

We need additional custom metrics within AWS CloudWatch Metrics to record IP address usage within AWS VPC Subnets. How would you build a solution to achieve this?

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.

If you launch an instance into your subnet after you create a flow log for your subnet or VPC, we create a log stream (for CloudWatch Logs).

Steps for VPC Flow Logs, publish flow logs to CloudWatch:

- 1- VPC and subnets created.
- 2- Launched an Amazon Linux 2 EC2 instance in Public Subnets
- 3- Installed and Configured Nginx Web Server to Run a Simple Web Page on the instance
- 4- IAM role created for publishing flow logs to CloudWatch Logs:

Nginx-flow-logs-policy (JSON):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Nginx-flow-logs-role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 5- Log group created in the CloudWatch console.
- 6- A flow log is created that publishes to CloudWatch Logs
Choose Subnets which the Nginx server inside

Subnets → Actions → Create Flow logs

Filter → All or Reject or Accept

Destination → Send to CloudWatch Logs

IAM Role → Nginx-flow-logs-role

Destination log group → Log group that is created

Create

Flow log created and published to CloudWatch Logs

To create flow logs by AWS CLI:

```
$ aws ec2 create-flow-logs --resource-type Subnet --resource-ids \  
subnet-0ef7e1e37b9a7c8d1 --traffic-type ACCEPT \  
--log-group-name Nginx-flow-logs --deliver-logs-permission-arn  
arn:aws:iam::452889875890:policy/nginx-flow-logs-policy
```

The screenshot shows the AWS CloudWatch console interface. The left sidebar contains navigation options: Dashboards, Alarms, Logs, Metrics, X-Ray traces, Events, and Application monitoring. The main content area displays the 'Log events' for the 'nginx-log-group' under the resource 'eni-0e93b96706ace9eba-all'. The interface includes a search bar, a filter bar, and a table of log events. The table has two columns: 'Timestamp' and 'Message'. The messages are JSON-formatted log entries from the Nginx server, showing details like IP addresses, ports, and HTTP status codes.

Timestamp	Message
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 10.0.12.151 104.149.163.115 80 61643 6 6 4095 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 104.149.163.115 10.0.12.151 61234 80 6 6 634 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 10.0.12.151 104.149.163.115 80 61234 6 5 542 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 104.149.163.115 10.0.12.151 61128 80 6 6 548 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 104.149.163.115 10.0.12.151 61643 80 6 6 555 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 104.149.163.115 10.0.12.151 61577 80 6 6 555 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 208.67.106.185 10.0.12.151 34103 5008 6 1 48 1665065527 1665065585 REJECT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 10.0.12.151 104.149.163.115 80 61128 6 6 4095 1665065527 1665065585 ACCEPT OK
2022-10-06T15:12:07.000+01:00	2 452889875890 eni-0e93b96706ace9eba 45.61.184.10 10.0.12.151 42292 5555 6 1 44 1665065527 1665065585 REJECT OK
2022-10-06T15:13:25.000+01:00	2 452889875890 eni-0e93b96706ace9eba 89.248.165.85 10.0.12.151 48384 55663 6 1 40 1665065605 1665065645 REJECT OK
2022-10-06T15:13:25.000+01:00	2 452889875890 eni-0e93b96706ace9eba 10.0.12.151 50.205.57.38 50864 123 17 1 76 1665065605 1665065645 ACCEPT OK
2022-10-06T15:13:25.000+01:00	2 452889875890 eni-0e93b96706ace9eba 45.227.253.99 10.0.12.151 41286 4979 6 1 40 1665065605 1665065645 REJECT OK
2022-10-06T15:13:25.000+01:00	2 452889875890 eni-0e93b96706ace9eba 185.180.143.165 10.0.12.151 14629 1604 6 1 40 1665065605 1665065645 REJECT OK
2022-10-06T15:13:25.000+01:00	2 452889875890 eni-0e93b96706ace9eba 51.195.228.194 10.0.12.151 58782 3390 6 1 40 1665065605 1665065645 REJECT OK