# Day 14

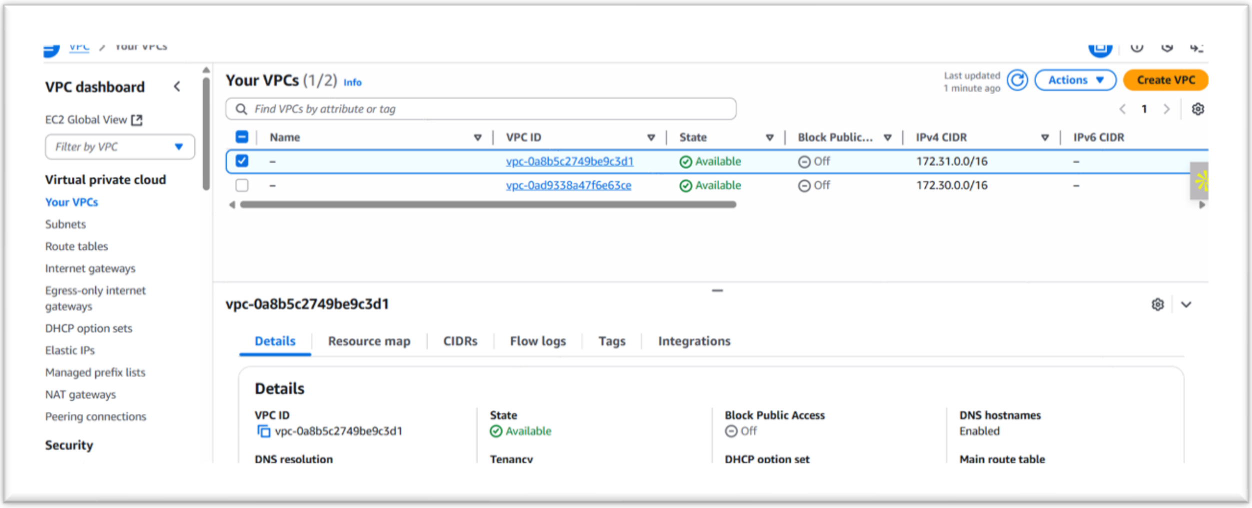
# “CLOUD SECURITY”

## Importance of enabling VPC Flow Logs:

1. **Traffic Monitoring & Troubleshooting:** VPC Flow Logs capture detailed info about IP traffic within and across subnets, helping identify connectivity issues, unauthorized access attempts, and security misconfigurations.
2. **Enhanced Security Visibility:** Logs show traffic allowed/denied by NACLs and Security Groups, including source/destination IPs, ports, protocols, and actions—crucial for forensic analysis and threat detection.
3. **Automation & Alerting:** Logs stored in CloudWatch can trigger alarms and generate metrics, allowing admins to automate responses to suspicious traffic patterns or policy violations.

## Where to find this Flow logs?

You will get it under “Your VPC” section in the “VPC” console.



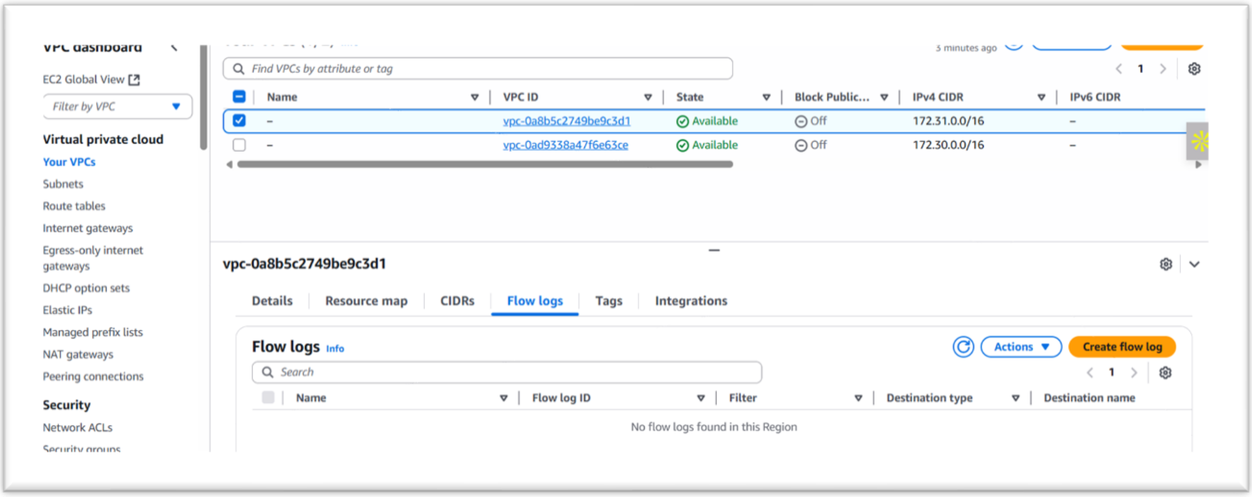
Your VPCs (1/2) Info

| | Name | VPC ID | State | Block Public... | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|---|---|
| ☑ | – | vpc-0a8b5c2749be9c3d1 | Available | Off | 172.31.0.0/16 | – |
| □ | – | vpc-0ad9338a47f6e63ce | Available | Off | 172.30.0.0/16 | – |

vpc-0a8b5c2749be9c3d1

Details

VPC ID: vpc-0a8b5c2749be9c3d1
State: Available
Block Public Access: Off
DNS hostnames: Enabled
DNS resolution
Tenancy
DHCP option set
Main route table



| | Name | VPC ID | State | Block Public... | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|---|---|
| ☑ | – | vpc-0a8b5c2749be9c3d1 | Available | Off | 172.31.0.0/16 | – |
| □ | – | vpc-0ad9338a47f6e63ce | Available | Off | 172.30.0.0/16 | – |

vpc-0a8b5c2749be9c3d1

Flow logs Info

| | Name | Flow log ID | Filter | Destination type | Destination name |
|---|---|---|---|---|---|

No flow logs found in this Region

## Basic information:

### What are Flow Logs?

Flow logs are records of IP traffic flowing to and from network interfaces within a VPC, capturing details like source/destination IPs, ports, protocol, and action (accept/reject).

### Why we need Flow Logs?

They help monitor, analyze, and troubleshoot network traffic, ensure security policies (NACLs/SGs) are functioning correctly, and detect unusual or unauthorized behavior.

### How Flow Logs help?

Flow logs provide visibility into network communications, assist in forensic investigations, support compliance auditing, and enable real-time alerts for suspicious traffic patterns.

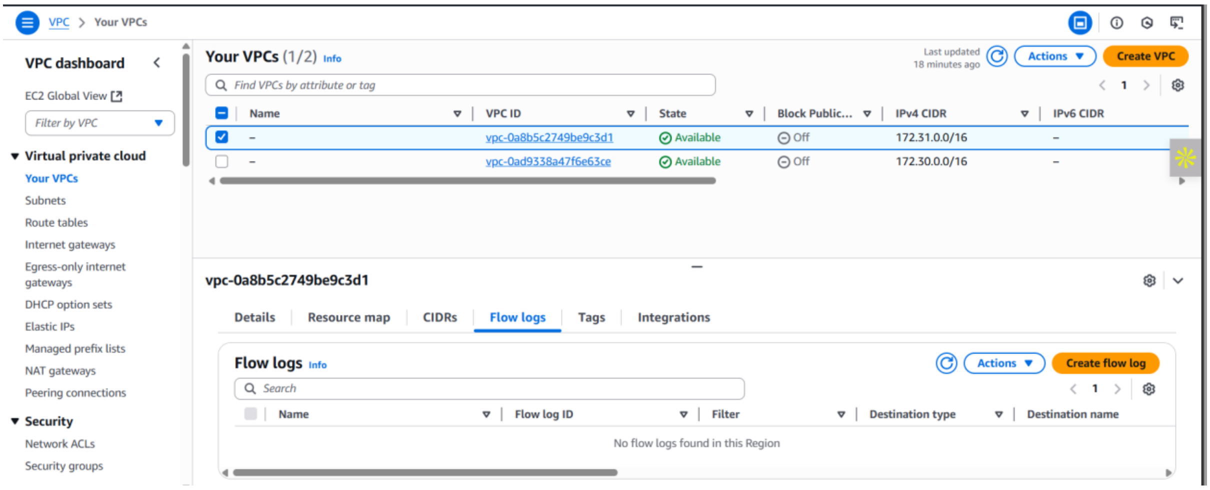
### What if Flow Logs are absent?

Without flow logs, administrators lose visibility into VPC traffic, making it harder to detect misconfigurations, identify attacks, troubleshoot connectivity issues, or prove compliance.

## Enable VPC Flow logs to monitor network traffic:

Steps:

Select the VPC whose Flow logs you want to generate: then click on the "create flow log" button.



Your VPCs (1/2) Info

| | Name | VPC ID | State | Block Public... | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|---|---|
| ☑ | – | vpc-0a8b5c2749be9c3d1 | Available | Off | 172.31.0.0/16 | – |
| □ | – | vpc-0ad9338a47f6e63ce | Available | Off | 172.30.0.0/16 | – |

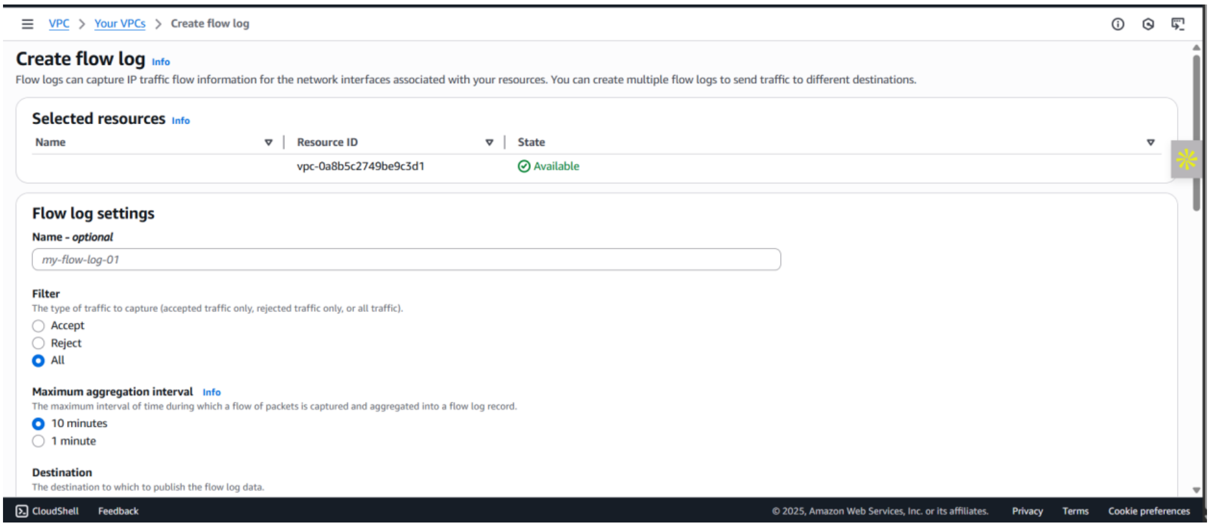
vpc-0a8b5c2749be9c3d1

Flow logs Info

| □ | Name | Flow log ID | Filter | Destination type | Destination name |
|---|---|---|---|---|---|

No flow logs found in this Region

Following screen will appear: fill the data and click on the orange button at the bottom of screen.



VPC > Your VPCs > Create flow log

**Create flow log** Info

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

**Selected resources** Info

| Name | Resource ID | State |
|---|---|---|
|  | vpc-0a8b5c2749be9c3d1 | Available |

**Flow log settings**

Name - *optional*

*my-flow-log-01*

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

○ Accept
○ Reject
● All

Maximum aggregation interval Info

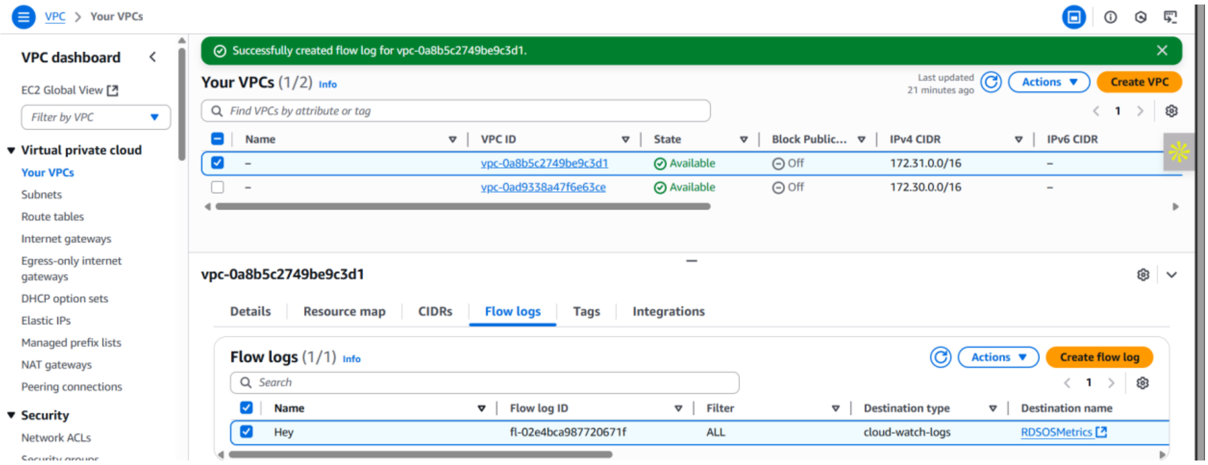
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

● 10 minutes
○ 1 minute

Destination

The destination to which to publish the flow log data.

You will see that the flow logs are created:



VPC > Your VPCs

Successfully created flow log for vpc-0a8b5c2749be9c3d1.

**Your VPCs** (1/2) Info

Last updated 21 minutes ago

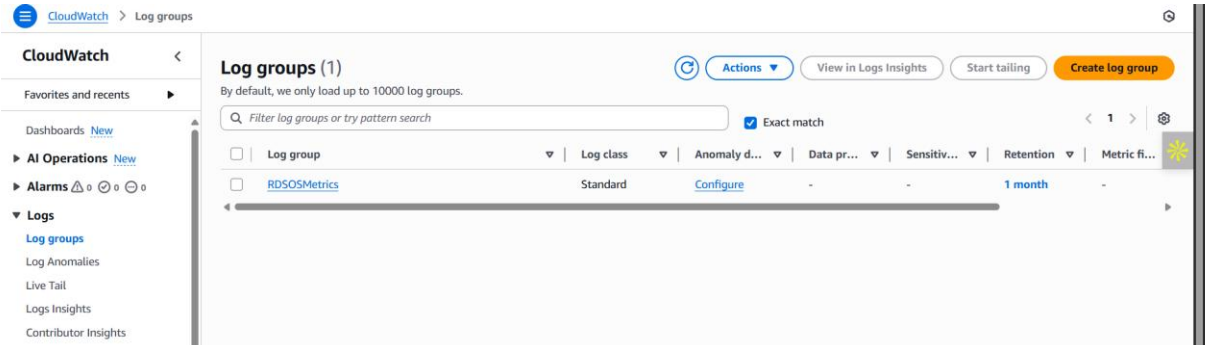
| ☐ | Name | VPC ID | State | Block Public... | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|---|---|
| ☑ | – | vpc-0a8b5c2749be9c3d1 | Available | Off | 172.31.0.0/16 | – |
| ☐ | – | vpc-0ad9338a47f6e63ce | Available | Off | 172.30.0.0/16 | – |

vpc-0a8b5c2749be9c3d1

**Flow logs** (1/1) Info

| ☑ | Name | Flow log ID | Filter | Destination type | Destination name |
|---|---|---|---|---|---|
| ☑ | Hey | fl-02e4bca987720671f | ALL | cloud-watch-logs | RDSOSMetrics |

To cross verify, visit the "Cloud Watch" services: clearly it can be seen there working fine.



CloudWatch > Log groups

**Log groups** (1)

By default, we only load up to 10000 log groups.

| ☐ | Log group | Log class | Anomaly d... | Data pr... | Sensitiv... | Retention | Metric fi... |
|---|---|---|---|---|---|---|---|
| ☐ | RDSOSMetrics | Standard | Configure | - | - | 1 month | - |

## Best practices to create and manage effective and secure VPC Flow Logs:

- **Enable Flow Logs selectively**: Capture logs at appropriate levels — VPC, subnet, or ENI — based on need and sensitivity. Avoid unnecessary logging to reduce noise and cost.
- **Use centralized logging with Amazon CloudWatch Logs or S3**: Store logs securely and centrally to streamline analysis, auditing, and long-term retention.

- **Apply encryption**: Enable encryption for CloudWatch log groups and S3 buckets to protect log data in transit and at rest.
- **Restrict access with IAM policies**: Limit access to flow logs using fine-grained IAM roles and permissions, allowing only trusted users to view or manage logs.
- **Set up alerts and metrics**: Use CloudWatch Alarms and filters to detect abnormal patterns, such as traffic spikes, denied connections, or suspicious IPs.
- **Automate log analysis**: Use AWS services like Athena or third-party tools to analyze flow logs for insights, compliance checks, and anomaly detection.
- **Rotate and archive logs**: Implement log rotation and lifecycle policies to manage storage costs and retain only necessary data for compliance or auditing.
- **Tag your resources**: Tag flow logs with metadata (e.g., environment, application) to easily filter and organize logs across multiple accounts or regions.
- **Integrate with SIEM tools**: Forward flow logs to your Security Information and Event Management (SIEM) platform for enhanced threat detection and response.

--The End--