A CLOUD GURU

# Creating VPC Flow Logs



Steven Moran
TRAINING ARCHITECT

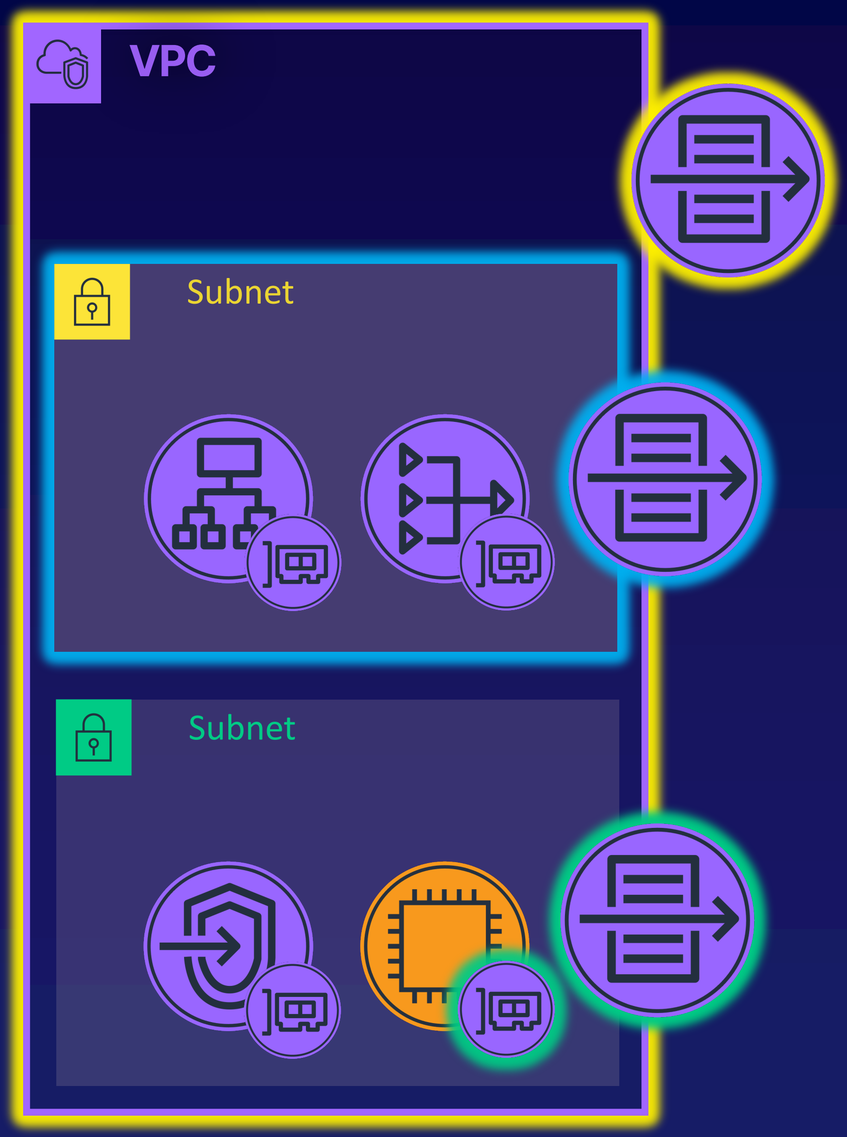
# VPC Flow Logs Overview



*Capture information about IP traffic sessions processed by elastic network interfaces in your VPC.*

# VPC Flow Logs Overview

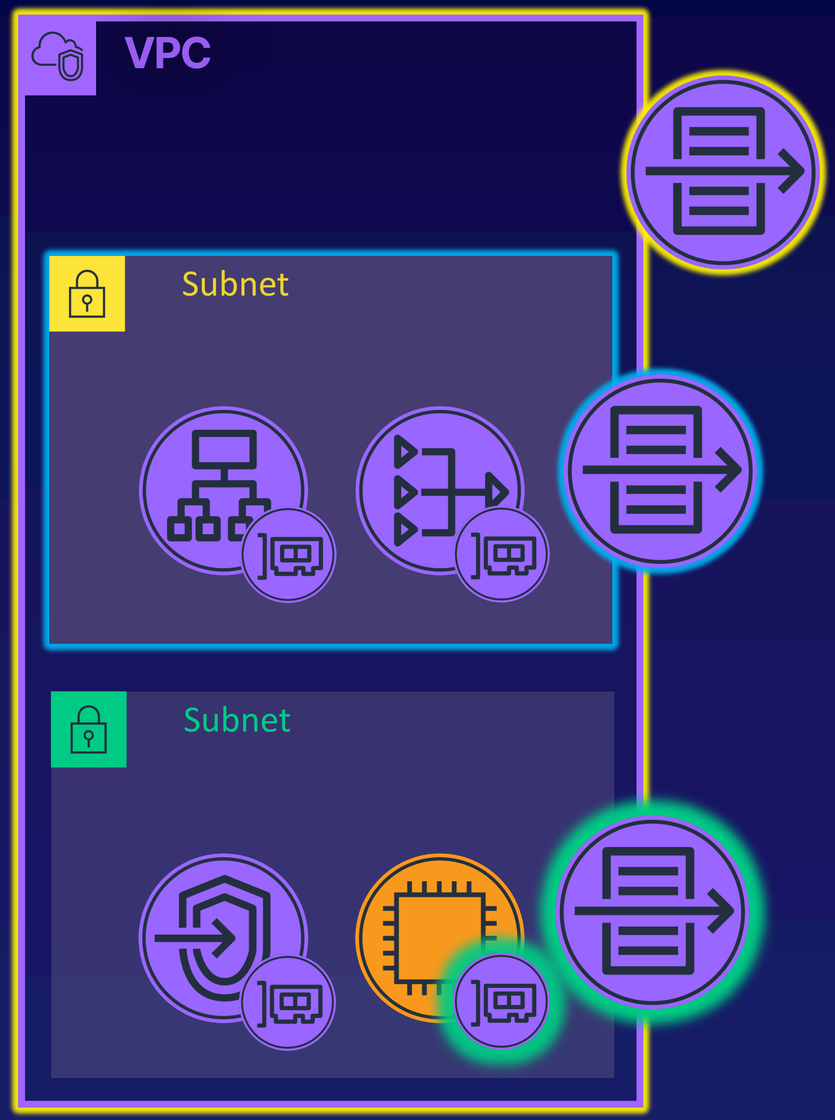





- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview

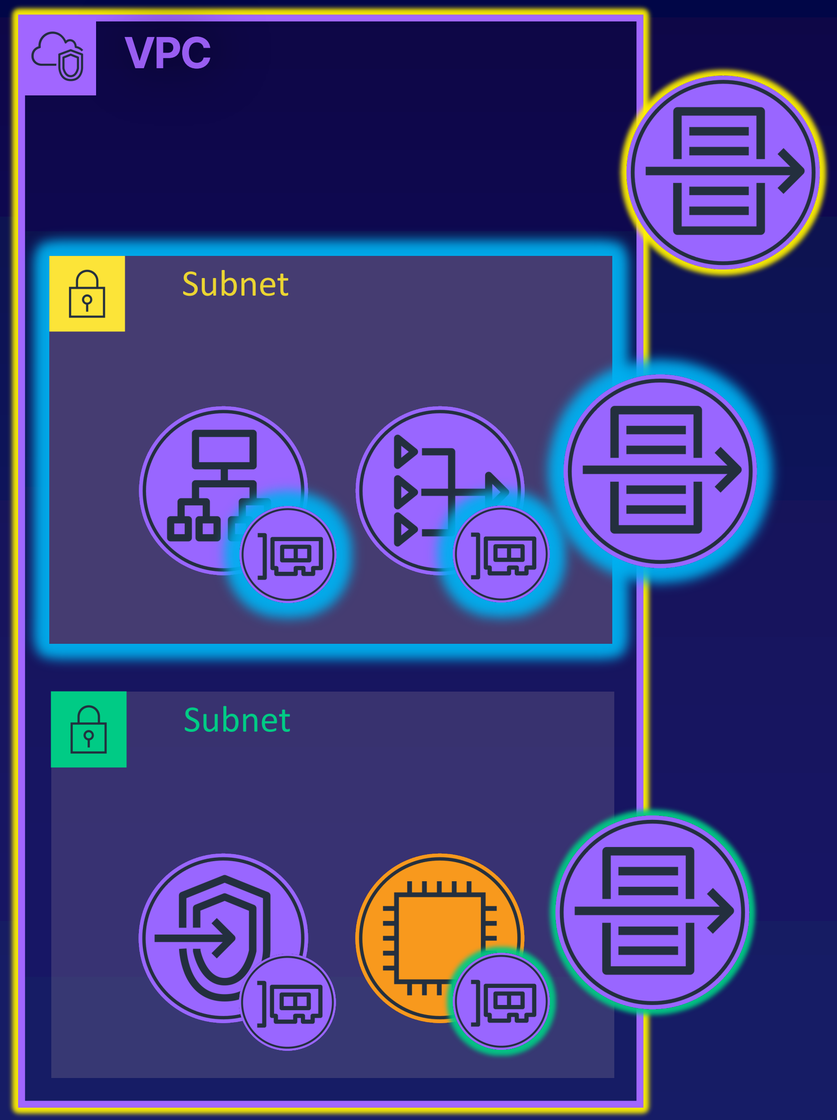





- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview

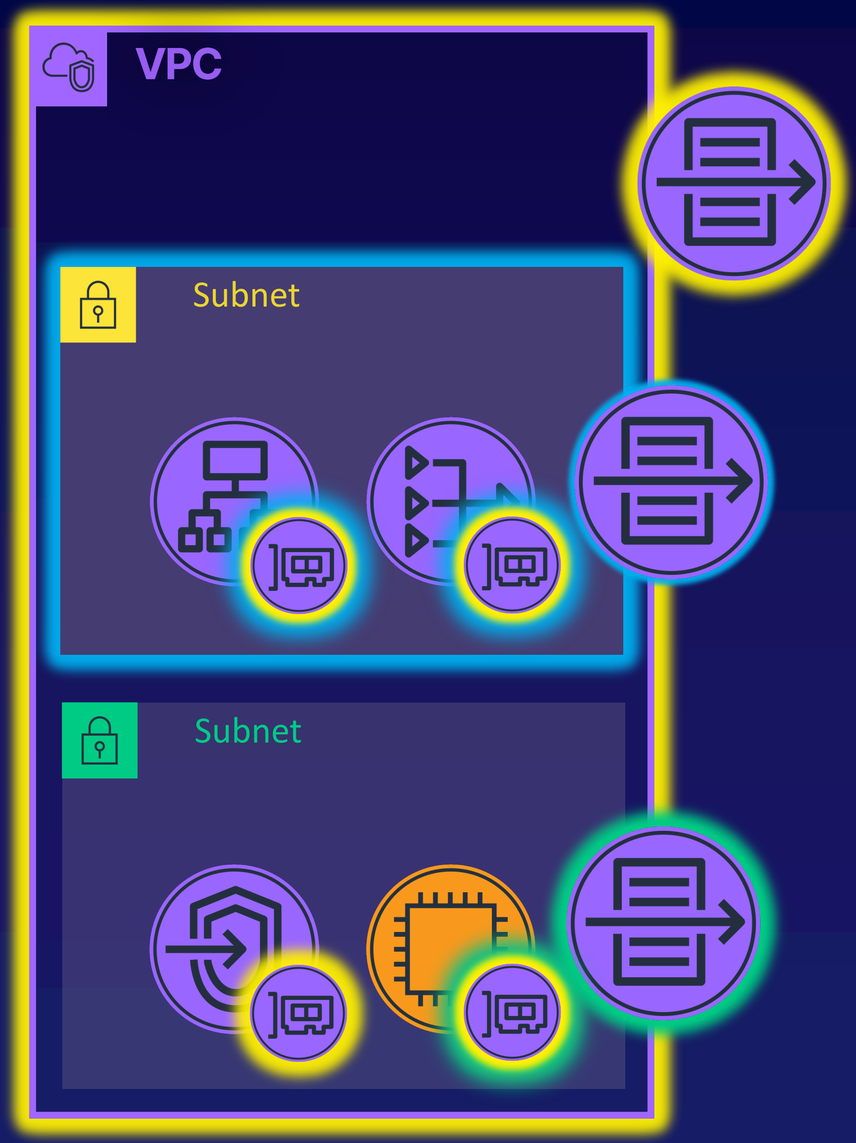





- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview

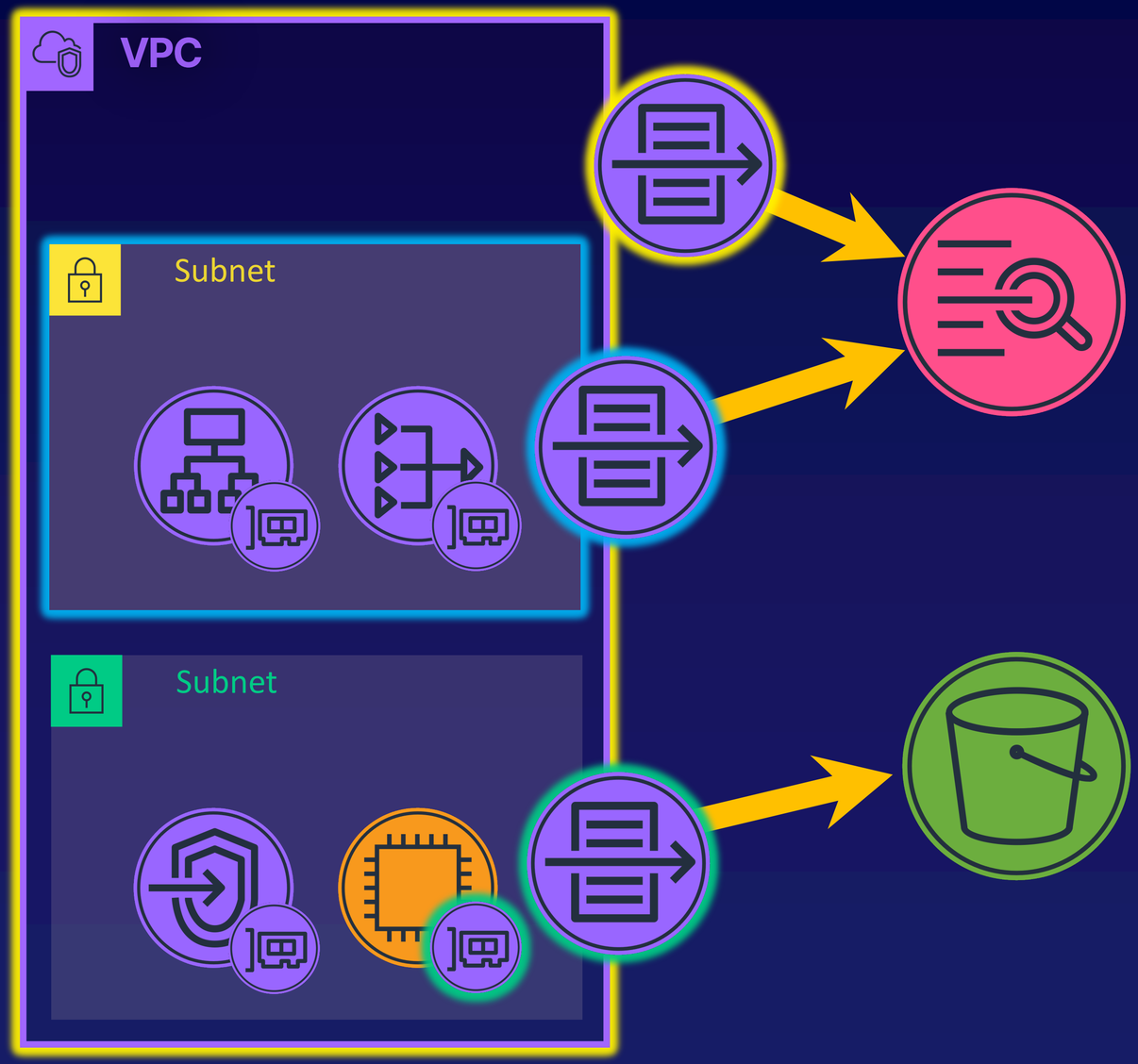





- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.
- Traffic will be logged separately for each definition.

# VPC Flow Logs Overview






- Flow log data may be sent to:
  - CloudWatch log group
    - 1 log stream per ENI
  - S3 bucket
    - 1 log file object per-publication

# Limitations



- Data reporting is not real-time.
  - Data aggregated over one- or ten-minute interval.
  - 5-10 minutes for publication to target.
- Definitions cannot be modified after creation.
- May not record “original” or “correct” IP addresses.

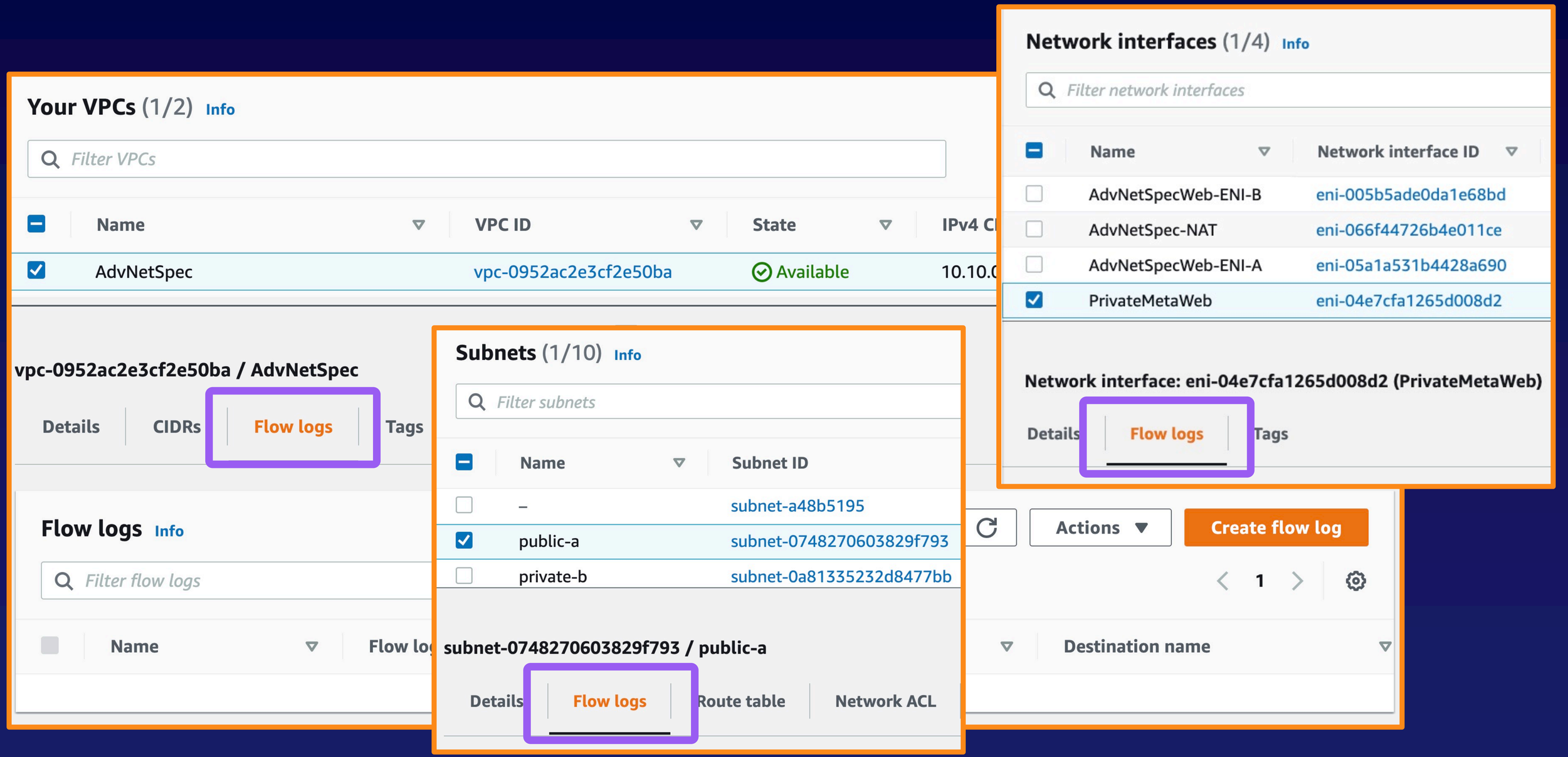
# Limitations



- Does not capture all IP traffic
  - EC2 DNS requests to Route 53
    - Requests to your own DNS servers are logged.
  - Amazon Windows license activation
  - Instance metadata
  - Amazon Time Sync Service
  - DHCP traffic
  - Default VPC router
  - Endpoint services
- Does not capture application data.

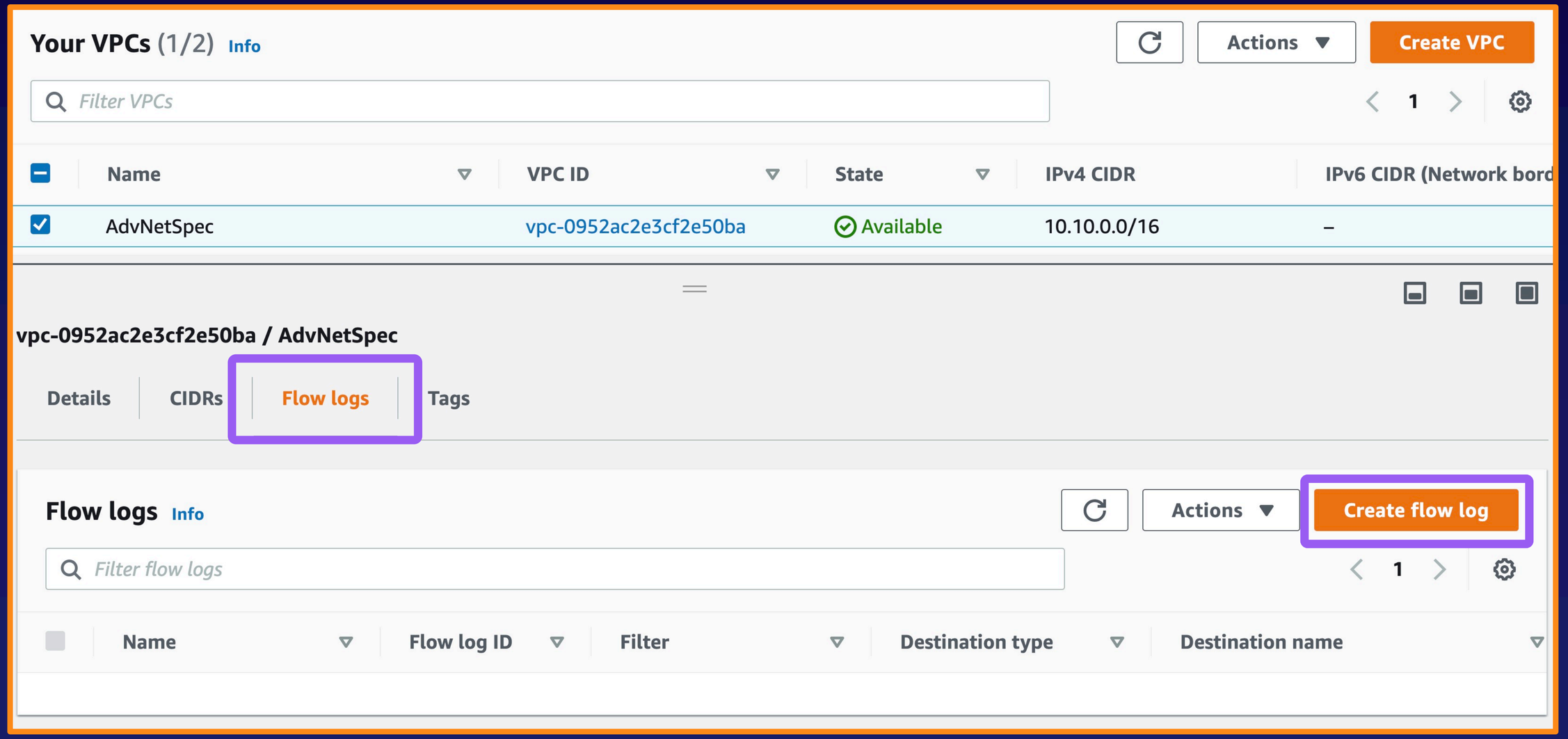
# Creating Flow Logs





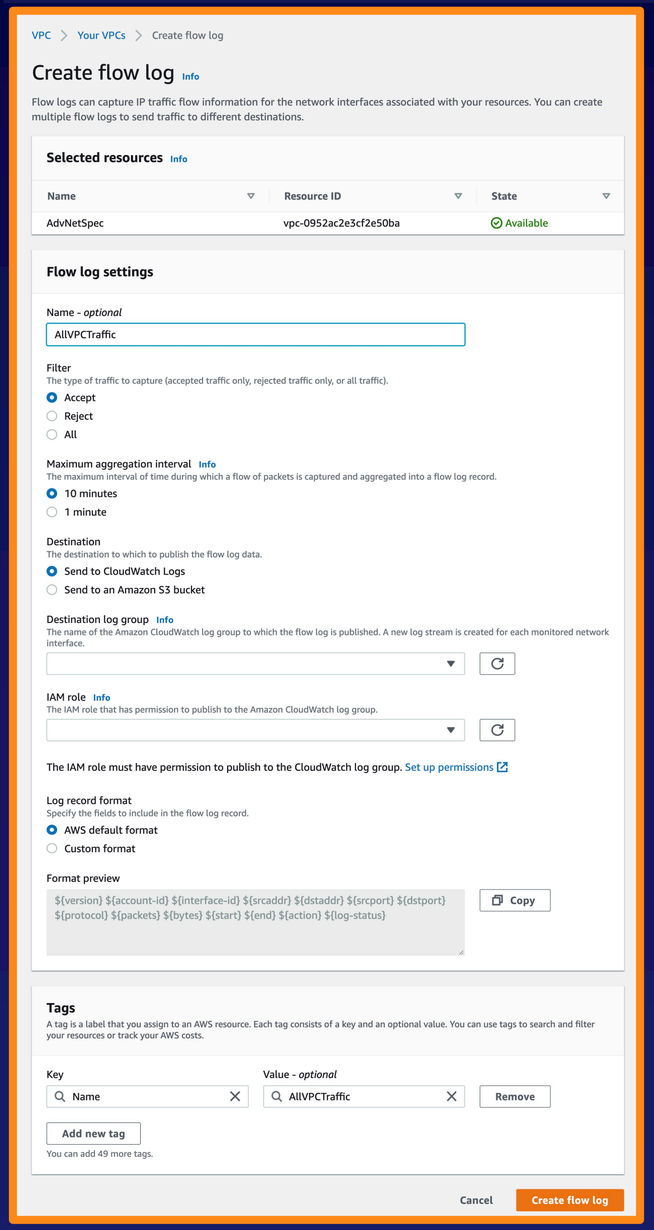
# Creating Flow Logs





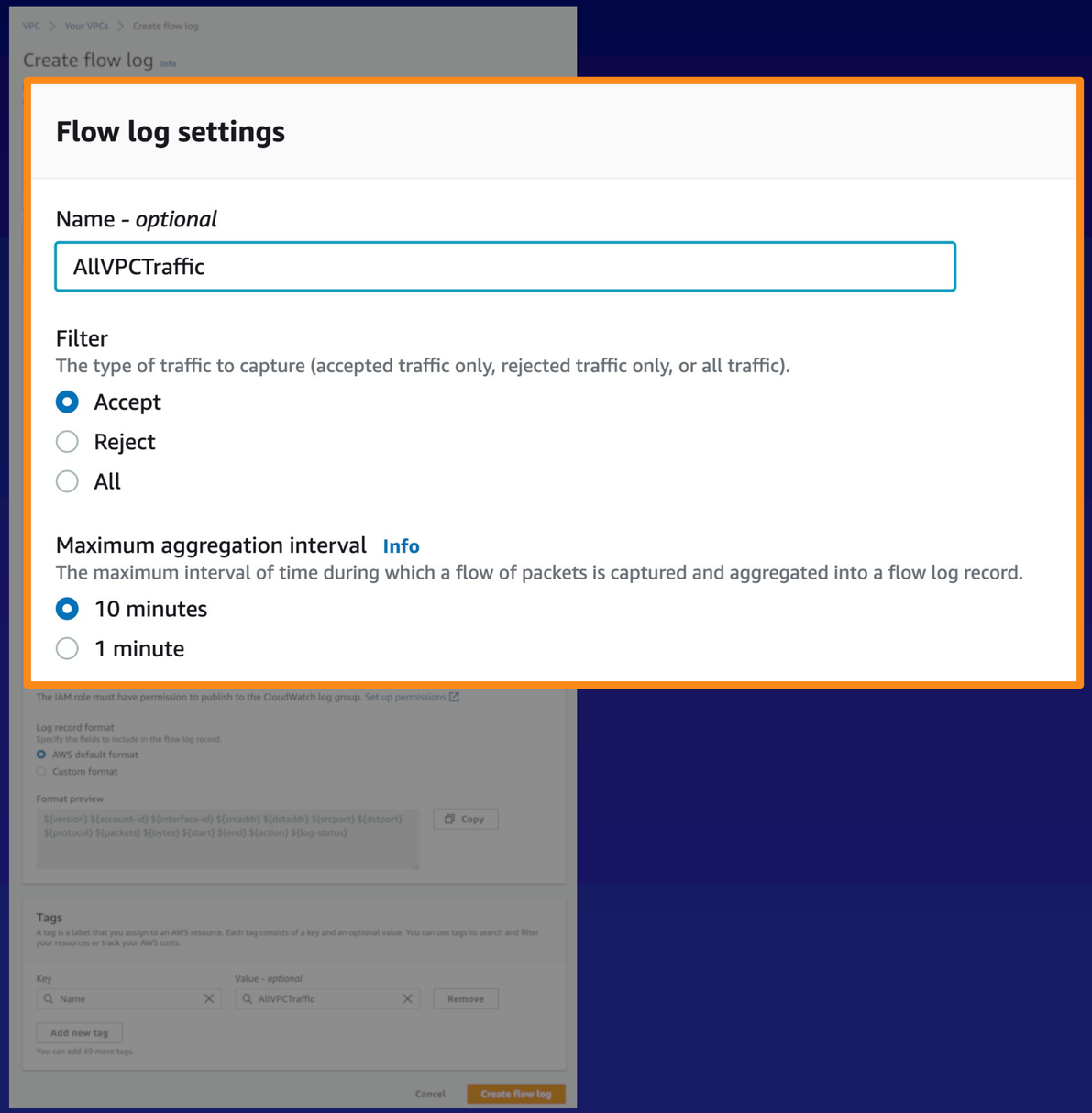
# Creating Flow Logs





# Creating Flow Logs

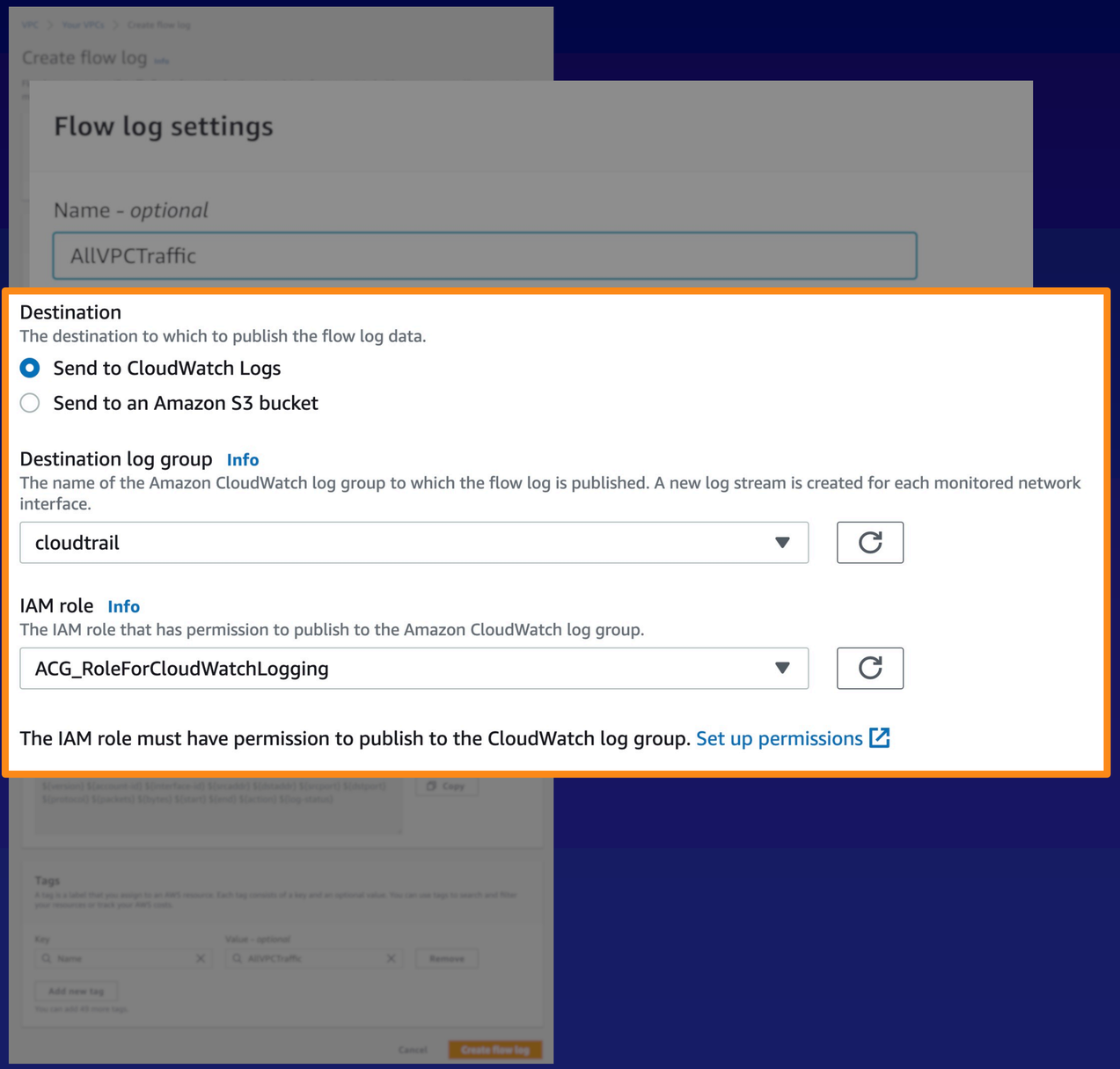





- Name
- Filter
- Maximum aggregation interval

# Creating Flow Logs

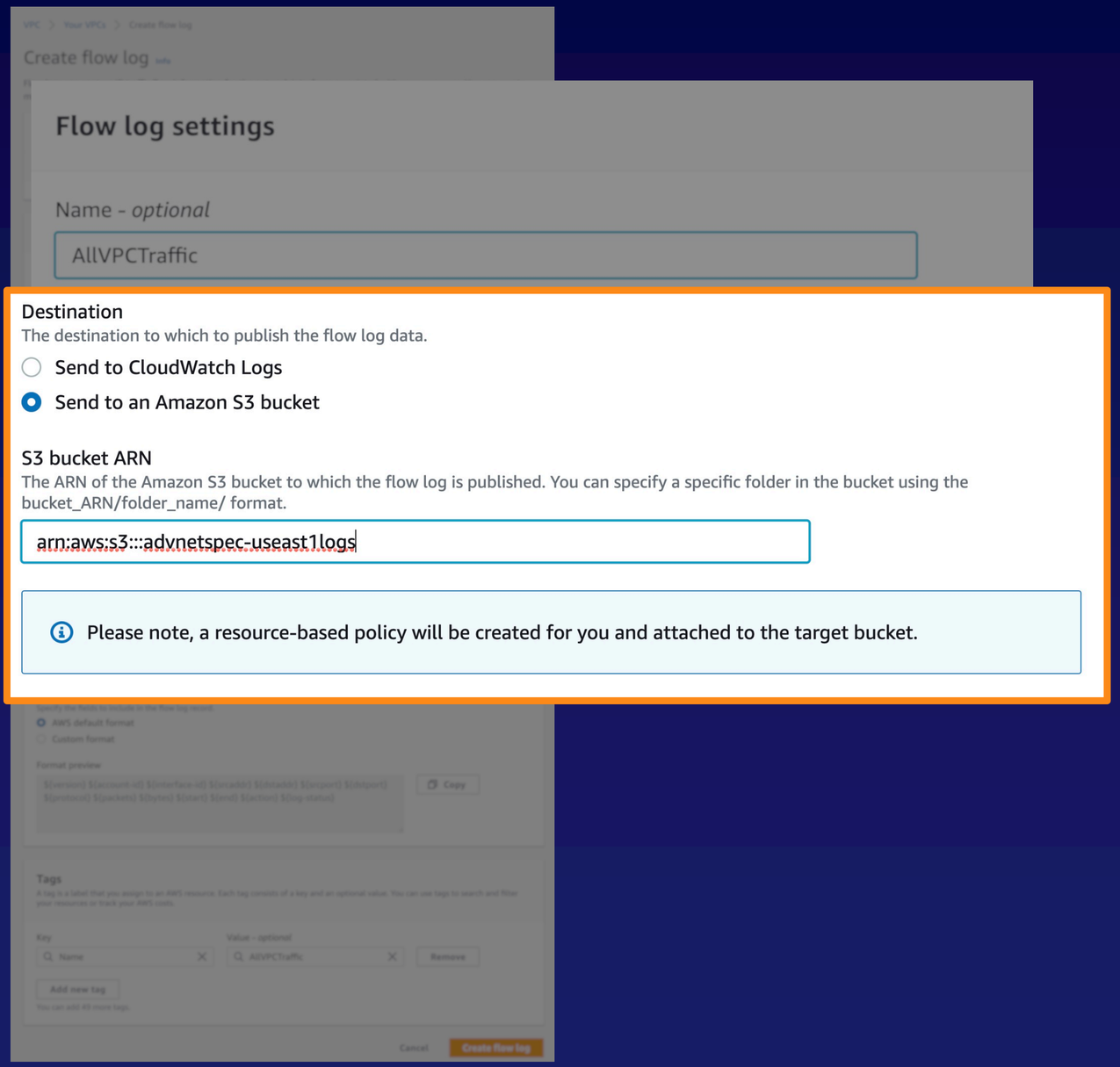
A CLOUD GURU




- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role

# Creating Flow Logs

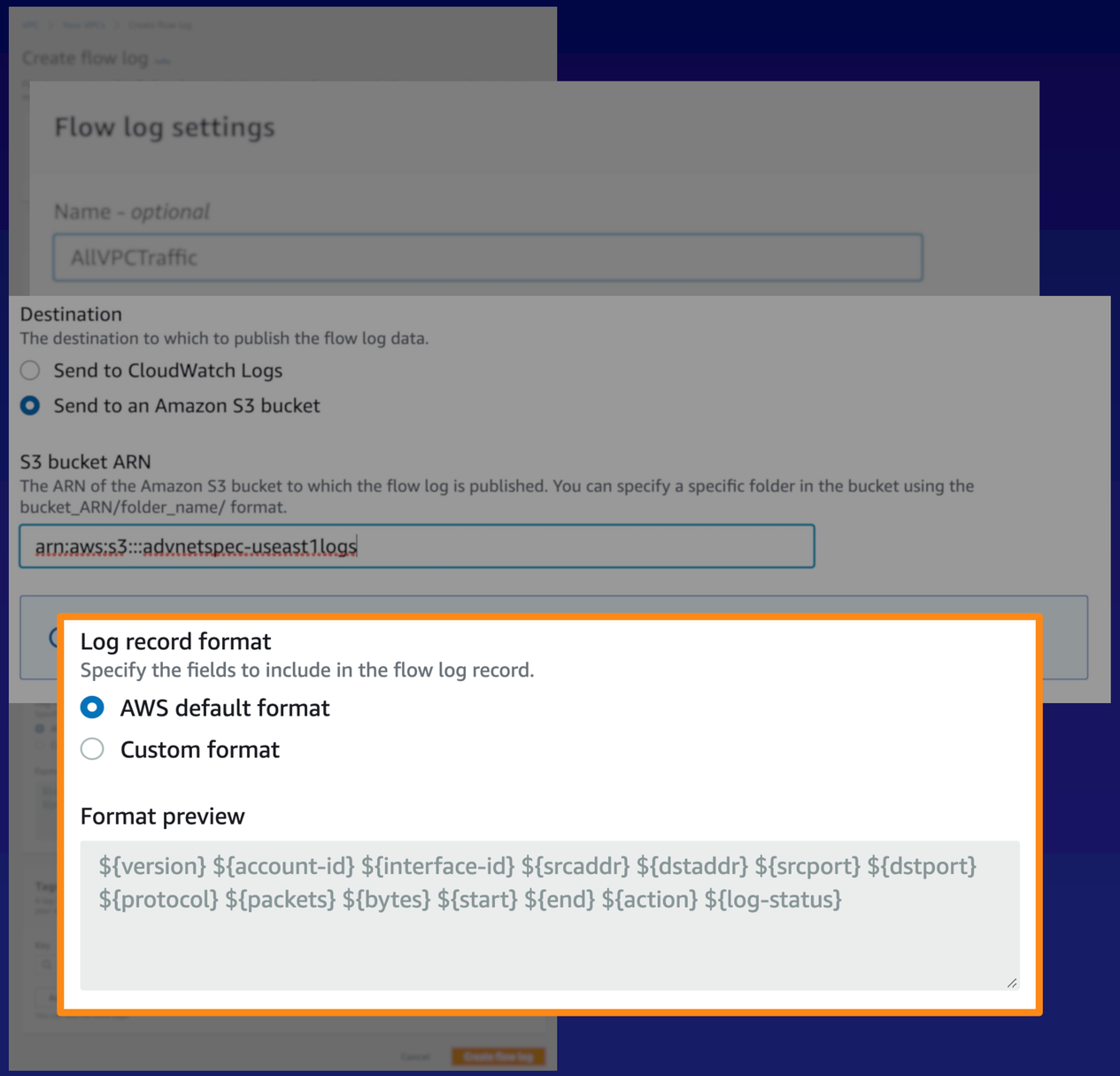





- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy

# Creating Flow Logs






- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

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

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version
- Highest field-version used in record
- AWS default format is version 2
- dstaddr
- srcport
- dstport
- protocol
- packets
- bytes
- start
- end
- action
- log-status

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version
- account-id
- interface-id
- srcaddr
- dstaddr
- srcport
- dstport
- protocol

- IP address & ports of the source and destination of link-local traffic.
- May be local or remote depending on direction of traffic flow
- Traffic to/from ENIs always show primary private IP address.

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version
- account-id
- interface-id
- s
- d
- s
- dstport
- protocol
- packets
- bytes
- start
- end
- action
- log-status

- Unix time when first and last packet of aggregated data was received.

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version
- account-id
- interface-id
- srcaddr
- dstport
- protocol
- packets
- bytes
- start
- end
- action
- log-status

- Traffic flow `ACCEPT`-ed or `REJECT`-ed by SGs and/or NACLs.

# Log Record Fields



- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

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

- OK
- NODATA
- SKIPDATA

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
    - IPv4, IPv6, or EFA
  - pkt-srcaddr
  - pkt-dstaddr

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr

- *Original* IP address of traffic source or destination

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id

# Log Record Fields



- Version 3
  - vpc-id
  - s
  - ir
  - t
  - type
  - pkt-srcaddr
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id

- AWS sublocation type that traffic comes from
  - `localzone`
  - `outpost`
  - `wavelength`
  - `-`

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id
- Version 5
  - pkt-src-aws-service
  - pkt-dst-aws-service
  - flow-direction
  - traffic-path

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-src
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id
- Version 5
  - pkt-src-aws-service
  - pkt-dst-aws-service
  - flow-direction
  - traffic-path

- Name of traffic source/destination AWS service

# Log Record Fields



- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srca
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id
- Version 5
  - pkt-src-aws-service
  - pkt-dst-aws-service
  - flow-direction
  - traffic-path

- Whether traffic is `ingress` or `egress`

# Log Record Fields

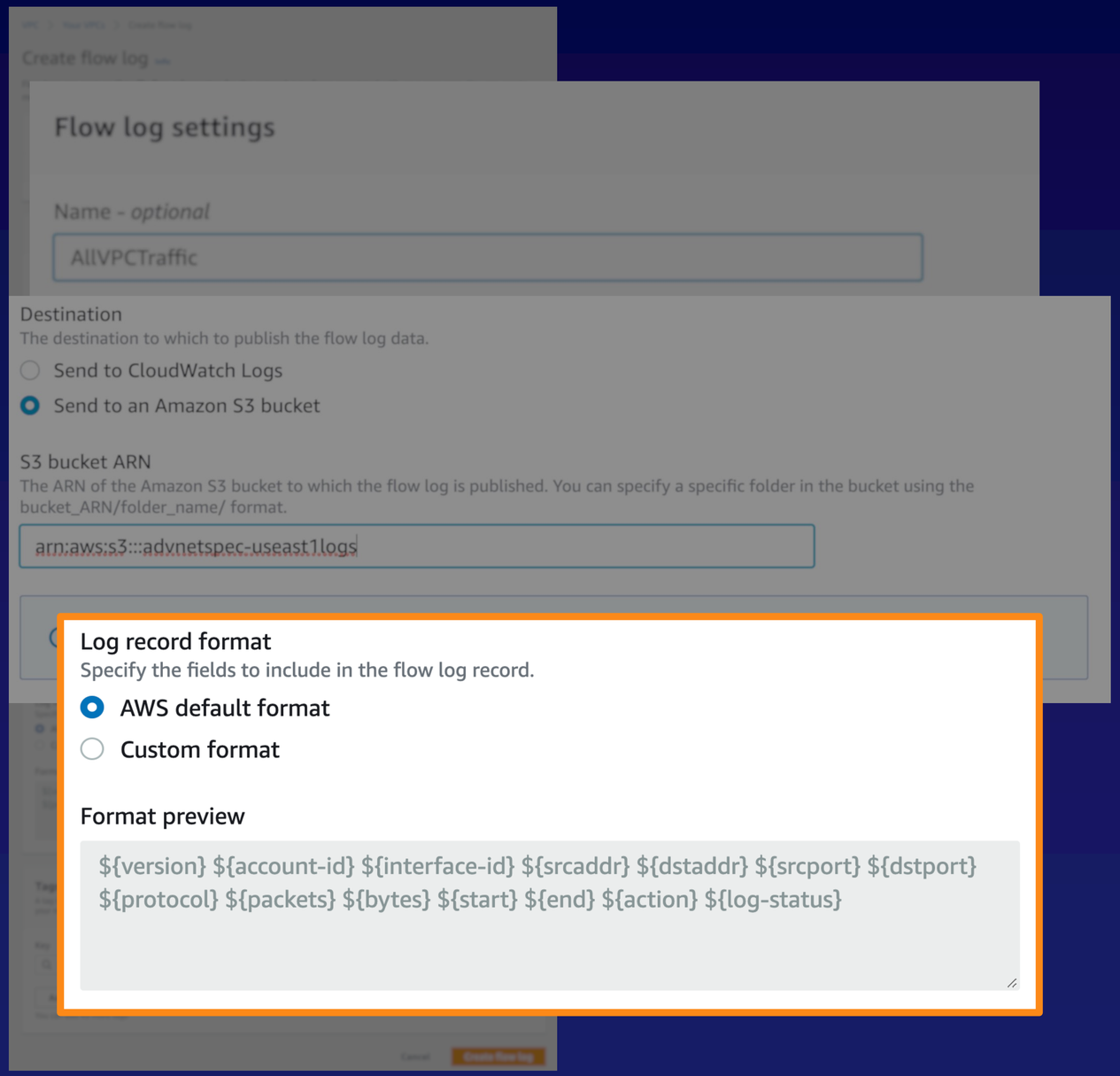


- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - p
  - p
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id
- Version 5
  - pkt-src-aws-service
  - pkt-dst-aws-service
  - flow-direction
  - traffic-path

- AWS object-type egress traffic is sent to

# Creating Flow Logs

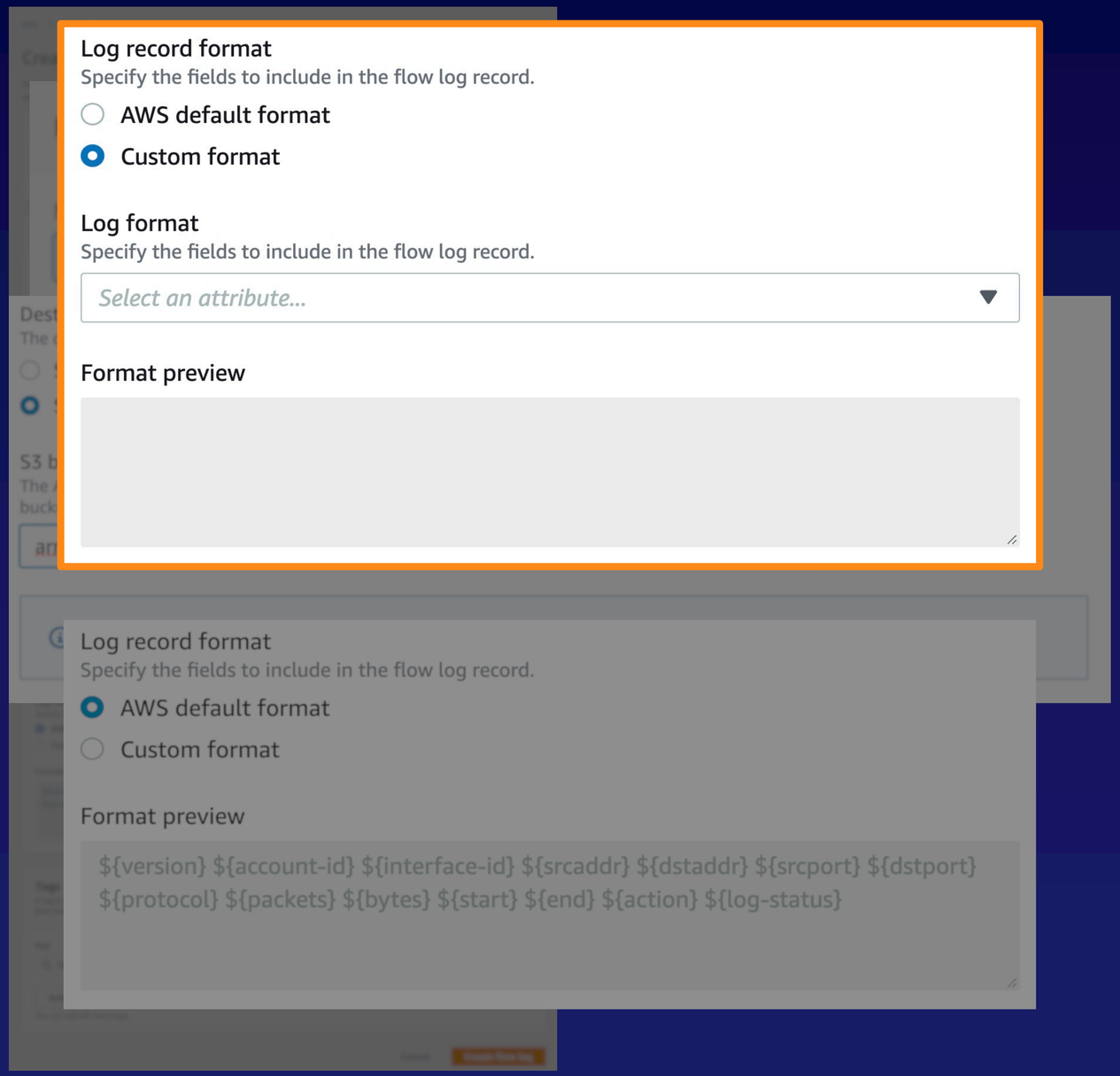





- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

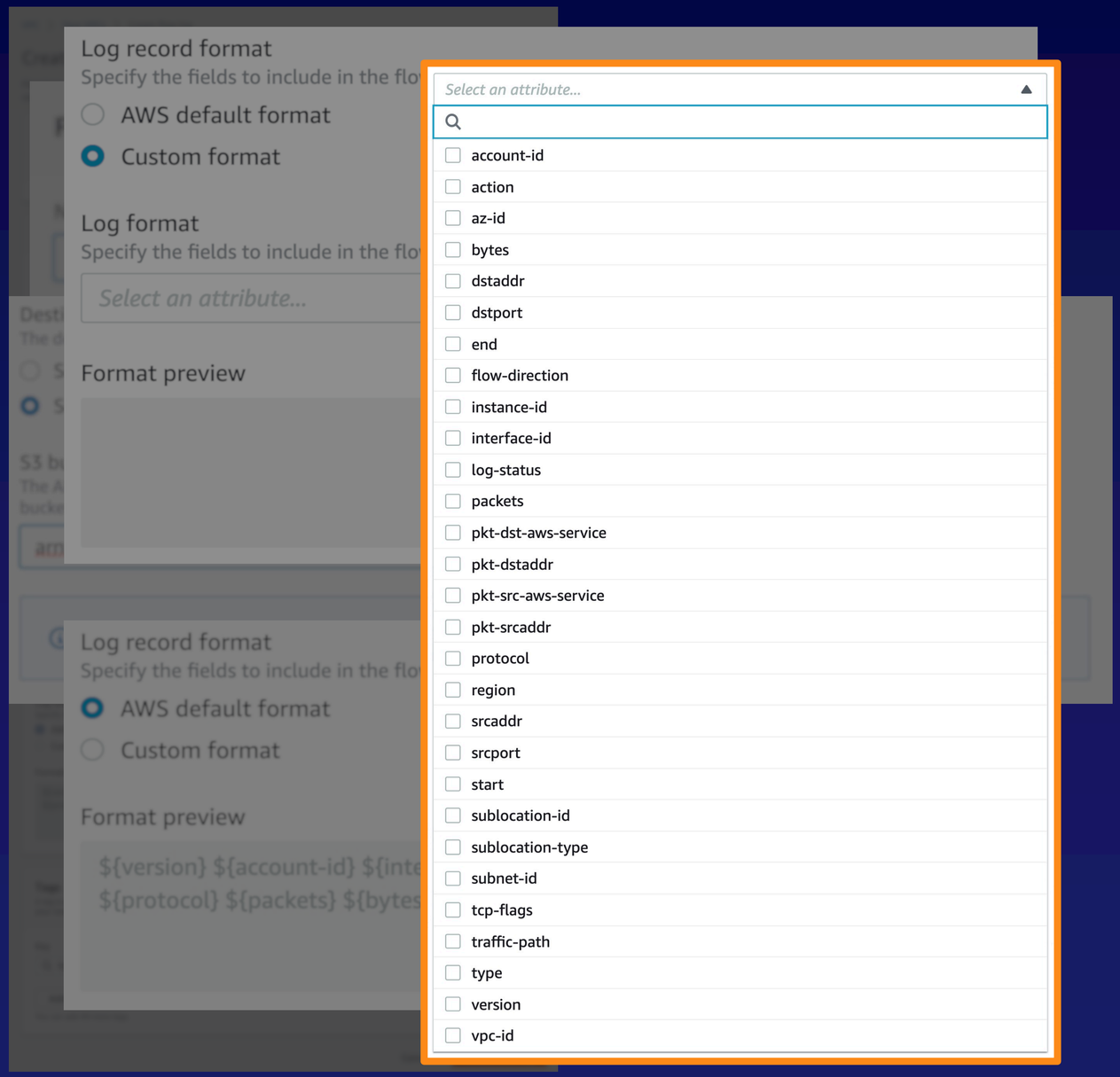





- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

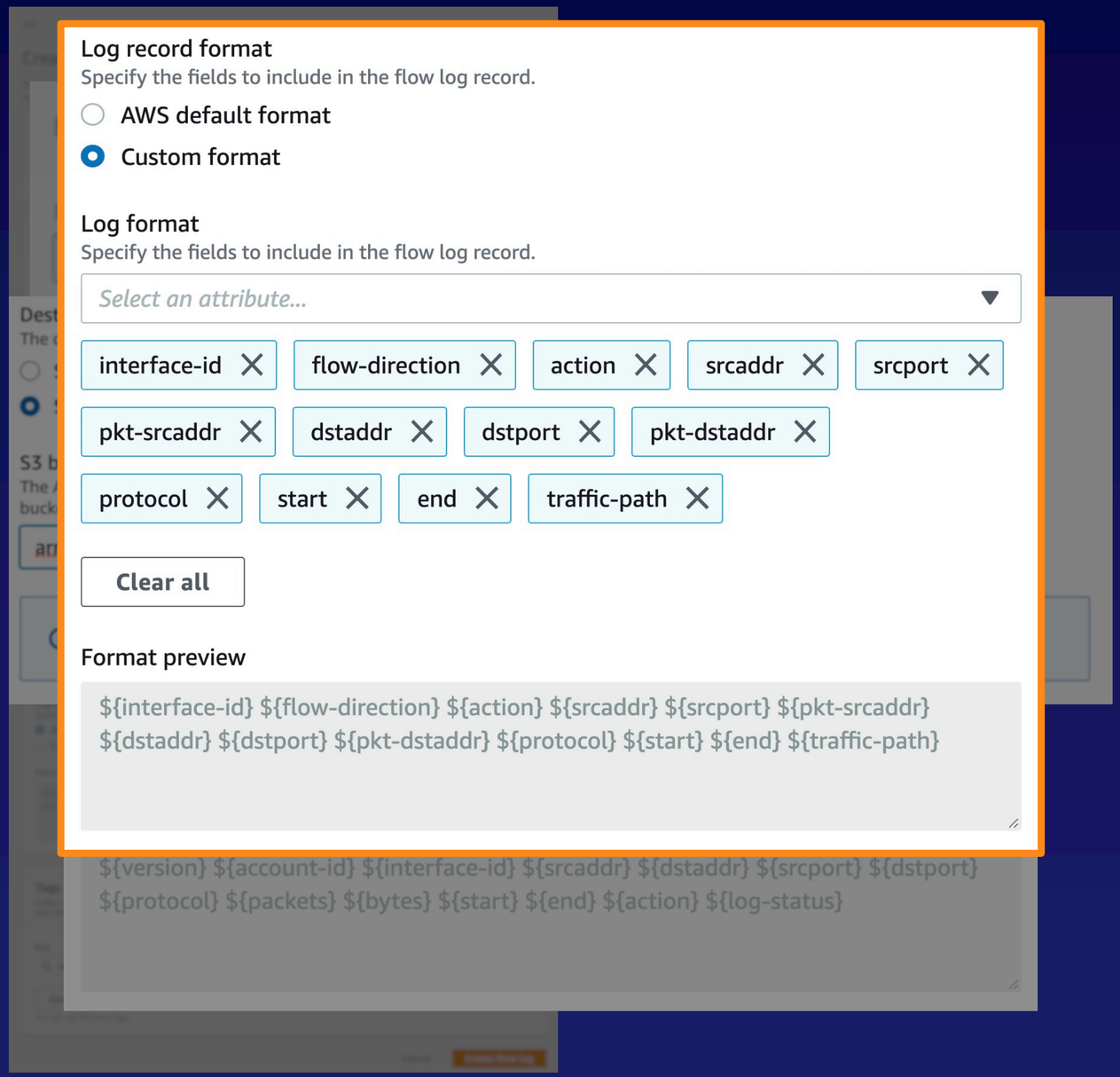





- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

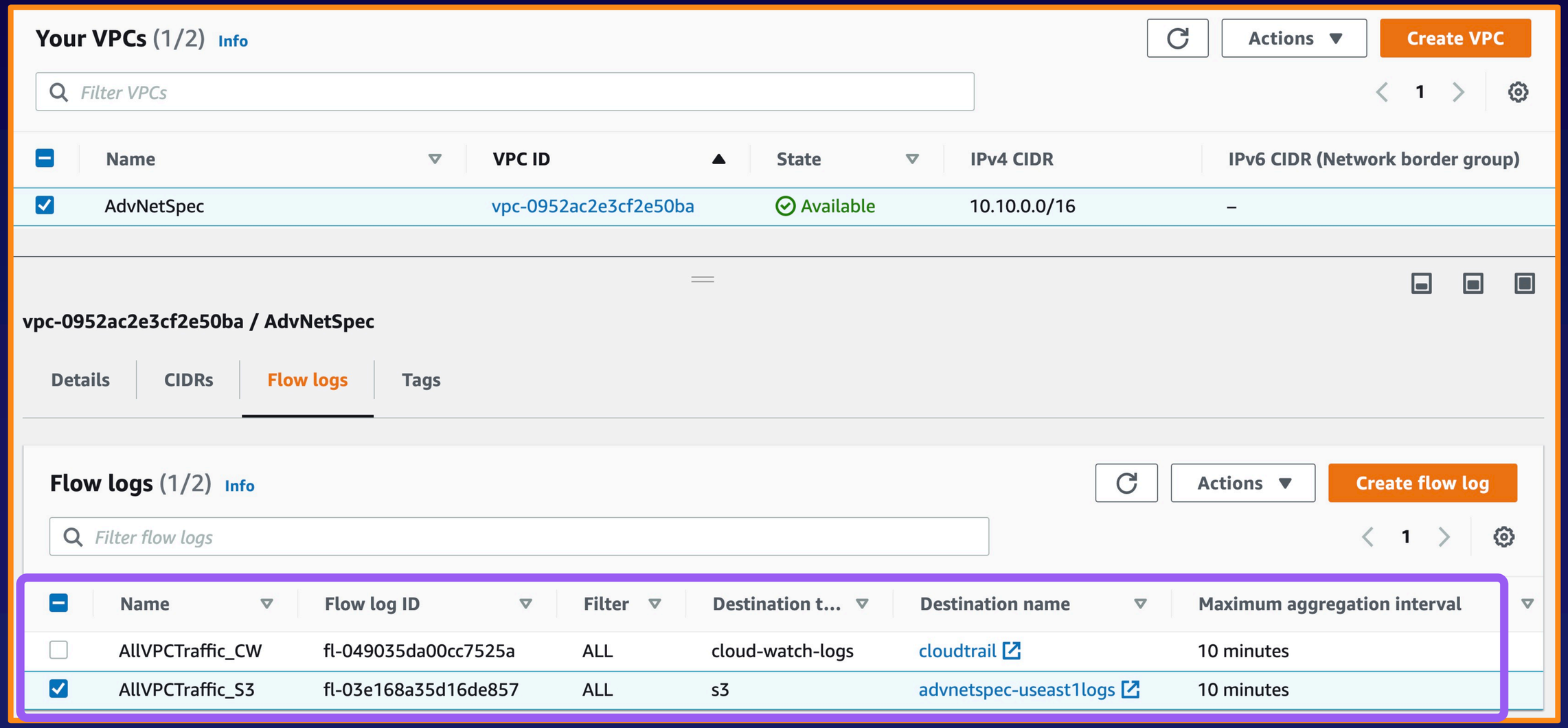





- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

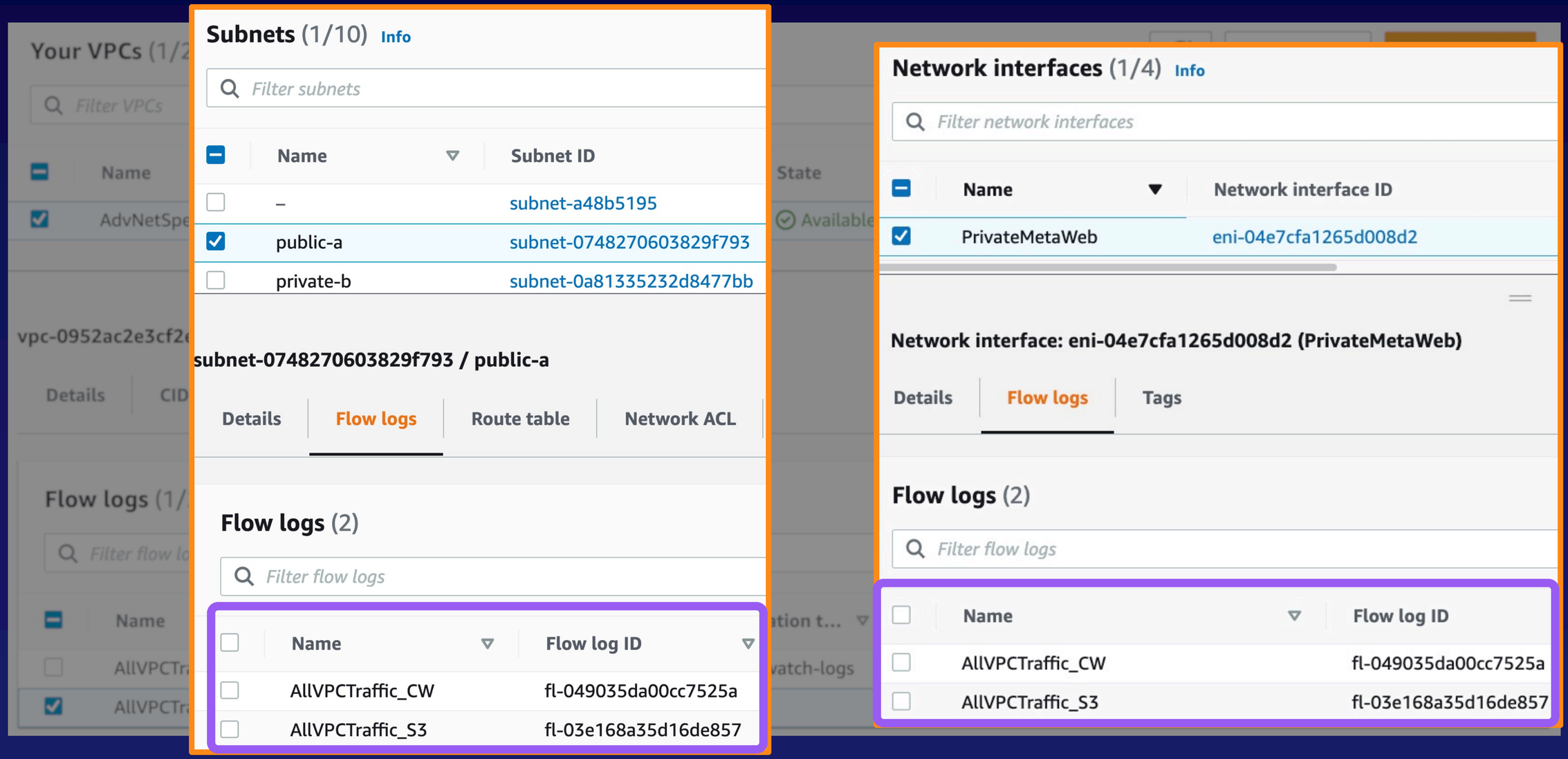
# Creating Flow Logs





# Creating Flow Logs

A CLOUD GURU



# Fast Takeaways



VPC flow logs capture information about IP traffic sessions processed by ENIs in your VPCs.

Log records may be sent to CloudWatch logs or stored in S3 buckets.

Customize fields recorded in logs using AWS-provided fields.

Do not record application-level data.

Log data is not published in real-time.