VPC Flow logs

We will create custom VPC.

Go to VPC
Click on create VPC
Select VPC only
Give Name — VPC-28
IPv4 CIDR — 10.10.0.0/16
Scroll down & click on create VPC

Go to Subnet
Click on create Subnet.
VPC ID — Select VPC-28
Subnet name — Public-Subnet
Availability zone — Select any
IPv4 CIDR block — 10.10.1.0/24
Click on create subnet

Go to Internet Gateway
Click on create Internet Gateway
Name — IGW-28
Click on Create Internet Gateway

Click on Actions
Click on Attach to VPC
Available VPCs Select VPC-28
Click on Attach Internet Gateway

Now Go to Route Table
Click on Create Route Table
Name - Public-Routing
Select VPC - VPC-28
Click on create Route table

Click on Routes
Click on Edit Routes
Click on Add Route
Enter 0.0.0.0/0 in destination
Select Internet Gateway in Target
Click on Save changes

Click on Subnet Associations
Click on Edit Subnet Associations
Select Public-Subnet
Click on Save Associations

Go to Cloud watch
click on log Groups
Click on create log group
log group name - flow-lg
Retention Setting - Never Expire
Scroll down & Click on create

Go to IAM
Click on Roles
Click on create role
Trusted Entity Type - AWS Service
Common use cases - EC2
Click on next

There is no flow-logs Policy

click on create Policy
It will redirect to new tab
Click on JSon
Select & Delete existing JSon Code
Copy & paste our JSon code

Click on next
Click on review
name - Policy-flow-logs
Description - Policy-flow-logs
Click on create policy
Go back to Previous Tab
Click on Refresh

Select our Policy- flow-logs
Click on next
Role name - flow-log-Role
Click on create Role

Now Go to Role
find our flow-log-Role
Open Role
Click on Trust Relationships
Edit Trust Policy
Select and delete existing code

copy & Paste our code
Click on update policy

Now Go to VPC
Select our VPC-28
In below Select flow logs
Click on create flow log
name - VPC.28-Flowlog
filter - All
maximum aggregation interval - 1 minute
Destination - Send to cloud watch logs
Destination log group - flow-lg
IAM Role - flow-log-role
log record format - AWS default Format
Click on create flow log

Now Go to EC2
Click on Launch instance
Select AMI
Select T2.micro
In instance configure details
Select VPC-28
Select Public-Subnet
Enable Public IP
Click next Add storage
Click next configure security group
Add SSH 22 & HTTP 80
Click Add Tags
Click Review & launch
launch Instance
wait for 2 min
~~Con~~ Select our instance
click on connect
Copy last command from SSH Client

Open MobaxTerm
Paste command & Press Enter.

use sudo su -
use cd /
use yum install httpd -y
use service httpd start.
use cd /var/www/html
use vi index.html
insert <h1> Homepage </h1> & Save file

Go to instances
Select our instance
Copy public IP
& open in browser

Now Go to Cloudwatch
Click on log group
Click on flow-lg
click on log stream name appear in blu
As we can see our flow log records
which is related to our IP.