CIDRs

Flow logs

Tags

Integrations

Flow logs Info

Search



Actions

Create flow log



Name



Flow log ID



Filter



Destination type



Destination name

No matching resource found

- Set Name of flow log as 'VPC-FL-2265'.
- Keep Filter as 'All'.
- Set 'Maximum aggregation interval' as '1 minute'.
- Set 'Destination' as 'Send to CloudWatch Logs'.
- Select Destination log group as 'VPC-LG-2265'.

Flow log settings

Name - optional

VPC-FL-2265

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

- ☐ Accept
- ☐ Reject
- ☒ All

Maximum aggregation interval Info

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

- ☐ 10 minutes
- ☒ 1 minute

Destination

The destination to which to publish the flow log data.

- ☒ Send to CloudWatch Logs
- ☐ Send to an Amazon S3 bucket
- ☐ Send to Amazon Data Firehose in the same account
- ☐ Send to Amazon Data Firehose in a different account

Destination log group Info

The name of an existing log group or the name of a new log group that will be created when you create this flow log. A new log stream is created for each monitored network interface.

VPC-LG-2265





School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

- Create a new Service role.
- Keep Log record format as 'AWS default format'.
- Click on 'Create flow log'.

Service access

VPC flow logs require permissions to create log groups and publish events in CloudWatch.

- ☐ Use an existing service role
- ☒ Create and use a new service role

Service role name [Info](#)

VPCFlowLogs-Cloudwatch-1738781644416

Log record format

Specify the fields to include in the flow log record.

- ☒ AWS default format
- ☐ Custom format

Additional metadata

Include additional metadata to AWS default log record format.

- ☐ Include Amazon ECS metadata

Format preview

```
 ${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end}
 ${action} ${log-status}
```

[Copy](#)

Step 7: Launch an EC2.

- Set name of EC2 as 'EC2-FL-2265'.
- Select AMI as 'Ubuntu'.
- Select Instance type as 't3.micro'.
- Select Key pair.
- Change Network Settings.
- Select VPC and Subnet that we created.
- Set 'Auto-assign public IP' as 'Enable'.
- Select Security Group 'SG-2265' that we created earlier.
- Click on 'Launch instance'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

Launch an instance [Info](#)

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 [Info](#)

Name

EC2-FL-2265

[Add additional tags](#)

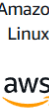






▼ Application and OS Images (Amazon Machine Image) [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

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

Recents

Quick Start

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


[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

▼ 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*

KY-CCSA-TY-2265

 [Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0766400fb5de851c2 (VPC-2265)
10.0.0.0/16



Subnet [Info](#)

subnet-0b42cb2e49526bbe8 Subnet-2265
VPC: vpc-0766400fb5de851c2 Owner: 908027405956 Availability Zone: ap-south-1c
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

 [Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

- Now, Select the EC2 instance – Actions – Security – Modify IAM Roles – Create new role.
- Search and select VPCFlowLogs-CloudWatch.
- Select Trusted entity type as ‘AWS Service’ – Use Case as EC2 instance.
- In Permissions search and select ‘AmazonVPCFullAccess’.
- Set name as ‘VPC_FL_2265’ and click on create.
- After creating and attaching role connect the instance on terminal and install apache on it.

```
ubuntu@ip-10-0-1-64: ~  
Enabling module setenvif.  
Enabling module filter.  
Enabling module deflate.  
Enabling module status.  
Enabling module reqtimeout.  
Enabling conf charset.  
Enabling conf localized-error-pages.  
Enabling conf other-vhosts-access-log.  
Enabling conf security.  
Enabling conf serve-cgi-bin.  
Enabling site 000-default.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean.service.  
Processing triggers for ufw (0.36.2-6) ...  
Processing triggers for man-db (2.12.0-4build2) ...  
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-10-0-1-64:~$
```

Step 8: Check if the Flow Logs are generated in CloudWatch.

- Go to CloudWatch – Log Groups – VPC-LG-2265 – Log Streams.
- Click on the log stream.

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

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

**Title of Practical: 3. Architecting VPC Flow Logs for efficient
network monitoring in AWS.**

VPC-LG-2265 Actions View in Logs Insights Start tailing Search log group

Log group details

Log class [info](#)
Standard

ARN
[arn:aws:logs:ap-south-1:908027405956:log-group:VPC-LG-2265:*](#)

Creation time
35 minutes ago

Retention
Never expire

Stored bytes
-

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

KMS key ID
-

Anomaly detection
[Configure](#)

Data protection
-

Sensitive data count
-

Field indexes
[Configure](#)

Transformer
[Configure](#)

[Log streams](#) [Tags](#) [Anomaly detection](#) [Metric filters](#) [Subscription filters](#) [Contributor Insights](#) [Data protection](#) [Field indexes - new](#) [Transformer - new](#)

Log streams (1) 🔄 Delete Create log stream Search all log streams

☐ Exact match ☐ Show expired [Info](#)

<input type="checkbox"/> Log stream	Last event time
<input type="checkbox"/> eni-02a1649fb964aa607-all	2025-02-05 19:36:27 (UTC)

- Here we can see generated 'Log Events'.

CloudWatch > Log groups > VPC-LG-2265 > eni-02a1649fb964aa607-all

CloudWatch

Alarms ☐ ☐ ☐ ☐ ☐

Logs

- Log groups [New](#)
- Log Anomalies
- Live Tail
- Logs Insights [New](#)
- Contributor Insights

Metrics

X-Ray traces [New](#)

Events

Application Signals

Network Monitoring [New](#)

Insights

Log events 🔄 Actions Start tailing Create metric filter

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Clear 1m 30m 1h 12h Custom UTC timezone Display

Timestamp	Message
There are older events to load. Load more .	
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 10.0.1.64 91.189.91.157 44686 123 17 1 76 1738785067 1738785083 ACCEPT OK
2 908027405956 eni-02a1649fb964aa607	10.0.1.64 91.189.91.157 44686 123 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 15.207.248.194 10.0.1.64 123 36630 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 10.0.1.64 15.207.248.194 36630 123 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 147.185.132.88 10.0.1.64 53771 8530 6 1 44 1738785067 1738785083 REJECT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 162.216.149.207 10.0.1.64 50012 18080 6 1 44 1738785067 1738785083 REJECT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 192.46.215.141 10.0.1.64 123 49340 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 10.0.1.64 192.46.215.141 49340 123 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 192.46.211.253 10.0.1.64 123 43743 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 10.0.1.64 192.46.211.253 43743 123 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 185.125.190.58 10.0.1.64 123 60025 17 1 76 1738785067 1738785083 ACCEPT OK
2025-02-05T19:51:07.000Z	2 908027405956 eni-02a1649fb964aa607 10.0.1.64 185.125.190.58 60025 17 1 76 1738785067 1738785083 ACCEPT OK