**Day 14**





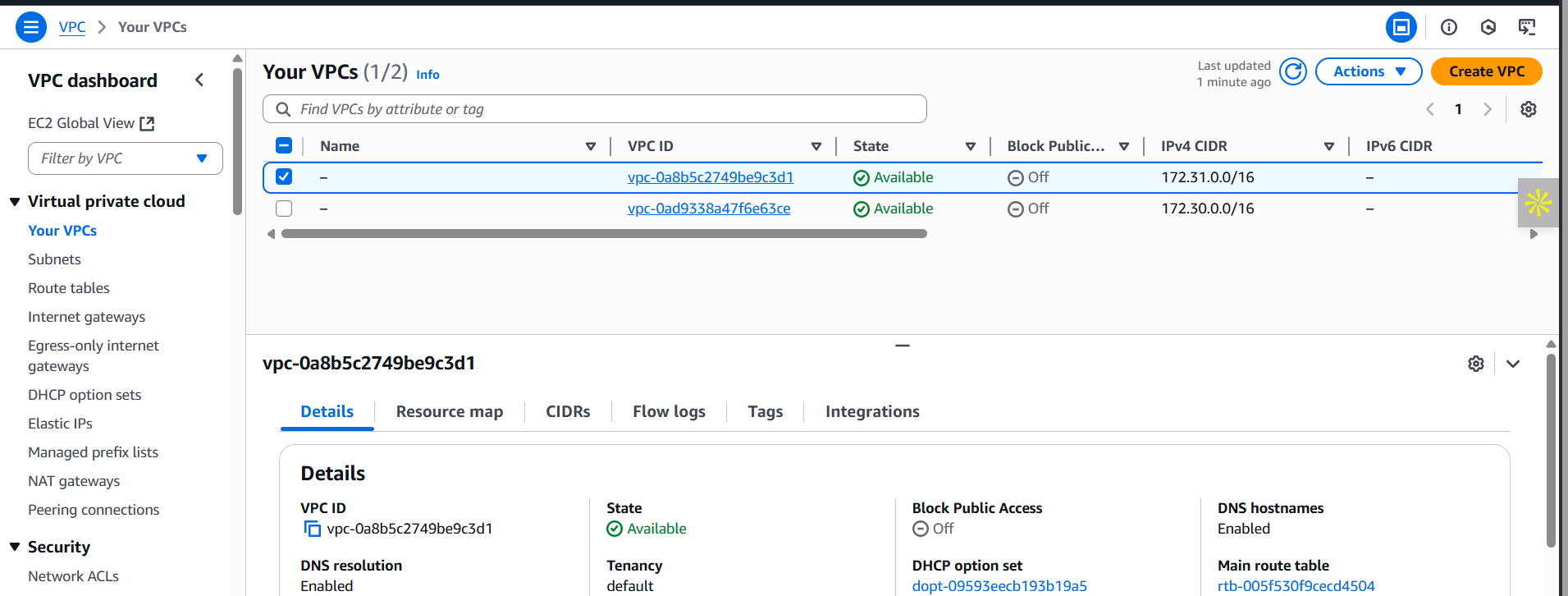
**“CLOUD SECURITY”**

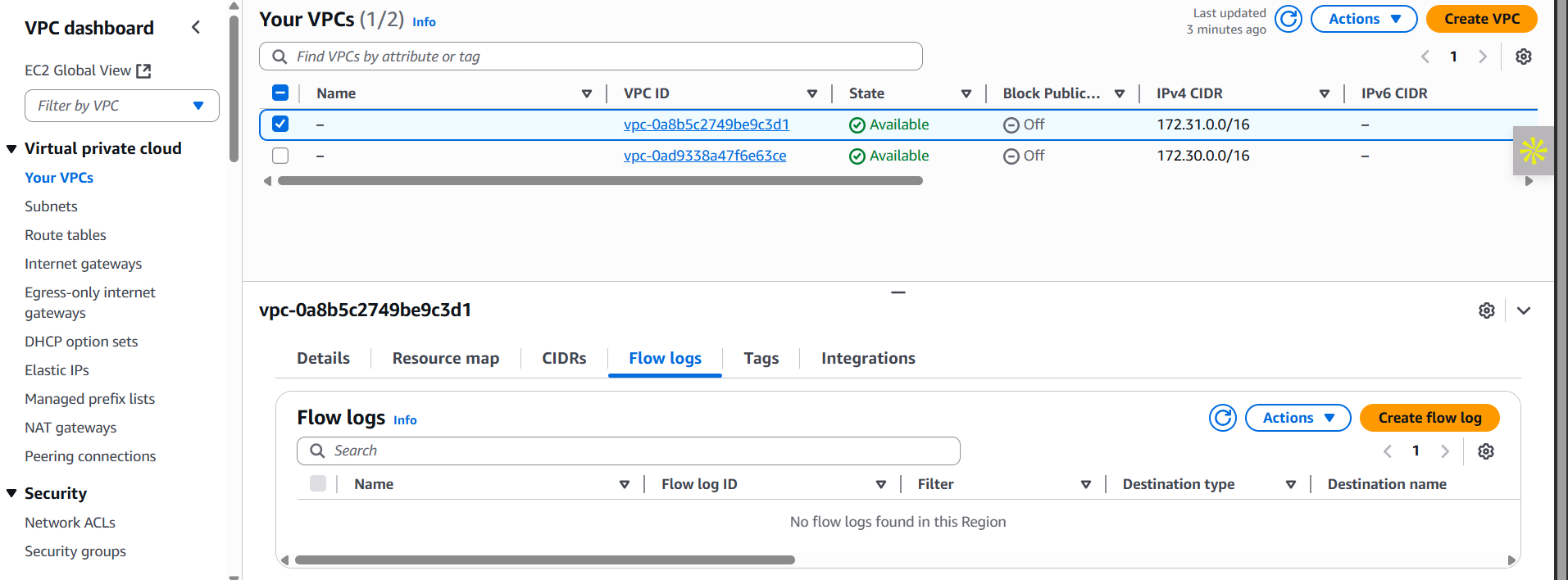
**Importance of enabling VPC Flow Logs:**

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.





**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.

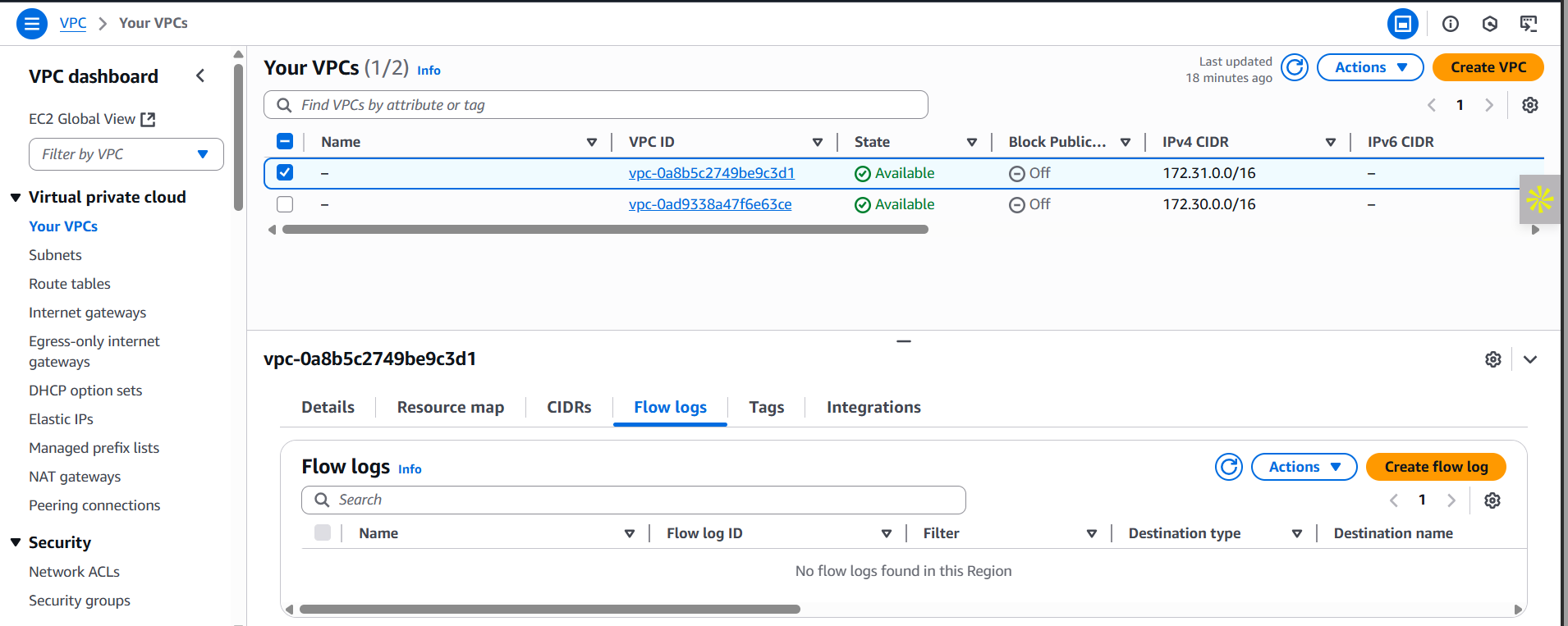
**How Flow Logs help?**  
Flow logs provide visibility into network communications, assist in forensic investigations, support compliance auditing, and enable real-time alerts for suspicious traffic patterns.

**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.

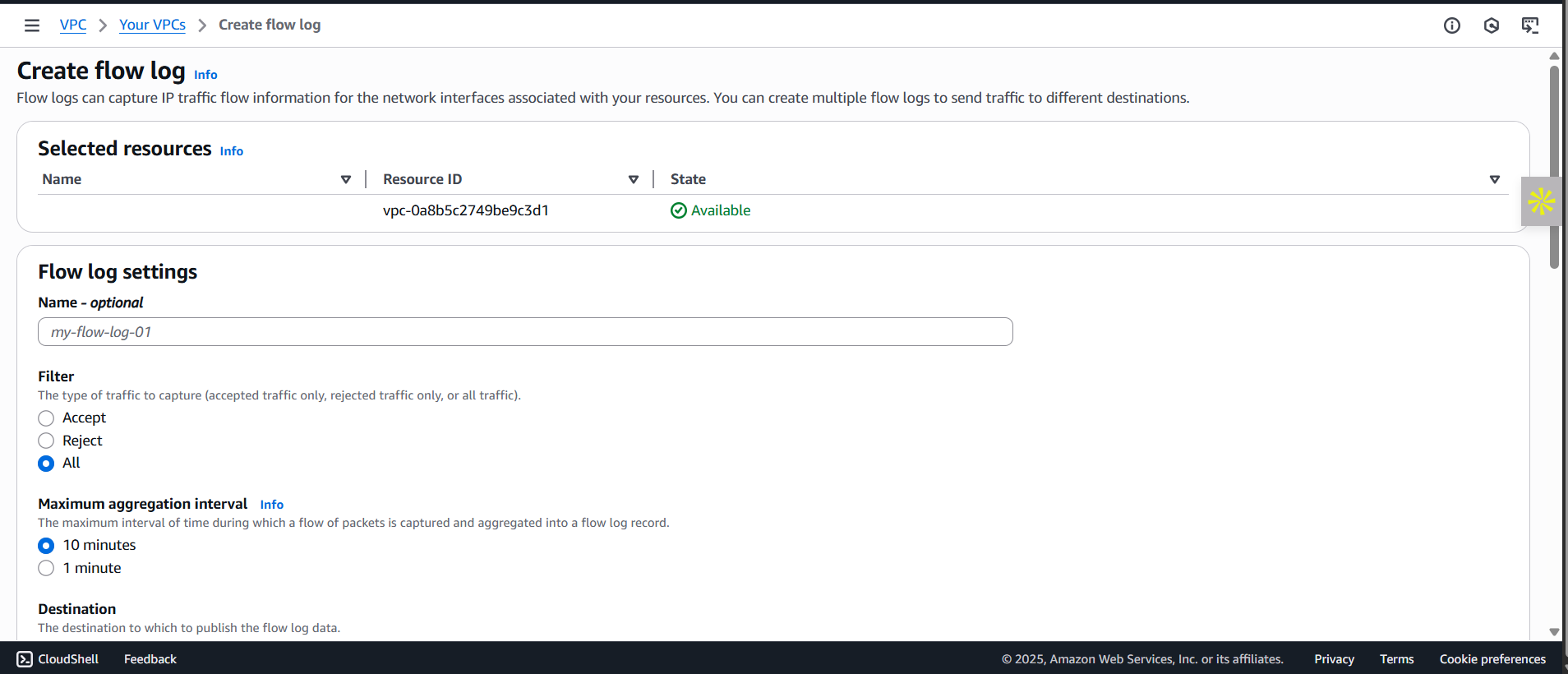
**Enable VPC Flow logs to monitor network traffic:**

Steps:

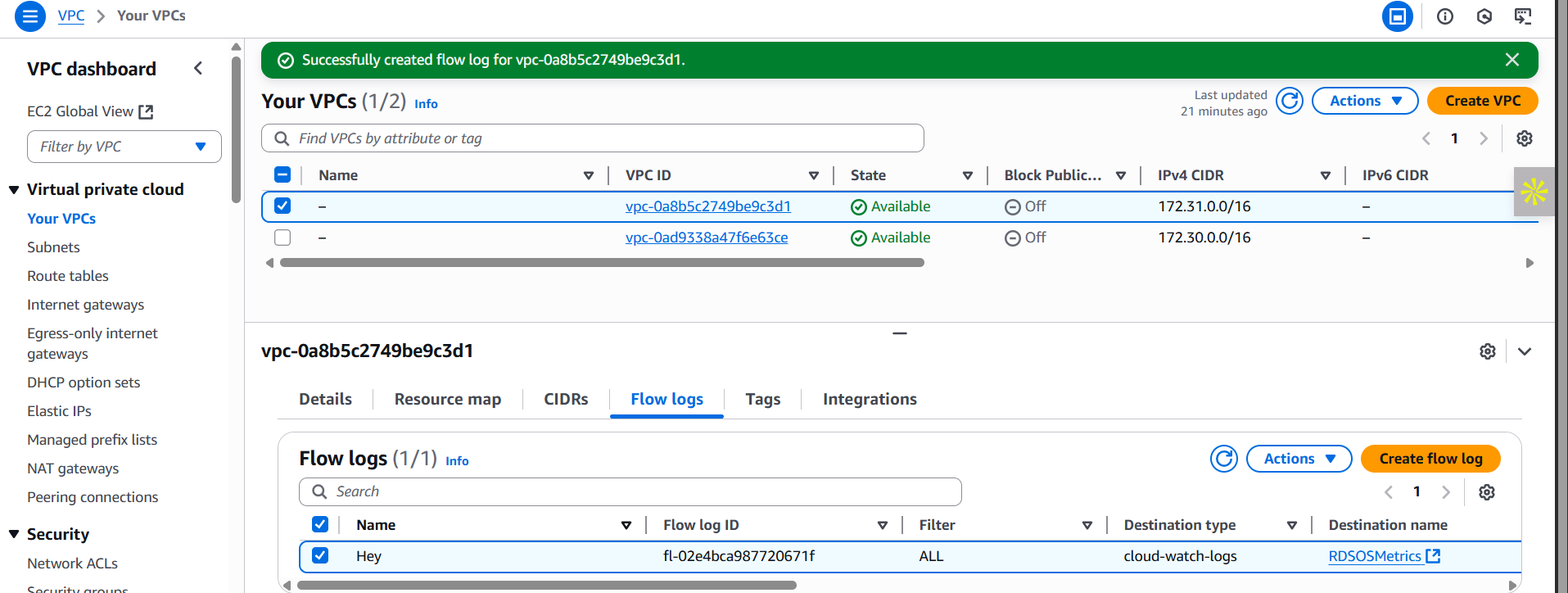
Select the VPC whose Flow logs you want to generate: then click on the “create flow log” button.

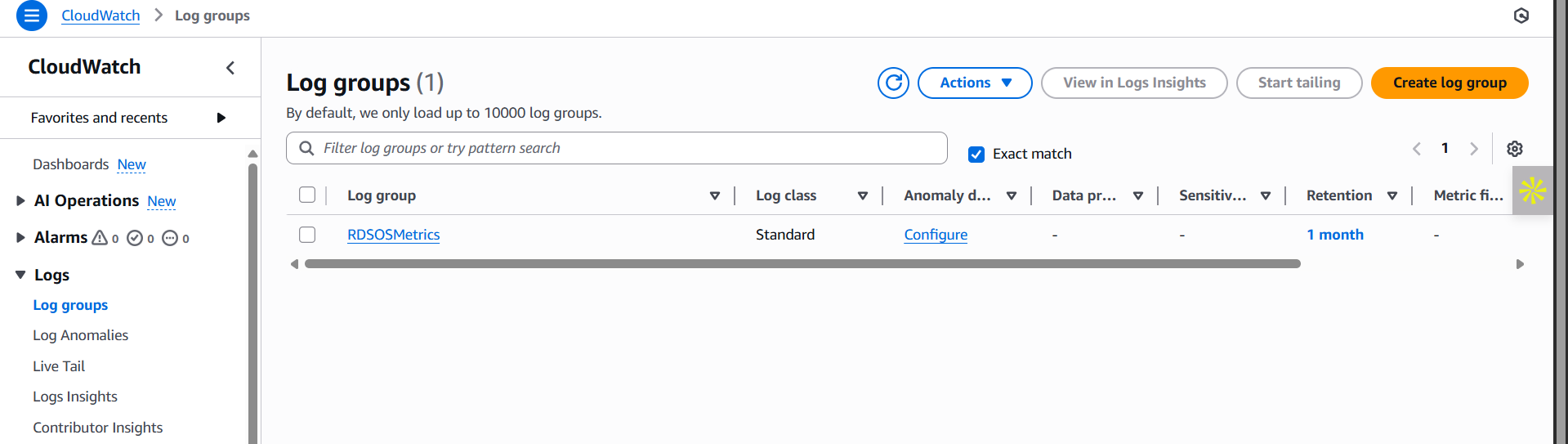


Following screen will appear: fill the data and click on the orange button at the bottom of screen.



You will see that the flow logs are created:



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

**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--