

AWS Lab 36

Flow Logs

Overview of the lab

In this lab you will learn how to publish flow log for ENI to cloudwatch log group

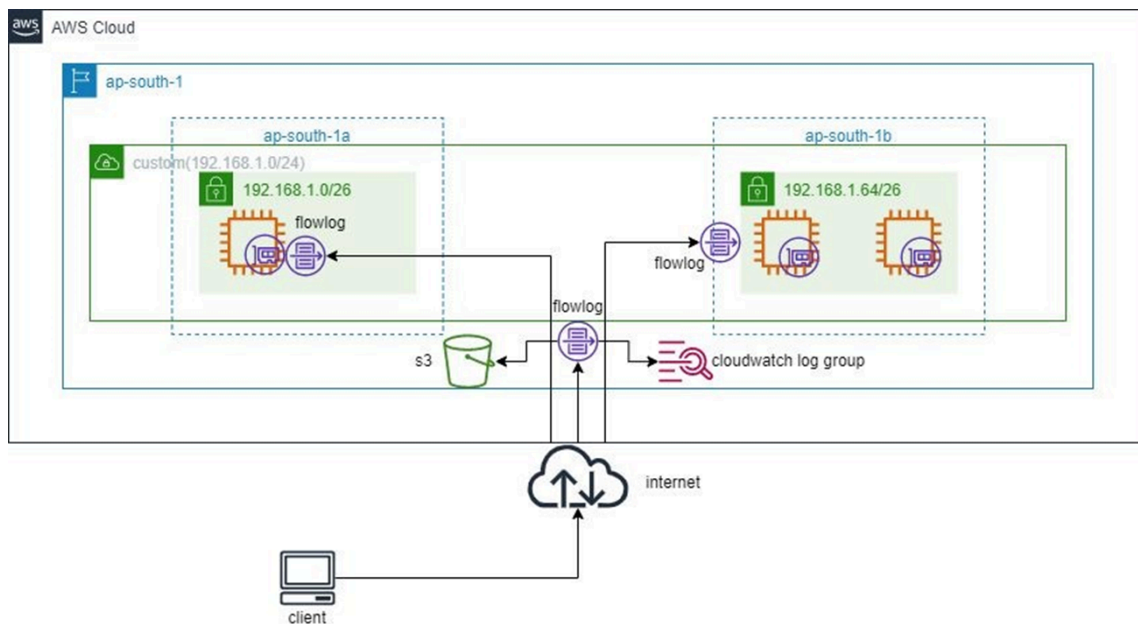
Flow Logs

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

It can be enabled in ENI / Subnet / VPC level

Logs can be pushed to CloudWatch / S3 / Kinesis

Architecture



Step by Step Lab

Launch an EC2 Linux Instance with Apache Web Server (lab4)

Create CloudWatch Log Group

1. In CloudWatch - click on [Log groups - Create log group](#)
 - 1.1. Log group name - **demo-flowlog**
2. Click on [Create](#)
3. Click on **demo-flowlog** (you dont see any Log streams)

Create an IAM Policy and Role

4. In IAM - Click on [Policies](#) and [Create policy](#)
 - 4.1. Click on JSON
 - 4.2. Remove the sample JSON and copy and paste the below policy

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

```

    "Resource": "*"
  }
]
}

```

4.3. Click on [Next](#)

4.4. Review and Create

4.4.1. Policy name - [flowlog-to-cw-policy](#)

4.5. Click on [Create policy](#)

5. Click on [Roles](#) and [Create role](#)

5.1. Trusted entity type - [Custom trust policy](#)

5.2. Remove the sample JSON / Copy and Paste the below JSON Trust policy

```

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

```

6. Click on [Next](#)

7. Search the [flowlog-to-cw-policy](#) and select

8. Click on [Next](#)
9. Role name - [flowlog-role](#)
10. Click on [Create role](#)

Create Flow Log


11. In EC2 - Select the instance - Click on [Networking](#)
12. Click on the [eni](#)
13. Click on [Create flow log](#)
 - 13.1. Name - [demo-flowlog](#)
 - 13.2. Filter - [All](#)
 - 13.3. Maximum aggregation interval - [1 minute](#)
 - 13.4. Destination - [Send to CloudWatch logs](#)
 - 13.5. Destination log group - [flowlog](#)
 - 13.6. IAM role - [flowlog-role](#)
14. Click on [Create flow log](#)

Verify the logs

15. In CloudWatch - click on [Log groups](#)
16. Click on [demo-flowlog](#) (now you see logs in Log streams)

Clean Up Step

1. In EC2 - Select the instance and [terminate it](#)
 2. In CloudWatch - Select the [loggroup \(flowlog\)](#) and in [Actions](#) - Click on [delete log groups](#)
-

- 
3. In IAM delete the **Role(flowlog-role)** and **Policy(flowlog-to-cw-policy)**
-