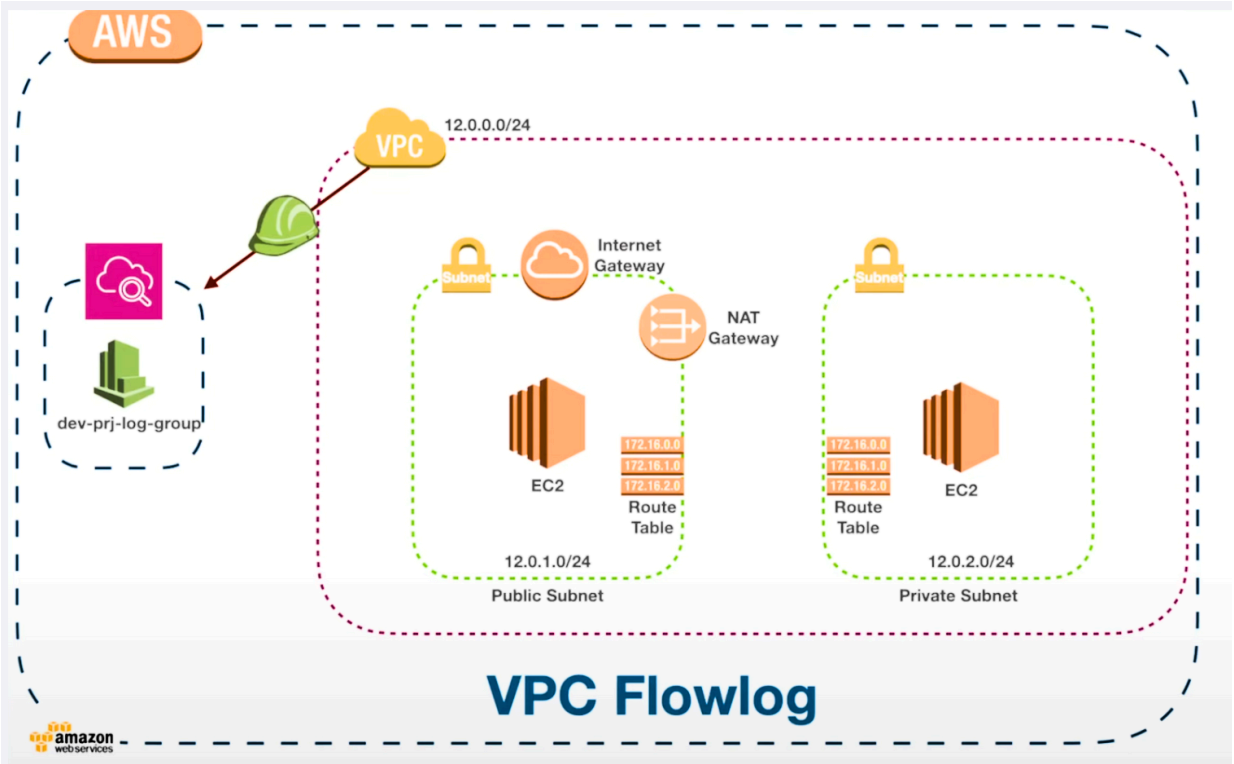
VPC Flow Logs



What is a VPC Flow Log?

VPC Flow Logs are used to **capture information about the IP traffic** going **to and from network interfaces** in your **Virtual Private Cloud (VPC)**.
This helps in **monitoring, troubleshooting, and securing** your network by analyzing the flow of data.

Flow log data can be published to **Amazon CloudWatch Logs** or **Amazon S3** for storage and analysis.

Use Case

- Monitor traffic to and from EC2 instances
- Detect security issues or misconfigured rules
- Audit network access for compliance

Steps to Set Up VPC Flow Logs with CloudWatch

1. Create a VPC

- Create a new Virtual Private Cloud using the VPC wizard or custom setup.

2. Create Subnets

- Create at least one **public subnet** and one **private subnet**.

3. Create and Attach Internet Gateway

- Create an **Internet Gateway (IGW)**.
- Attach the IGW to the VPC.

4. Create and Configure Route Table

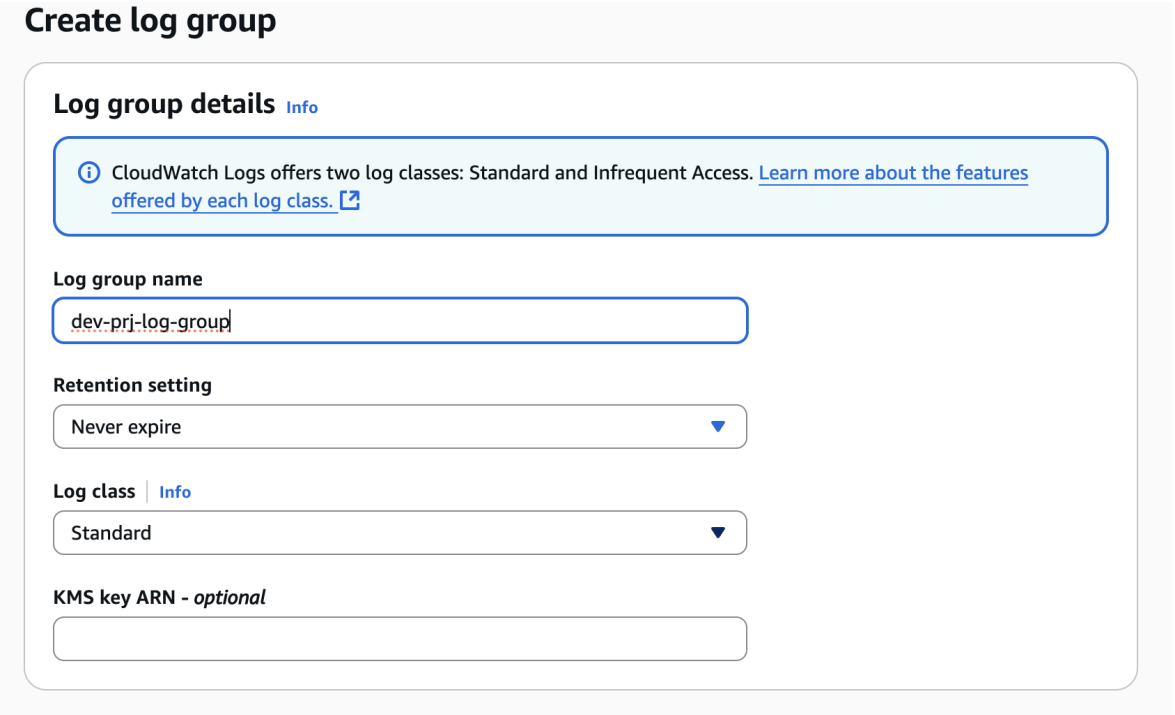
- Create a custom **Route Table**.
- Add a route to the internet via the IGW.
- **Edit subnet association** to associate the **public subnet** with this route table.

5. Launch an EC2 Instance

- Launch an instance in the public subnet.
- Ensure **Security Group** allows:
  - **SSH (port 22)** from your IP
  - **All ICMP - IPv4** for ping access

6. Set Up CloudWatch Log Group

- Go to **CloudWatch > Log Groups**.
- Create a **new log group** (e.g., `VPCFlowLogsGroup`).



7. Create IAM Role with Required Permissions

Create an IAM role or policy with the following **CloudWatch Logs permissions**:

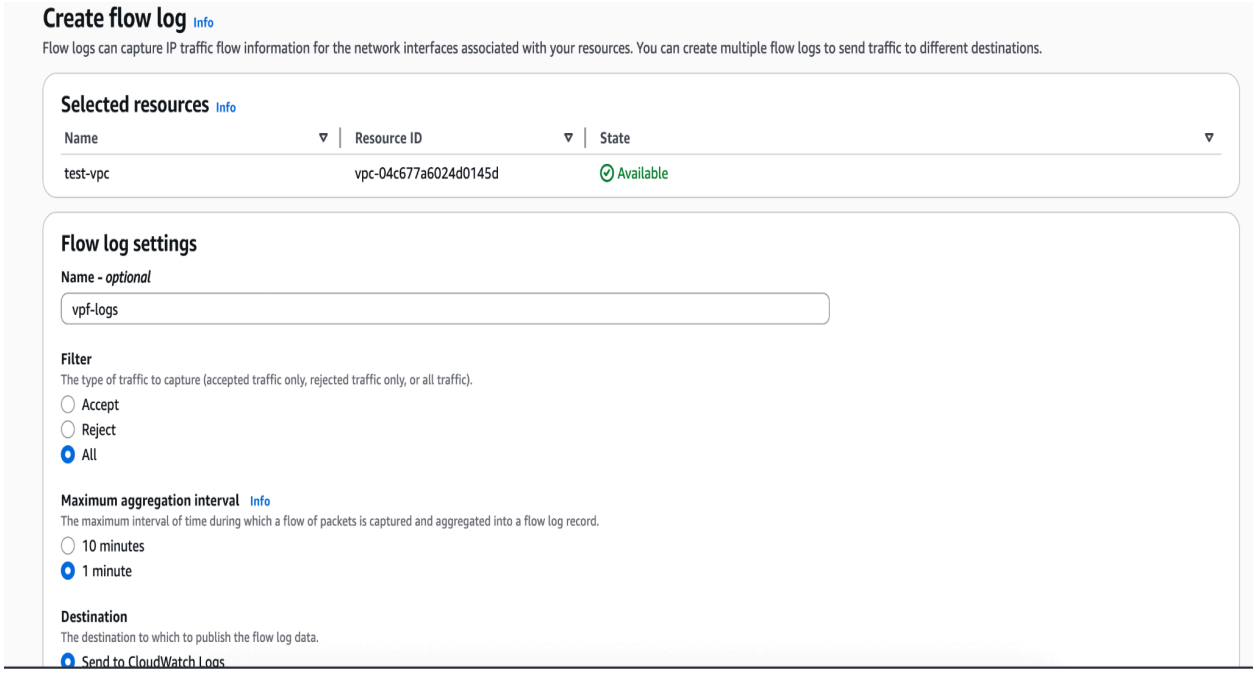
```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

- Attach this IAM role to your account or the service creating the flow log.

8. Create the VPC Flow Log

- Go to **VPC > Your VPC > Flow Logs tab**.
- Click **Create Flow Log**.
- Select:
  - **Resource Type**: VPC, Subnet, or Network Interface (ENI)
  - **Destination**: CloudWatch Logs
  - **Log Group**: Select the one you created
  - **IAM Role**: Select the role with the right permissions



9. Verify the Flow Logs

- Go to **CloudWatch > Log Groups**.
- Open your log group and check for log streams.
- Open a log stream to view entries of traffic data.

2025-05-28T12:12:49.269Z	INIT_START Runtime Version: python:3.9.v94 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:b0187a72e2a…
2025-05-28T12:12:49.547Z	START RequestId: 9f098412-5d2b-4698-af54-22b088ab4fc6 Version: $LATEST
2025-05-28T12:12:49.547Z	[INFO] 2025-05-28T12:12:49.547Z 9f098412-5d2b-4698-af54-22b088ab4fc6 {'RequestType': 'Create', 'ServiceToken'…
2025-05-28T12:12:49.548Z	[INFO] 2025-05-28T12:12:49.547Z 9f098412-5d2b-4698-af54-22b088ab4fc6 35
2025-05-28T12:12:49.733Z	[INFO] 2025-05-28T12:12:49.733Z 9f098412-5d2b-4698-af54-22b088ab4fc6 Found credentials in environment variabl…
2025-05-28T12:12:51.815Z	[INFO] 2025-05-28T12:12:51.815Z 9f098412-5d2b-4698-af54-22b088ab4fc6 https://cloudformation-custom-resource-r…
2025-05-28T12:12:51.815Z	Response body:
2025-05-28T12:12:51.815Z	{"Status": "SUCCESS", "Reason": "See the details in CloudWatch Log Stream: 2025/05/28/[$LATEST]4c5b1e1764ac40…
2025-05-28T12:12:52.152Z	Status code: OK
2025-05-28T12:12:52.171Z	END RequestId: 9f098412-5d2b-4698-af54-22b088ab4fc6
2025-05-28T12:12:52.171Z	REPORT RequestId: 9f098412-5d2b-4698-af54-22b088ab4fc6 Duration: 2624.32 ms Billed Duration: 2625 ms Memory S…

Conclusion

VPC Flow Logs are a powerful tool for gaining visibility into the network traffic within your AWS environment. By capturing IP-level data about traffic to and from network interfaces, Flow Logs help in monitoring activity, troubleshooting connectivity issues, detecting potential security threats, and maintaining compliance.

Through this setup, we learned how to:

- Create a VPC with public and private subnets,
- Set up logging infrastructure using CloudWatch,
- Assign the necessary IAM permissions, and
- Enable and verify VPC Flow Logs.

This foundational knowledge is essential for anyone working with AWS networking, security monitoring, or cloud infrastructure management.