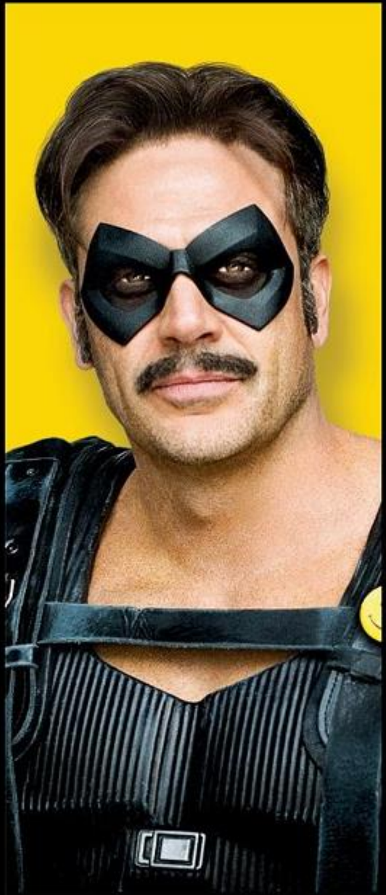
BeSA

# WATCHMEN

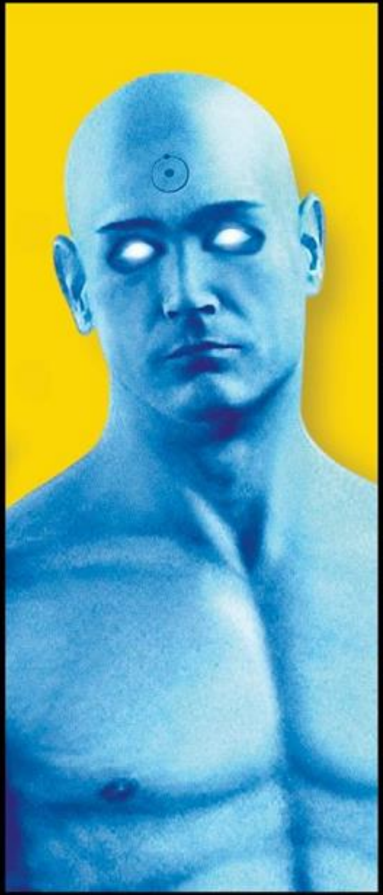
## OF NETWORK OBSERVABILITY

**Live Session**
25th May
9.00 AM UK



AWS Network Manager

Network Access Analyzer



VPC Flow Logs

Reachability Analyzer

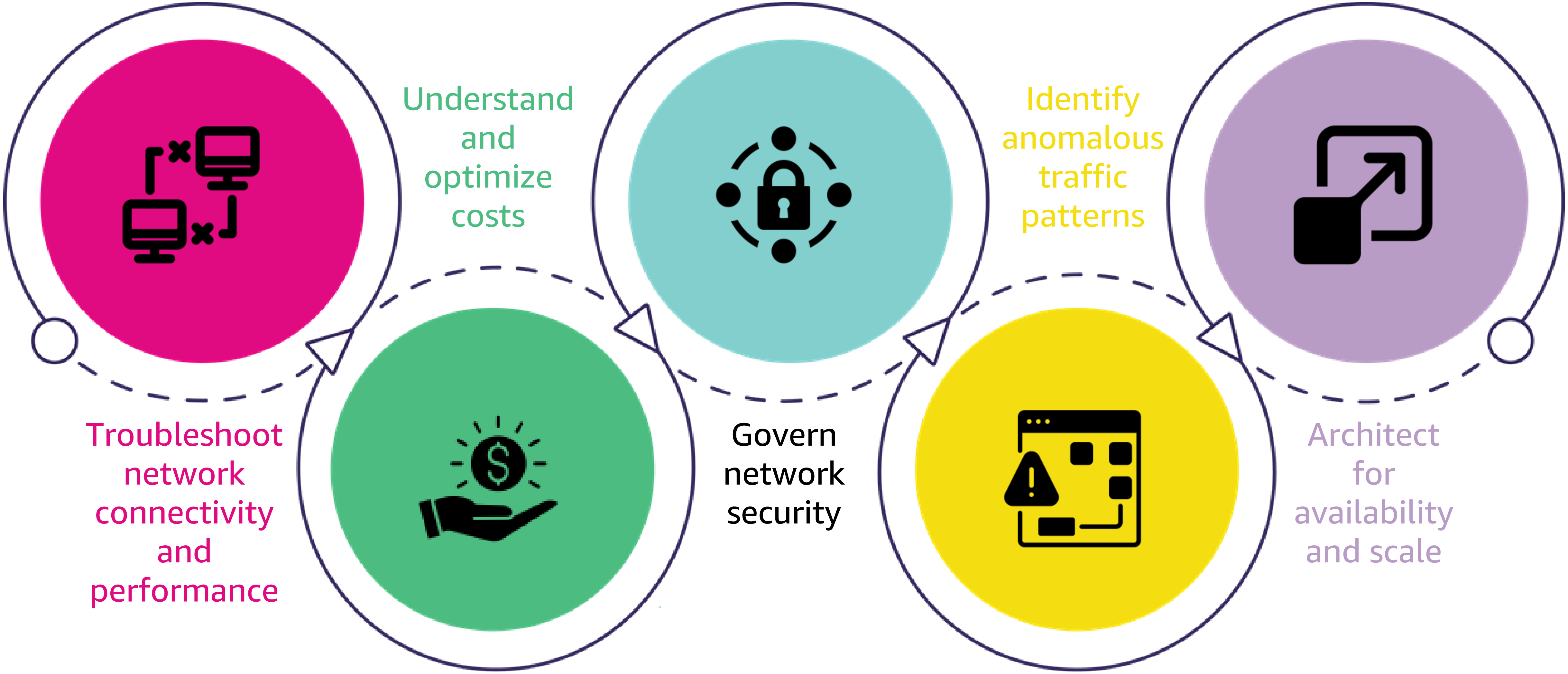
Route 53 Logs

VPC Traffic Mirroring

# Network Observability

# Network Observability

# Why observe your network?



Troubleshoot network connectivity and performance

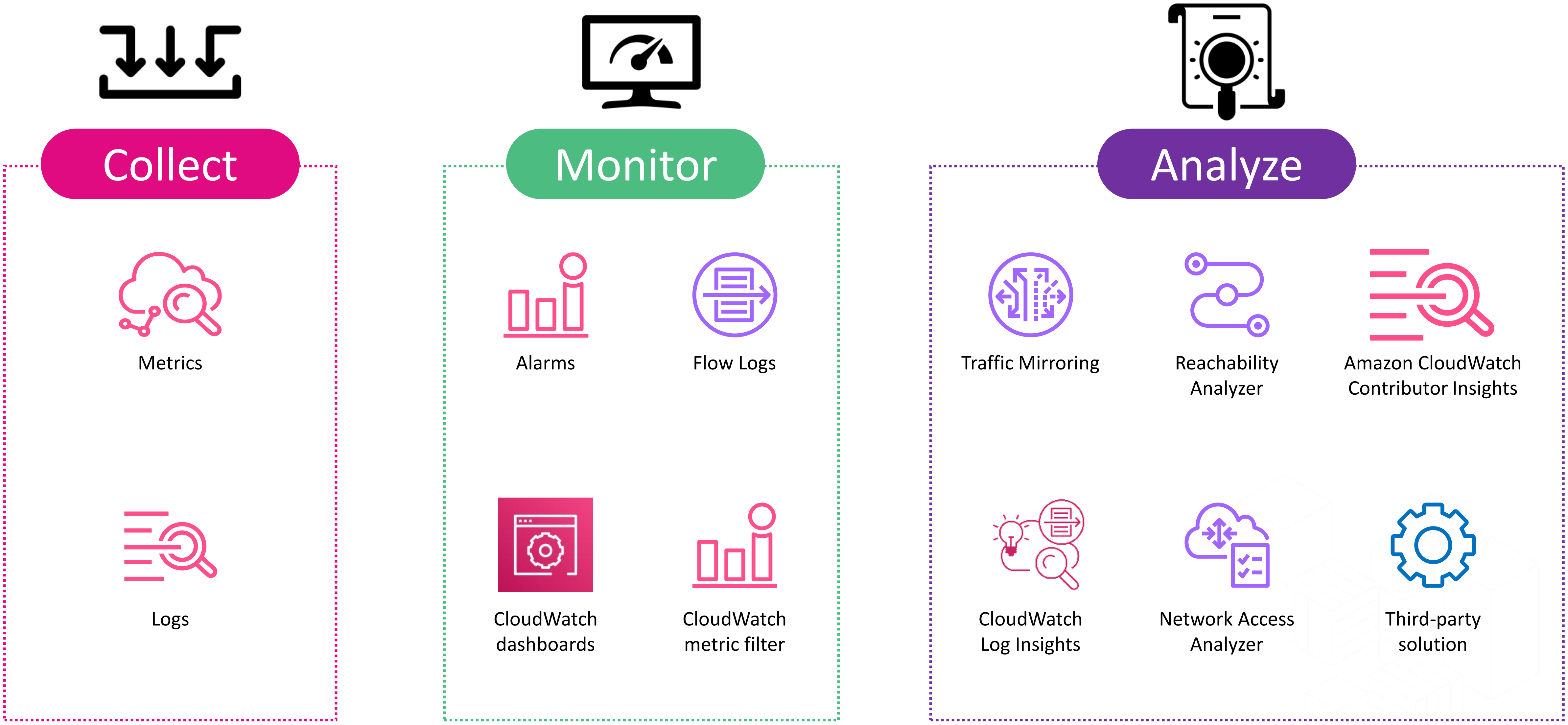
Understand and optimize costs

Govern network security

Identify anomalous traffic patterns

Architect for availability and scale

# Overview of network observability



## Collect

- Metrics
- Logs

## Monitor

- Alarms
- Flow Logs
- CloudWatch dashboards
- CloudWatch metric filter

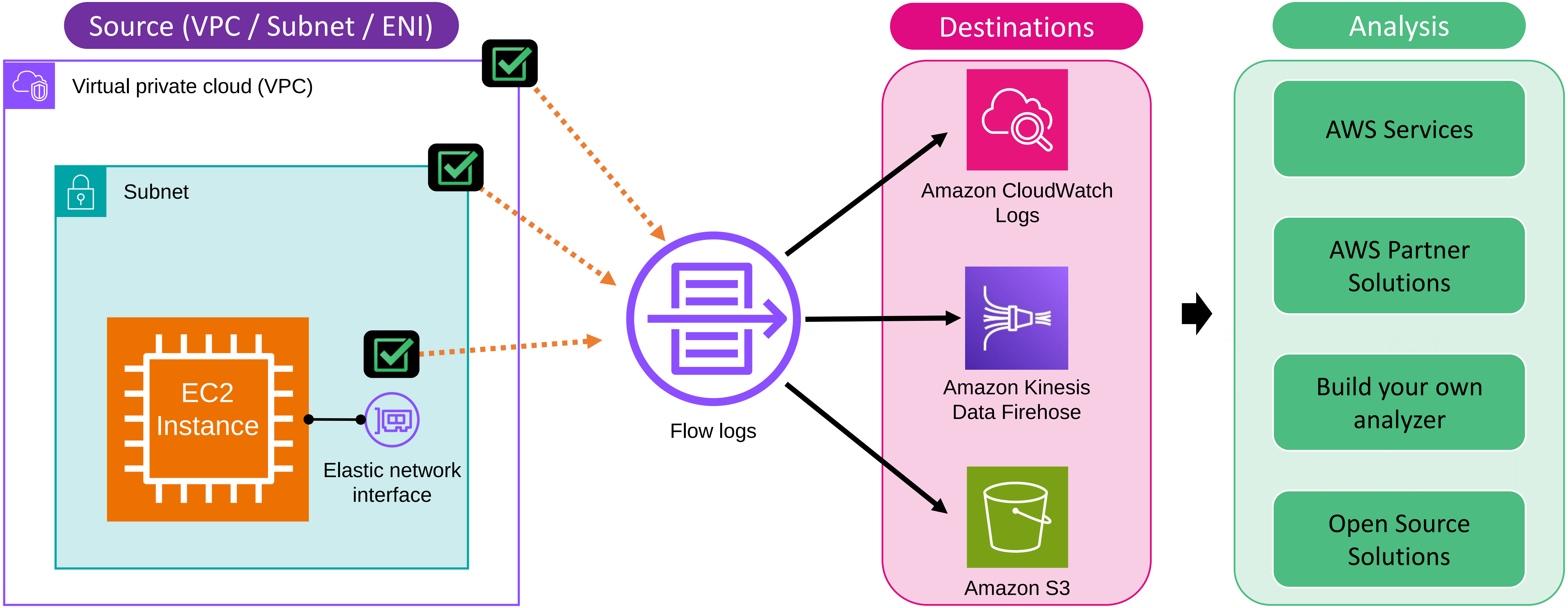
## Analyze

- Traffic Mirroring
- Reachability Analyzer
- Amazon CloudWatch Contributor Insights
- CloudWatch Log Insights
- Network Access Analyzer
- Third-party solution

# VPC Flow Logs

# VPC Flow Logs

- 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.



# Key Facts

**Doesn't affect performance**

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency.

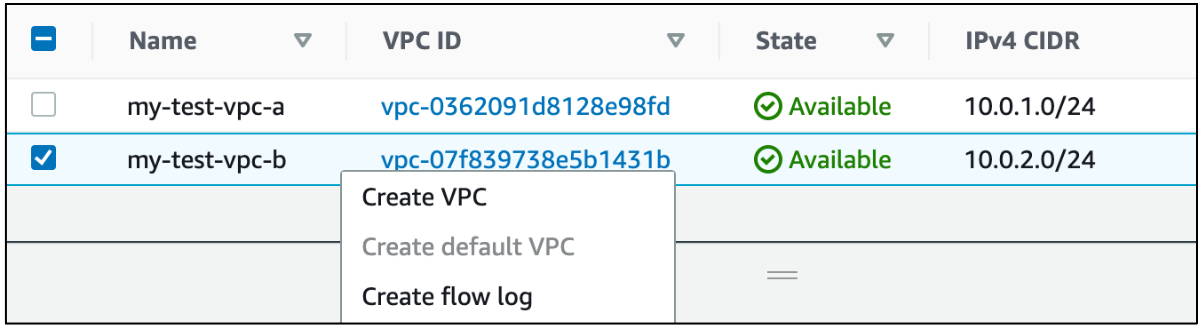
**Not real-time**

After you create a flow log, it can take several minutes to begin collecting and publishing data to the chosen destinations. Flow logs do not capture real-time log streams.

**Choice of Format**

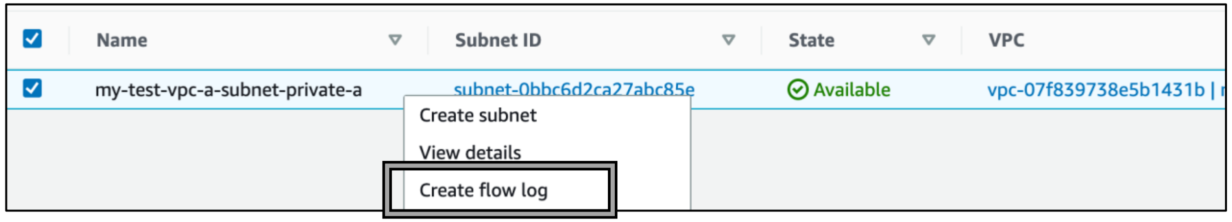
When you create a flow log, you can use the default format for the flow log record, or you can specify a custom format.

# Capturing Flow logs



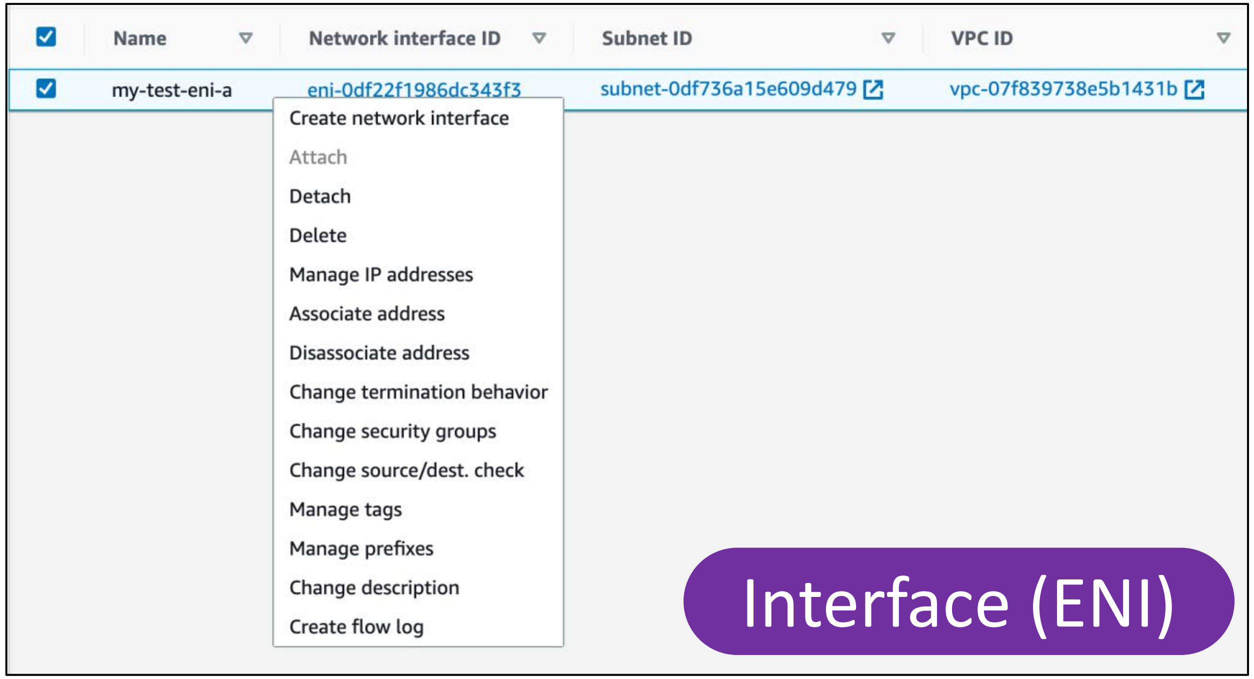
| ☐ | Name | VPC ID | State | IPv4 CIDR |
|---|---|---|---|---|
| ☐ | my-test-vpc-a | vpc-0362091d8128e98fd | ✓ Available | 10.0.1.0/24 |
| ☑ | my-test-vpc-b | vpc-07f839738e5b1431b | ✓ Available | 10.0.2.0/24 |

VPC



| ☑ | Name | Subnet ID | State | VPC |
|---|---|---|---|---|
| ☑ | my-test-vpc-a-subnet-private-a | subnet-0bbc6d2ca27abc85e | ✓ Available | vpc-07f839738e5b1431b \| r |

Subnet



| ☑ | Name | Network interface ID | Subnet ID | VPC ID |
|---|---|---|---|---|
| ☑ | my-test-eni-a | eni-0df22f1986dc343f3 | subnet-0df736a15e609d479 | vpc-07f839738e5b1431b |

Interface (ENI)

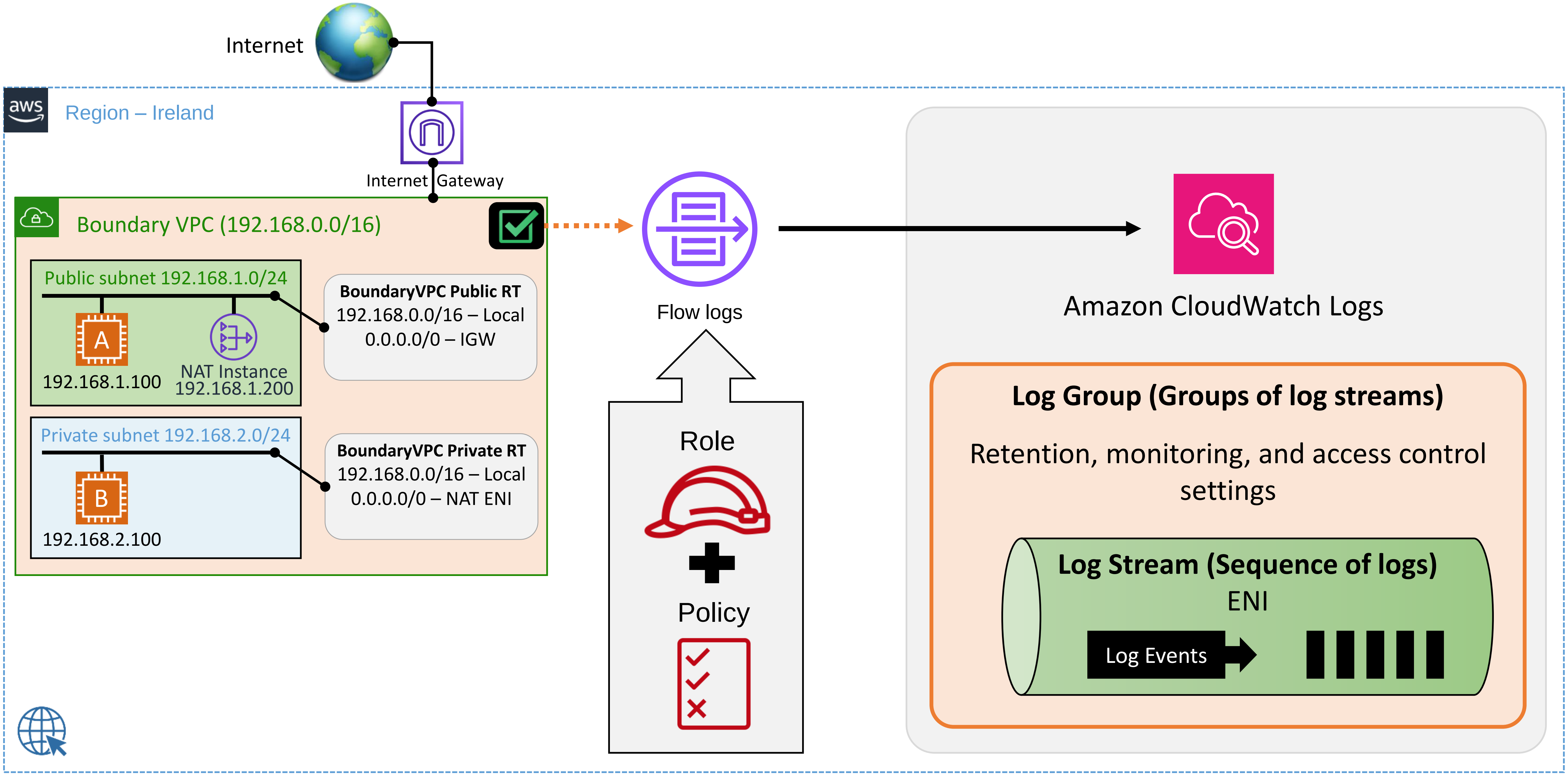
# Workshop

Networking Workshop 0.2

VPCs, Subnets, Peering, Transit Gateways, VPNs and Traffic Mirroring

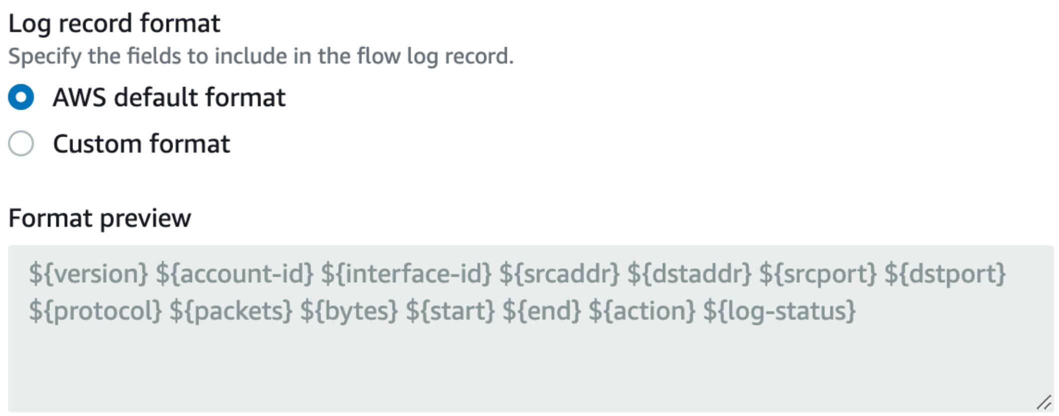
Labs and Instructions

# Demo Environment



# Flow Log Fields

## Default flow log fields



Log record format

Specify the fields to include in the flow log record.

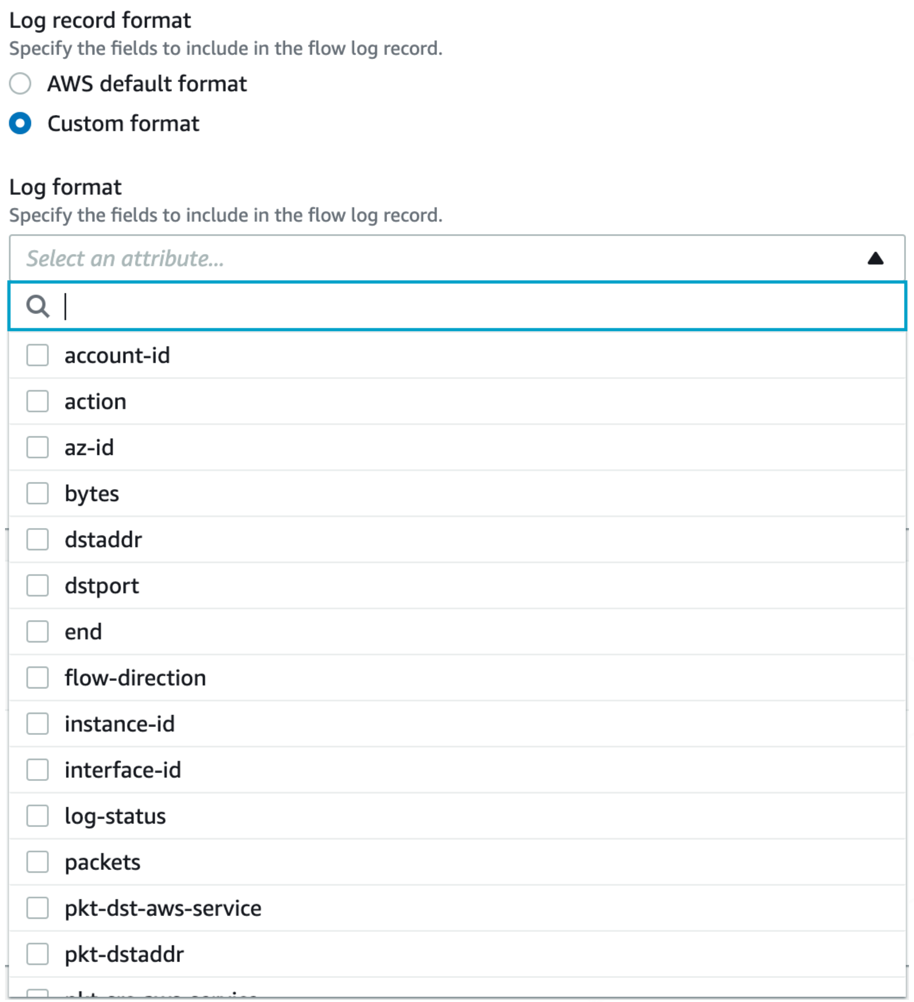
● AWS default format

○ Custom format

Format preview

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

## Custom flow log fields



Log record format

Specify the fields to include in the flow log record.

○ AWS default format

● Custom format

Log format

Specify the fields to include in the flow log record.

- □ account-id
- □ action
- □ az-id
- □ bytes
- □ dstaddr
- □ dstport
- □ end
- □ flow-direction
- □ instance-id
- □ interface-id
- □ log-status
- □ packets
- □ pkt-dst-aws-service
- □ pkt-dstaddr

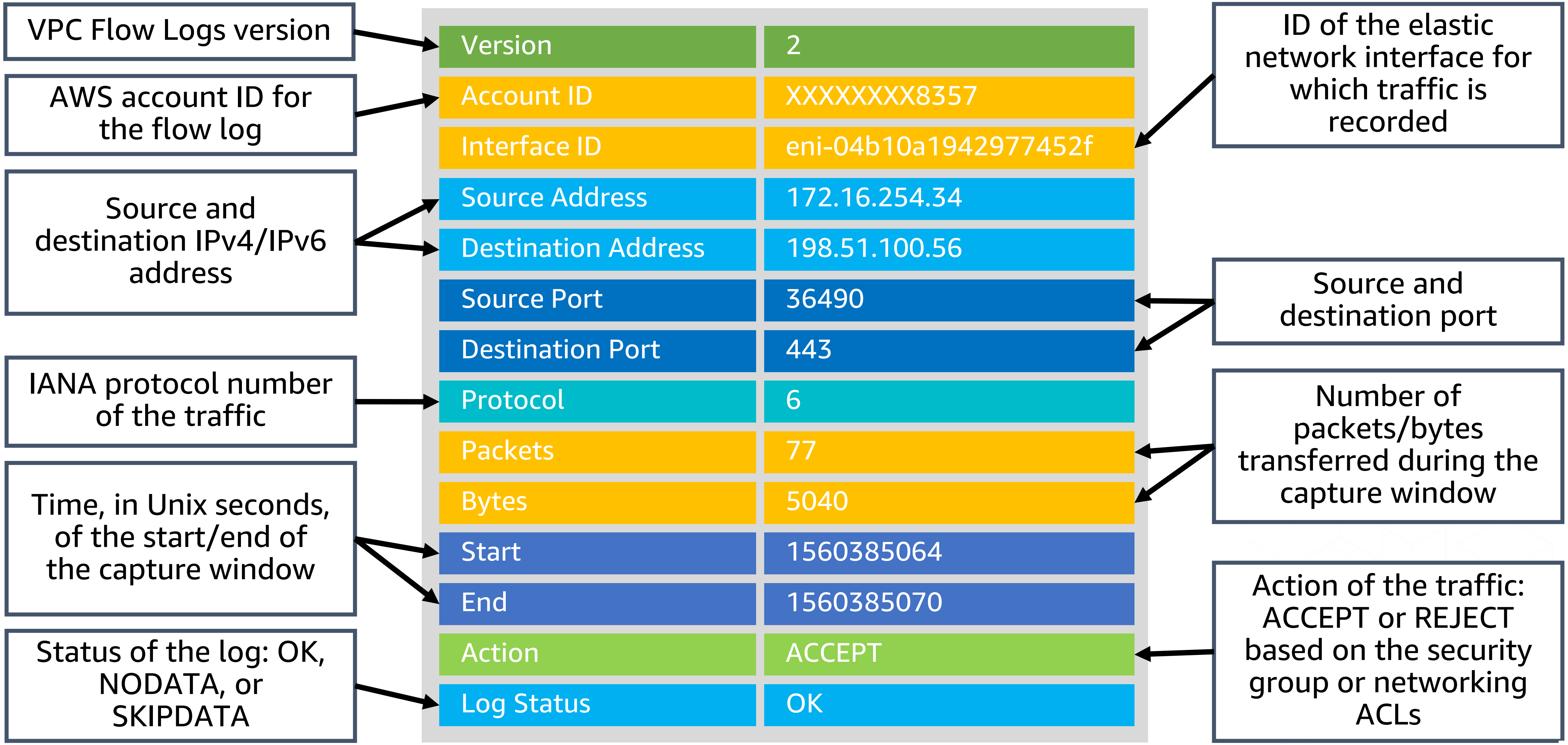
# Additional Flow Log Fields that can be captured with a custom format:

| VPC Flow Log Fields | Version |
|---|---|
| VPC id | 3 |
| Subnet id | 3 |
| Instance id | 3 |
| TCP Flags (e.g. SYN, ACK, FIN) | 3 |
| Type (IPv4, IPv6) | 3 |
| Packet Source Address | 3 |
| Packet Destination Address | 3 |

| VPC Flow Log Fields | Version |
|---|---|
| Region | 4 |
| Availability Zone ID | 4 |
| Sublocation-type | 4 |
| Sublocation-id | 4 |

| VPC Flow Log Fields | Version |
|---|---|
| Pkt-src-aws-service | 5 |
| Pkt-dst-aws-service | 5 |
| Flow-direction | 5 |
| Traffic-path | 5 |

# Anatomy of a Flow Log



| | |
|---|---|
| Version | 2 |
| Account ID | XXXXXXXX8357 |
| Interface ID | eni-04b10a1942977452f |
| Source Address | 172.16.254.34 |
| Destination Address | 198.51.100.56 |
| Source Port | 36490 |
| Destination Port | 443 |
| Protocol | 6 |
| Packets | 77 |
| Bytes | 5040 |
| Start | 1560385064 |
| End | 1560385070 |
| Action | ACCEPT |
| Log Status | OK |

VPC Flow Logs version

AWS account ID for the flow log

Source and destination IPv4/IPv6 address

IANA protocol number of the traffic

Time, in Unix seconds, of the start/end of the capture window

Status of the log: OK, NODATA, or SKIPDATA

ID of the elastic network interface for which traffic is recorded

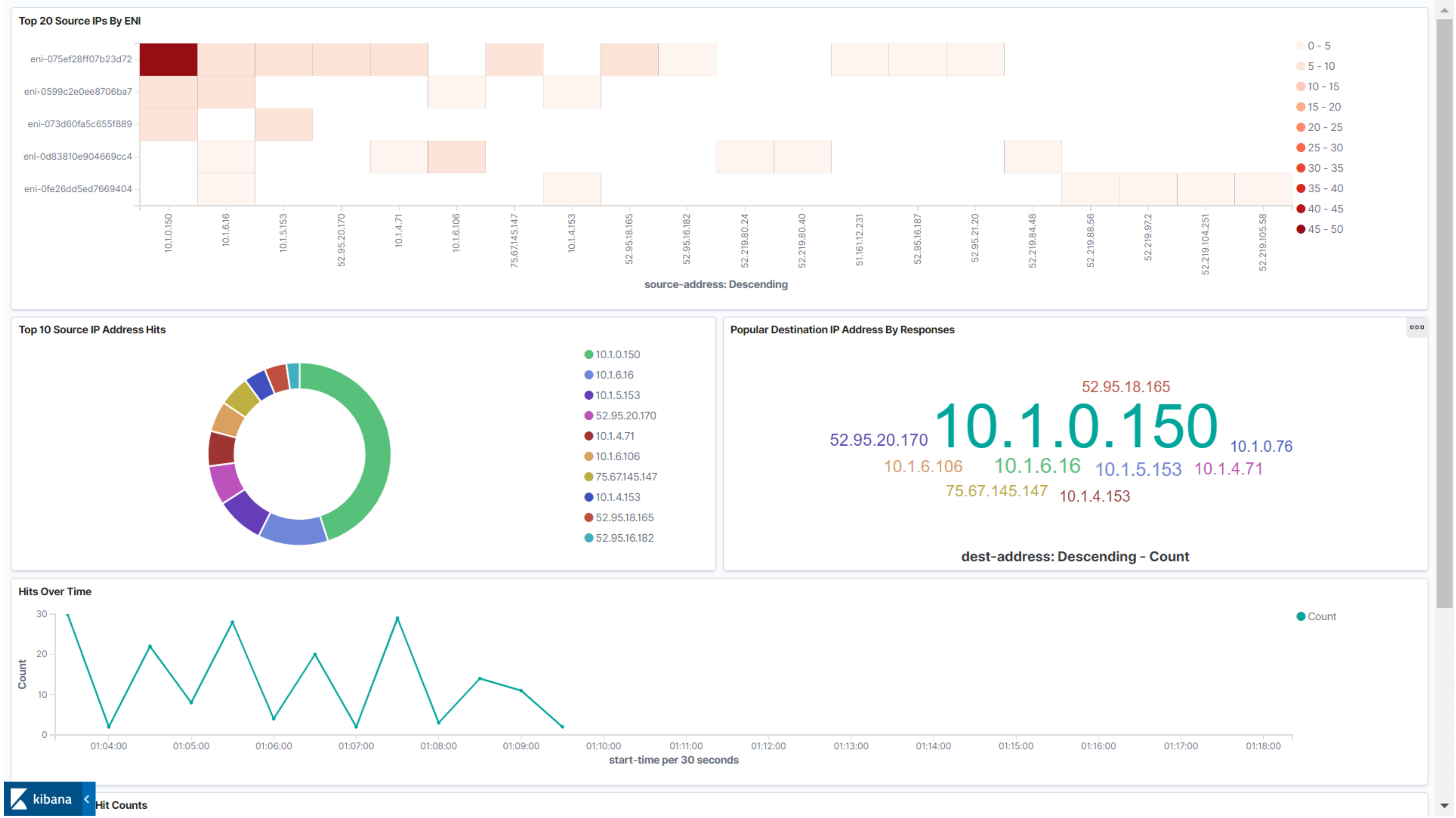
Source and destination port

Number of packets/bytes transferred during the capture window

Action of the traffic: ACCEPT or REJECT based on the security group or networking ACLs

# VPC Flow logs analysis using Amazon Elasticsearch service

- https://vpc-flowlogs.aesworkshops.com/



# VPC Traffic Mirroring

# VPC Traffic Mirroring – Use-cases

Content Inspection

Threat Monitoring

Troubleshooting

- Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from an elastic network interface (ENI).
- You can then send the traffic to out-of-band security and monitoring appliances

# VPC Traffic Mirroring

- Amazon VPC traffic mirroring replicates network traffic to and from an Amazon EC2 instance and forward it to security and monitoring appliances.
- These appliances can be deployed on an individual EC2 instance or a fleet of instances behind a Network Load Balancer (NLB) with User Datagram Protocol (UDP) listener.
- Traffic mirroring supports network packet captures at the Elastic Network Interface (ENI) level for EC2 instances.
- Customers can either use open source tools or choose from a wide-range of monitoring solution available on AWS Marketplace.

# Traffic Mirroring concepts

**Source**

The network interface to monitor

**Target**

The destination for mirrored traffic

**Filter**

A set of rules that defines which traffic is mirrored

**Session**

Establishes a relationship between a source, a filter, and a target

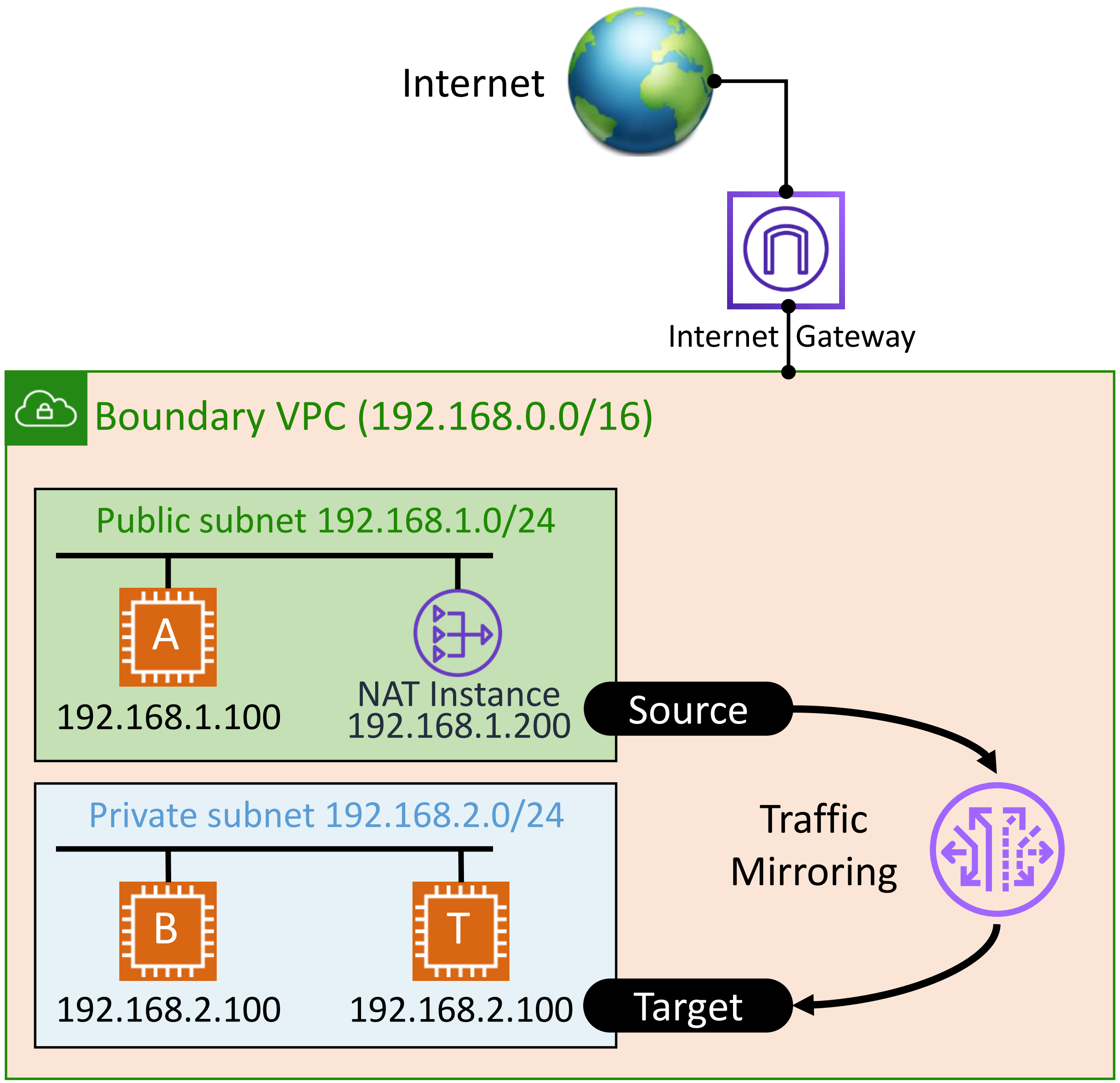
- Mirrored traffic is encapsulated with a VXLAN header.
- Virtual Extensible LAN (VXLAN) is a network virtualization technology that attempts to address the scalability problems associated with large cloud computing deployments.

# Setting up traffic mirroring

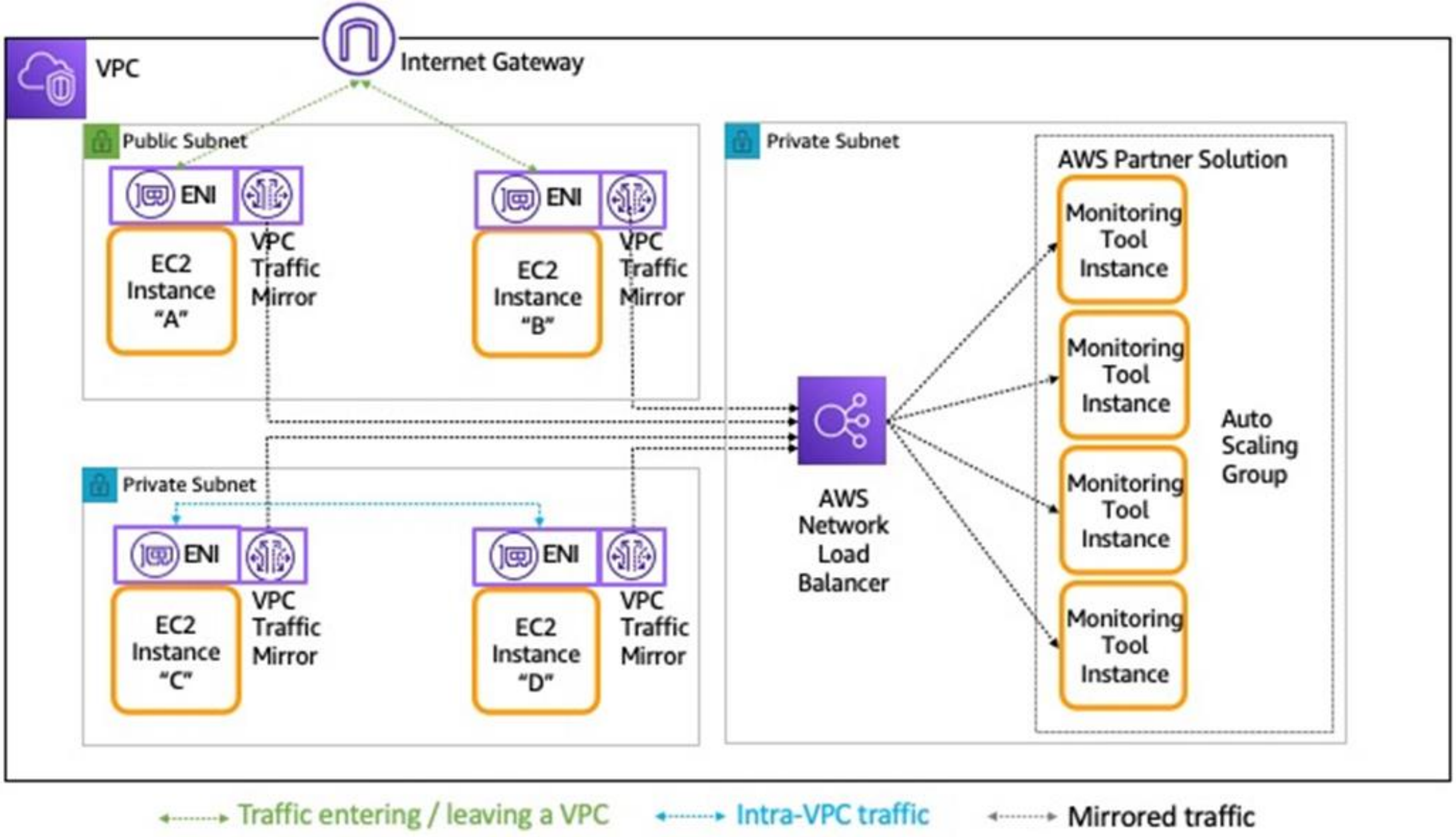
1. Creating the mirror target
2. Creating the mirror filter
3. Setting up the mirror session

## Testing the traffic mirroring

- sudo tcpdump -nni eth1



# NLB as Target



# Comparison

| VPC Flow Logs | VPC Traffic Mirroring |
|---|---|
| Captures information about the IP traffic in your VPC | Streams a copy of the network traffic from an ENI to a target |
| Can be enabled for:<br>• VPC, Subnet or ENI | Can be captured from:<br>• ENI |
| Target:<br>• CW Logs, Kinesis Firehose, Amazon S3 | Target:<br>• ENI of an instance, NLB, GWLB |
| Captures:<br>• Header of the packet, Metadata | Mirros:<br>• Actual packet (including payload) |
| Use-cases: Troubleshoot connectivity and security issues | Use-cases: Content inspection, Threat monitoring, Network troubleshooting |

# Cloud Career Journeys – Starter Kit | Group Mentoring Session

The Starter Kit equips you with tools and resources to transform and advance your career within 6 to 12 months.

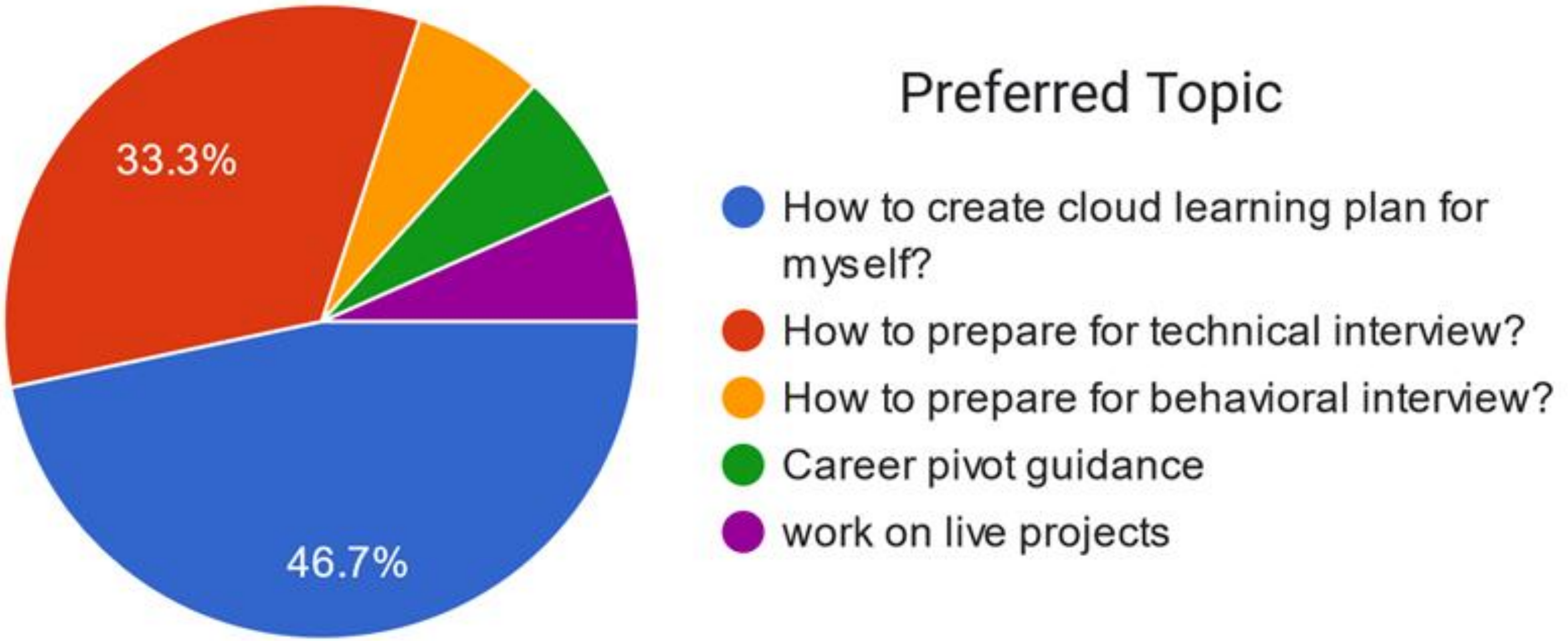
- 6 months Whizlabs Access
- 6 months Pluralsight Access
- Monthly group mentoring session
- Other resources

https://cloudcareerjourneys.com/

# Cloud Career Journeys – Starter Kit | Group Mentoring Session

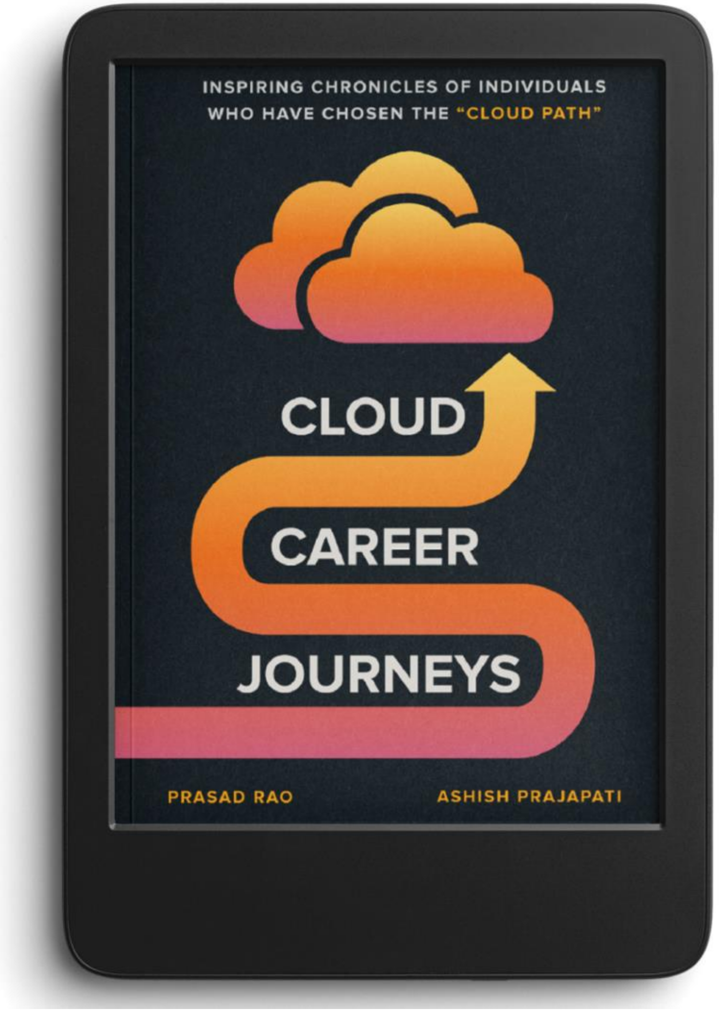
**Tentative Agenda:**

- How to get the maximum benefit from Starter-Kit? (15 mins)
- Main Topic - to be decided based on the responses (45 mins)
- Q&A - questions gathered via form and Live Q&A on career guidance (30 mins)



1st June

# Giveaway Sponsors



INSPIRING CHRONICLES OF INDIVIDUALS WHO HAVE CHOSEN THE "CLOUD PATH"

CLOUD CAREER JOURNEYS

PRASAD RAO

ASHISH PRAJAPATI

and WHIZLABS

# Giveaways

## Limited to first 50 buyers

- 50% discount on – Cloud Career Journeys – eBook
- 50% discount on – Cloud Career Journeys – Starter Kit
  - (QR Code displayed at the end of the session)

## Weekly Giveaways (Selection based on engagement)

- 1 x Cloud Career Journeys – eBook
- 10 x Whizlabs Sandbox Access for 3 months

## 12th Week Giveaways (Selection from regular participants)

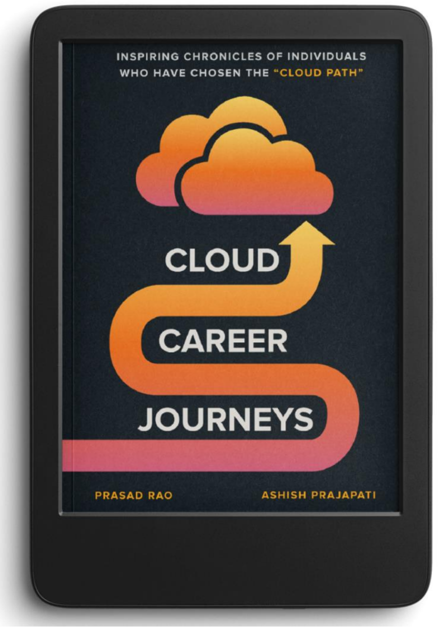
- 10 x Whizlabs Premium Plus Subscription for 12 months

# Register Here

- https://cloudcareerjourneys.gumroad.com/l/besagiveawayweek8

# Week 07 Winners

| | |
|---|---|
| Cloud Career Journey ebook | Linet Kiunga |
| Whizlabs 3 months AWS Sandbox Access | Harshita cheemakurthi |
| | Sunil Kumar |
| | Samuel Macharia |
| | Ritu Srivastava |
| | Seshu Koorella |
| | Md Saif Zamanas |
| | Swati Gupta |
| | Unni Vishawanathan |
| | Serhil Babinskyi |
| | Dmytro Voytko |


INSPIRING CHRONICLES OF INDIVIDUALS WHO HAVE CHOSEN THE "CLOUD PATH"
CLOUD
CAREER
JOURNEYS
PRASAD RAO
ASHISH PRAJAPATI