Prashant Lakhera
Mar 12, 2019 · 4 min read · Updated

100 Days of DevOps — Day 28- Introduction to VPC Flow Logs

Welcome to Day 28 of 100 Days of DevOps, Focus for today is VPC Flow logs

- *What are VPC Flow logs?*
  - *It comprised of IP traffic information*
  - *These logs are useful for troubleshooting network conversations and can be assigned toCategory Points)*

```
- Source
- Destination
- Elastic Network Interface
```

NOTE: Flow logs don't capture data, so you can't do packet analysis even if is un-encrypted.

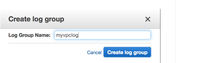
- **Setup VPC Flow Logs**

```
Go To AWS Console --> VPC --> Select your VPC --> Flow logs --> Create
Flow log
```

```
- Filter: Select All(Other options Accept/Reject)

- Destination: Send to CloudWatch Logs

- Destination log group: Go to AWS Console --> CloudWatch --> Logs -->
Create log group
```



- *IAM Role(Click on Set Up Permissions)*

- *After filling all the values it will look like this*

- *After creating flow logs, if you look for the subnet of this VPC, you will see subnet have flow logs associated with it and this is because it inherited flowlogs from VPC*

- **Flow Log Record Syntax**

A flow log record is a space-separated string that has the following format:

```
<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport>
<dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-
status>

2 123456789010 eni-abc123de 172.31.16.139 172.31.16.21 20641 22 6 20
4249 1418530010 1418530070 ACCEPT OK
```

Field	Description
version	The VPC Flow Logs version.
account-id	The AWS account ID for the flow log.
interface-id	The ID of the network interface for which the traffic is recorded.
srcaddr	The source IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
dstaddr	The destination IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
srcport	The source port of the traffic.
dstport	The destination port of the traffic.
protocol	The IANA protocol number of the traffic. For more information, see Assigned Internet Protocol Numbers.
packets	The number of packets transferred during the capture window.
bytes	The number of bytes transferred during the capture window.
start	The time, in Unix seconds, of the start of the capture window.
end	The time, in Unix seconds, of the end of the capture window.
action	The action associated with the traffic: • ACCEPT, if the traffic was accepted for its destination. • REJECT, if the traffic was not accepted for its destination.
log-status	The logging status of the flow log: • OK: Data is logging normally to the chosen destinations. • NODATA: There was no network traffic to or from your network interface during the capture window. • SKIPDATA: Some flow log records were skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

Reference: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

- If you go back to CloudWatch Log group, you will see something like this

- *As I applied flow logs at the VPC level and as we see that subnet automatically inherited it, if we go at the instance create under this VPC and check the Network Interface, you will see that eve your Elastic Network Interface(ENI) inherited those logs*

Flow logs do not capture all IP traffic. The following types of traffic are not logged:

- *Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.*
- *Traffic generated by a Windows instance for Amazon Windows license activation.*
- *Traffic to and from 169.254.169.254 for instance metadata.*
- *Traffic to and from 169.254.169.123 for the Amazon Time Sync Service.*
- *DHCP traffic.*
- *Traffic to the reserved IP address for the default VPC router.*
- *Traffic between an endpoint network interface and a Network Load Balancer network interface.*

- *Terraform Code*

```
resource "aws_flow_log" "example" {
  iam_role_arn    = "${aws_iam_role.example.arn}"
  log_destination = "${aws_cloudwatch_log_group.example.arn}"
  traffic_type    = "ALL"
  vpc_id          = "${var.vpc_id}"
}

resource "aws_cloudwatch_log_group" "example" {
  name = "example"
}

resource "aws_iam_role" "example" {
  name = "example"

  assume_role_policy = <<EOF

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
}

resource "aws_iam_role_policy" "example" {
  name = "example"
  role = "${aws_iam_role.example.id}"

  policy = <<EOF

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

GitHub Code Link

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.

- *Twitter: @100daysofdevops OR @LakheraJ2013*
- *Facebook: https://www.facebook.com/groups/795382630800402/*
- *Medium: https://medium.com/100daysofdevops*
- *Slack: https://devops-myworld.slack.com/messages/CPA1EFG45/*
- *GitHub Link https://github.com/100daysofdevops*

Reference

```
100 days of DevOps — Day 0
D-day is just one day away and finally, this is a continuation of the post(I posted a month
before)
medium.com
```

Get an email whenever Prashant Lakhera publishes.
Your email
Subscribe
By signing up, you will create a Medium account if you don't already have one. Review our Privacy Policy for more information about our privacy practices.

Love podcasts or audiobooks? Learn on the go with our new app. Try Knowable
Recommended from Medium
Gabriel Bauer
Getting your First Telegram Bot
Sponsoring Devs
Learning to Code
Apostolos Papadimitriou
Laravel Hashtag Through Pivot Model
Bandmaybe
Infio 100ks, 1.5bad to rank VIG 2000 in 2 years, 1.5bad to drop down the street from our house.
Stefan Kumar P.
String
JinXiaoHei
JSON is Out Dated?
Samuel Ebah
Framework Challenges Hash Tables Remain Rude
Prosperity Paul
Top Best Mobile Application Development Frameworks 2020