Enterprise Centralized Logging and Observability Architecture on AWS

Author: Adedayo
Specialization: Cloud Security & Observability
Platform: Amazon Web Services (AWS)

1. Introduction

This document describes the design and implementation of a centralized logging and observability framework in AWS to improve visibility, security monitoring, and compliance across multi-account and multi-region environments.

I implemented this solution to ensure that critical logs from distributed workloads are consistently collected, securely stored, retained according to compliance requirements, and analyzed through a centralized SIEM platform.

2. Objectives

The primary objectives of this implementation were to:

- Centralize AWS service and application logs
- Improve security monitoring and incident investigation
- Support regulatory and compliance requirements
- Enable real-time detection and alerting
- Ensure secure and durable log storage
- Reduce operational blind spots

3. Logging Architecture Overview

The centralized logging platform was built using:

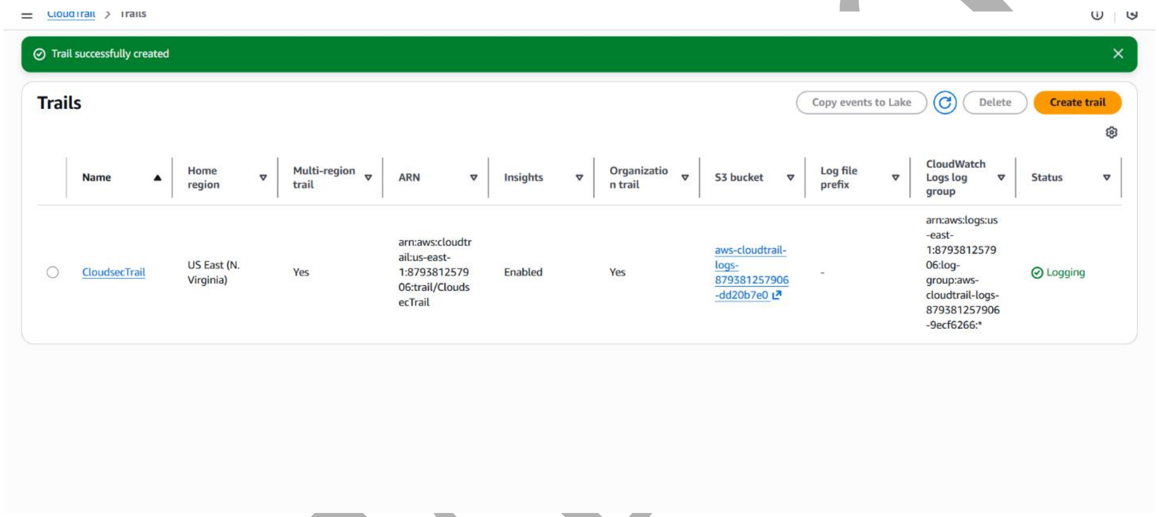
- AWS CloudTrail
- Amazon CloudWatch Logs
- Amazon Kinesis Data Firehose
- AWS Lambda
- Amazon OpenSearch

- Amazon S3

All service and application logs are routed through CloudWatch and streamed into a secure analytics platform.

4. CloudTrail Configuration

CloudTrail was configured as a multi-region, organization-level trail.



Trails

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	CloudsecTrail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:879381257906:trail/CloudsecTrail	Enabled	Yes	aws-cloudtrail-logs-879381257906-dd20b7e0	-	arn:aws:logs:us-east-1:879381257906:log-group:aws-cloudtrail-logs-879381257906-9ecf6266:*	✓ Logging

The configuration includes:

- Management event logging
- CloudTrail Insights for anomaly detection
- Centralized S3 storage
- Streaming to CloudWatch Logs

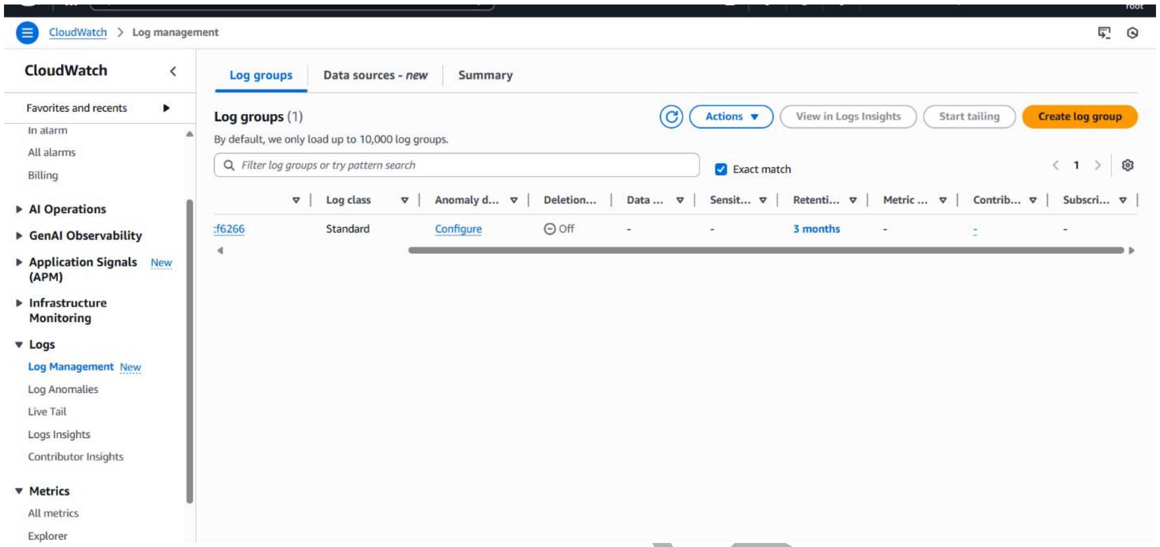
This ensured full visibility into account activity across regions.

5. Log Retention and Lifecycle Management

CloudWatch Log Groups were configured with defined retention periods to prevent indefinite storage.

CloudTrail logs stored in S3 are managed using lifecycle policies that:

- Retain logs in S3 Standard for 90 days



CloudWatch > Log management

CloudWatch

Favorites and recents
In alarm
All alarms
Billing
AI Operations
GenAI Observability
Application Signals (APM) New
Infrastructure Monitoring
Logs
Log Management New
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
All metrics
Explorer

Log groups | Data sources - *new* | Summary

Log groups (1)
By default, we only load up to 10,000 log groups.

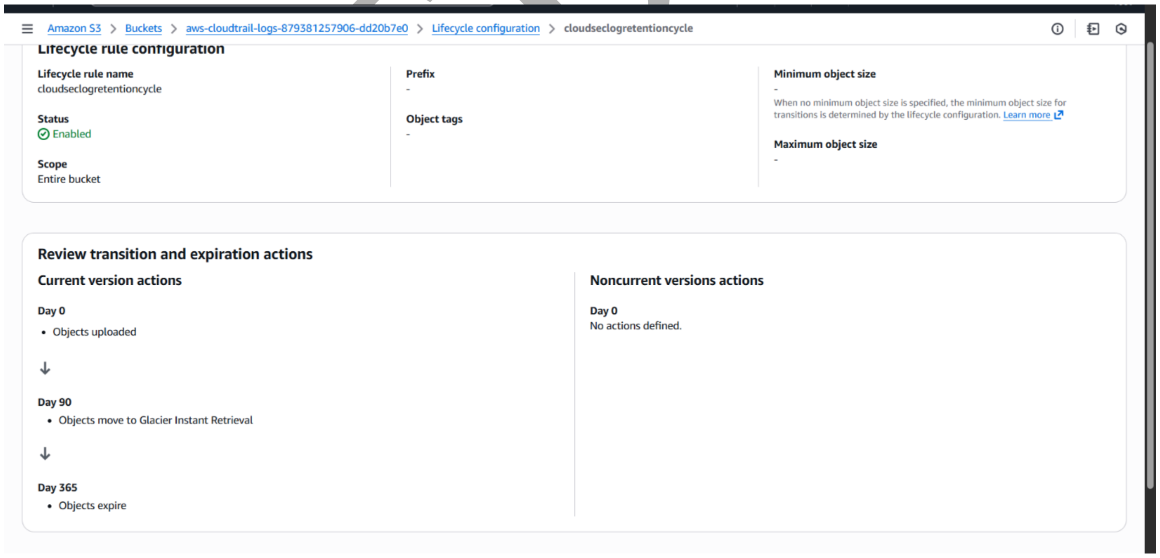
Actions | View in Logs Insights | Start tailing | Create log group

Filter log groups or try pattern search
☑ Exact match

	Log class	Anomaly d...	Deletion...	Data ...	Sensit...	Retenti...	Metric ...	Contrib...	Subscri...
:f6266	Standard	Configure	Off	-	-	3 months	-	-	-

- Archive older logs to S3 Glacier

- Delete logs after one year



Amazon S3 > Buckets > aws-cloudtrail-logs-879381257906-dd20b7e0 > Lifecycle configuration > cloudseclogretentioncycle

Lifecycle rule configuration

Lifecycle rule name cloudseclogretentioncycle	**Prefix** -	**Minimum object size** - When no minimum object size is specified, the minimum object size for transitions is determined by the lifecycle configuration. Learn more
Status ✓ Enabled	**Object tags** -	**Maximum object size** -
Scope Entire bucket		

Review transition and expiration actions

Current version actions

Day 0
- Objects uploaded

↓

Day 90
- Objects move to Glacier Instant Retrieval

↓

Day 365
- Objects expire

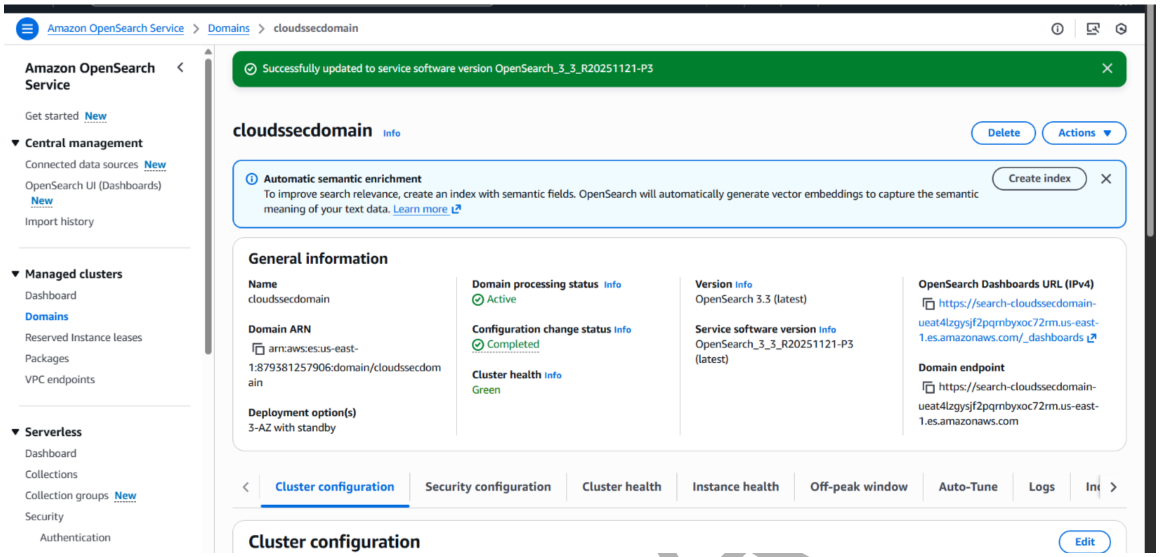
Noncurrent versions actions

Day 0
No actions defined.

This approach aligns with common compliance standards such as PCI-DSS while controlling storage costs.

6. Centralized SIEM Platform (Amazon OpenSearch)

Amazon OpenSearch was deployed as the centralized log analytics and SIEM platform.



Successfully updated to service software version OpenSearch_3_3_R20251121-P3

cloudssecdomain Info

Automatic semantic enrichment
To improve search relevance, create an index with semantic fields. OpenSearch will automatically generate vector embeddings to capture the semantic meaning of your text data. Learn more

General information

Name
cloudssecdomain

Domain ARN
arn:aws:es:us-east-1:879381257906:domain/cloudssecdomain

Deployment option(s)
3-AZ with standby

Domain processing status Info
Active

Configuration change status Info
Completed

Cluster health Info
Green

Version Info
OpenSearch 3.3 (latest)

Service software version Info
OpenSearch_3_3_R20251121-P3 (latest)

OpenSearch Dashboards URL (IPv4)
https://search-cloudssecdomain-ueat4lzgysjf2pqrnbyxoc72rm.us-east-1.es.amazonaws.com/_dashboards

Domain endpoint
https://search-cloudssecdomain-ueat4lzgysjf2pqrnbyxoc72rm.us-east-1.es.amazonaws.com

Cluster configuration

The domain was configured with:

- No public internet exposure
- VPC-based deployment
- Fine-grained access control
- IAM-based authentication
- Encrypted storage
- Node-to-node encryption

Access was restricted using security groups to authorized ingestion services.

7. Secure Log Ingestion Pipeline

7.1 CloudWatch Subscription Filters

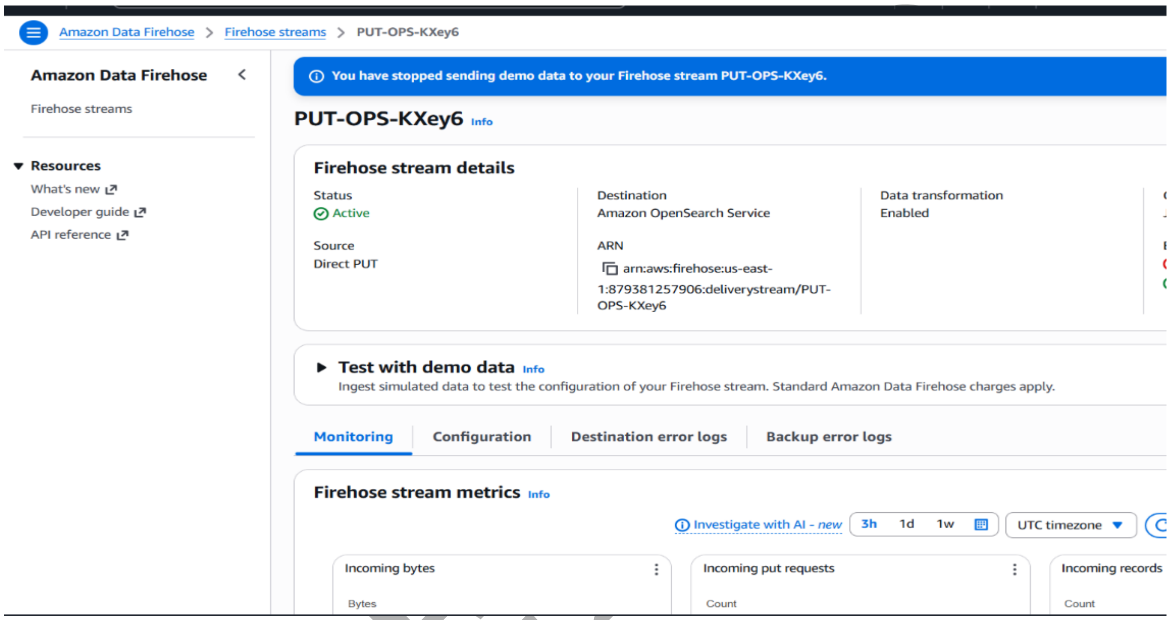
Subscription filters were created to forward all CloudTrail events to Kinesis Data Firehose.

No filtering was applied to ensure complete audit coverage.

7.2 Kinesis Data Firehose Configuration

Firehose was configured with:

- OpenSearch as primary destination
- S3 backup destination
- VPC delivery enabled



Amazon Data Firehose > Firehose streams > PUT-OPS-KXey6

You have stopped sending demo data to your Firehose stream PUT-OPS-KXey6.

PUT-OPS-KXey6 Info

Firehose stream details

Status: Active
Source: Direct PUT
Destination: Amazon OpenSearch Service
ARN: arn:aws:firehose:us-east-1:879381257906:deliverystream/PUT-OPS-KXey6
Data transformation: Enabled

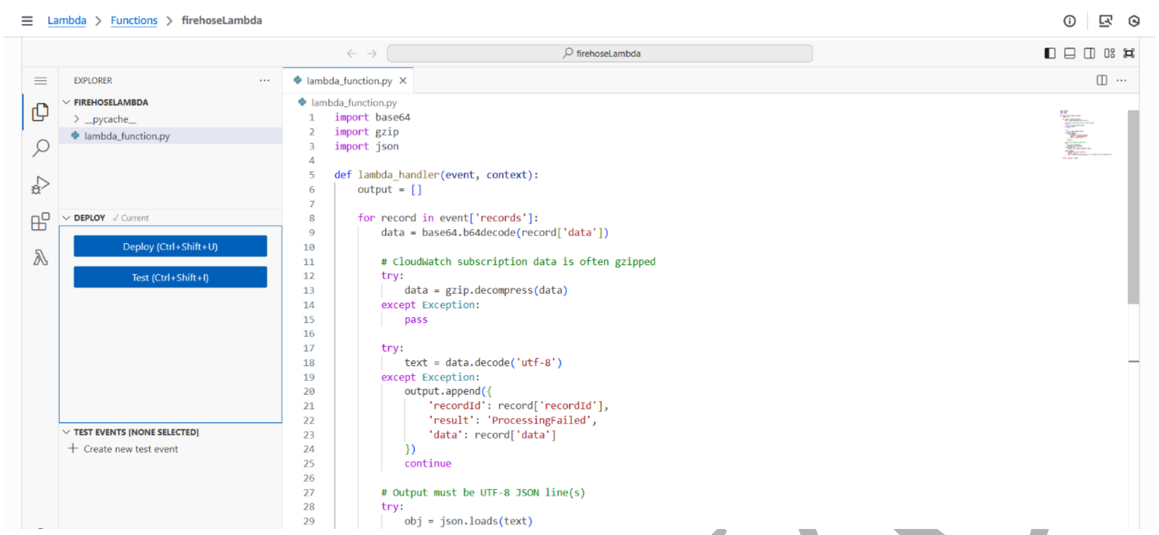
Test with demo data Info
Ingest simulated data to test the configuration of your Firehose stream. Standard Amazon Data Firehose charges apply.

An IAM role was created with permissions for:

- Writing to OpenSearch
- Delivering data to S3
- Managing network interfaces

7.3 Lambda Log Transformation

A Lambda function was integrated into Firehose to perform log transformation.



```python
import base64
import gzip
import json

def lambda_handler(event, context):
    output = []

    for record in event['records']:
        data = base64.b64decode(record['data'])

        # CloudWatch subscription data is often gzipped
        try:
            data = gzip.decompress(data)
        except Exception:
            pass

        try:
            text = data.decode('utf-8')
        except Exception:
            output.append({
                'recordId': record['recordId'],
                'result': 'ProcessingFailed',
                'data': record['data']
            })
            continue

        # Output must be UTF-8 JSON line(s)
        try:
            obj = json.loads(text)
```

Functions included:

- Normalizing log formats
- Adding metadata
- Ensuring indexing compatibility

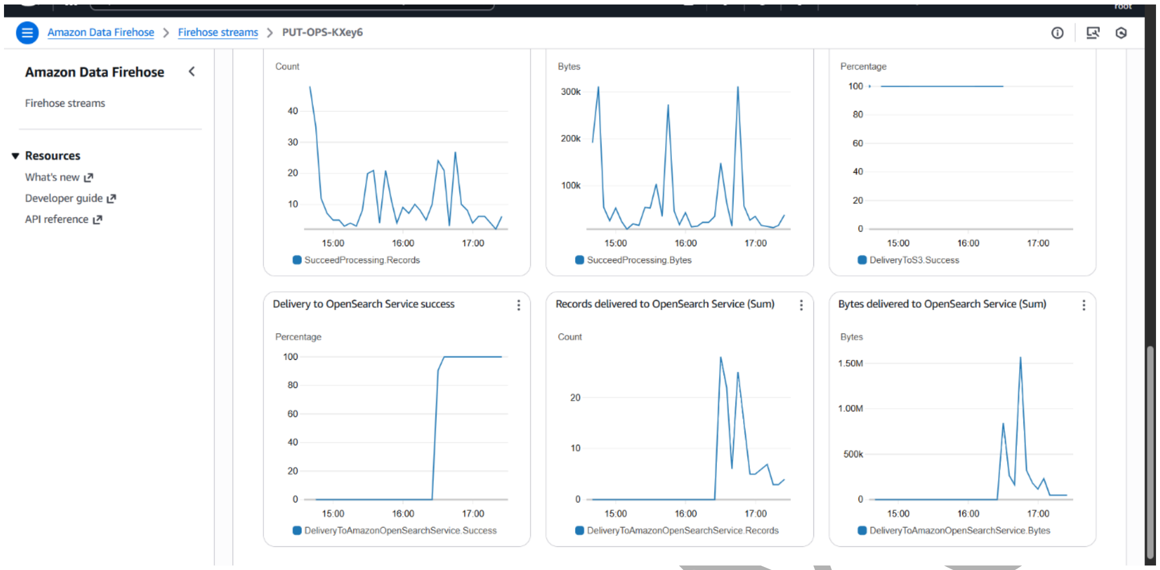
This improved searchability and consistency.

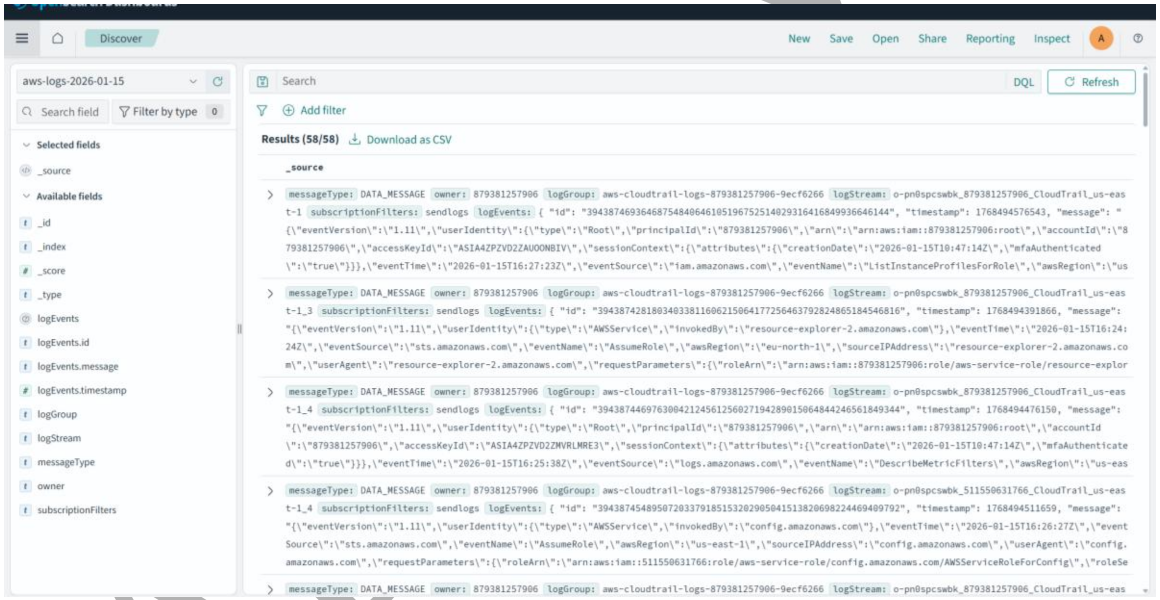
8. Pipeline Validation and Testing

The logging pipeline was validated end-to-end.

After resolving VPC network restrictions, log ingestion was confirmed in OpenSearch.

Indexed records were verified to be searchable and complete.





Results (58/58)

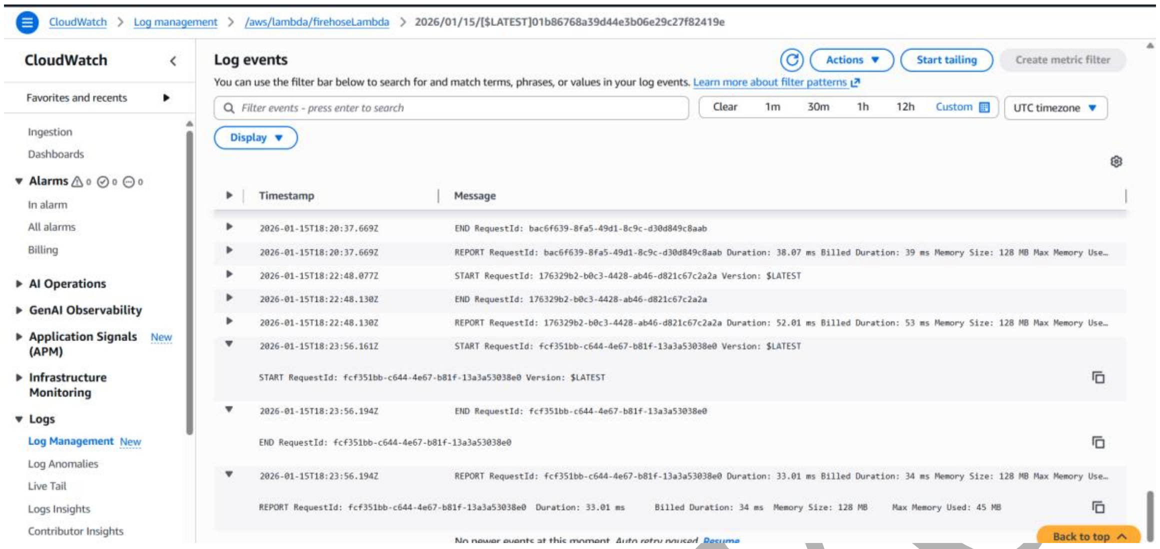
```
_source
messageType: DATA_MESSAGE owner: 879381257906 logGroup: aws-cloudtrail-logs-879381257906-9ecf6266 logStream: o-pn0spcswbk_879381257906_CloudTrail_us-eas
t-1 subscriptionFilters: sendlogs logEvents: { "id": "39438746936468754840646105196752514029316416849936646144", "timestamp": 1768494576543, "message": "
{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"Root\",\"principalId\":\"879381257906\",\"arn\":\"arn:aws:iam::879381257906:root\",\"accountId\":\"8
79381257906\",\"accessKeyId\":\"ASIA4ZPZVD2ZAUOONBIV\",\"sessionContext\":{\"attributes\":{\"creationDate\":\"2026-01-15T10:47:14Z\",\"mfaAuthenticated
\":\"true\"}}},\"eventTime\":\"2026-01-15T16:27:23Z\",\"eventSource\":\"iam.amazonaws.com\",\"eventName\":\"ListInstanceProfilesForRole\",\"awsRegion\":\"us
messageType: DATA_MESSAGE owner: 879381257906 logGroup: aws-cloudtrail-logs-879381257906-9ecf6266 logStream: o-pn0spcswbk_879381257906_CloudTrail_us-eas
t-1_3 subscriptionFilters: sendlogs logEvents: { "id": "39438742818034033811606215064177256463792824865184546816", "timestamp": 1768494391866, "message":
"{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"AWSService\",\"invokedBy\":\"resource-explorer-2.amazonaws.com\"},\"eventTime\":\"2026-01-15T16:24:
24Z\",\"eventSource\":\"sts.amazonaws.com\",\"eventName\":\"AssumeRole\",\"awsRegion\":\"eu-north-1\",\"sourceIPAddress\":\"resource-explorer-2.amazonaws.co
m\",\"userAgent\":\"resource-explorer-2.amazonaws.com\",\"requestParameters\":{\"roleArn\":\"arn:aws:iam::879381257906:role/aws-service-role/resource-explor
messageType: DATA_MESSAGE owner: 879381257906 logGroup: aws-cloudtrail-logs-879381257906-9ecf6266 logStream: o-pn0spcswbk_879381257906_CloudTrail_us-eas
t-1_4 subscriptionFilters: sendlogs logEvents: { "id": "39438744697630042124561256027194289015064844246561849344", "timestamp": 1768494476150, "message":
"{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"Root\",\"principalId\":\"879381257906\",\"arn\":\"arn:aws:iam::879381257906:root\",\"accountId
\":\"879381257906\",\"accessKeyId\":\"ASIA4ZPZVD2ZMVRLMRE3\",\"sessionContext\":{\"attributes\":{\"creationDate\":\"2026-01-15T10:47:14Z\",\"mfaAuthenticate
d\":\"true\"}}},\"eventTime\":\"2026-01-15T16:25:38Z\",\"eventSource\":\"logs.amazonaws.com\",\"eventName\":\"DescribeMetricFilters\",\"awsRegion\":\"us-eas
messageType: DATA_MESSAGE owner: 879381257906 logGroup: aws-cloudtrail-logs-879381257906-9ecf6266 logStream: o-pn0spcswbk_511550631766_CloudTrail_us-eas
t-1_4 subscriptionFilters: sendlogs logEvents: { "id": "39438745489507203379185153202905041513820698224469409792", "timestamp": 1768494511659, "message":
"{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"AWSService\",\"invokedBy\":\"config.amazonaws.com\"},\"eventTime\":\"2026-01-15T16:26:27Z\",\"event
Source\":\"sts.amazonaws.com\",\"eventName\":\"AssumeRole\",\"awsRegion\":\"us-east-1\",\"sourceIPAddress\":\"config.amazonaws.com\",\"userAgent\":\"config.
amazonaws.com\",\"requestParameters\":{\"roleArn\":\"arn:aws:iam::511550631766:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig\",\"roleSe
messageType: DATA_MESSAGE owner: 879381257906 logGroup: aws-cloudtrail-logs-879381257906-9ecf6266 logStream: o-pn0spcswbk_879381257906_CloudTrail_us-eas
```

9. Workload Log Integration

9.1 AWS Lambda Logging

Lambda workloads were verified to emit logs to CloudWatch.

Test invocations confirmed correct log group and stream creation.


CloudWatch > Log management > /aws/lambda/firehoseLambda > 2026/01/15/[$LATEST]01b86768a39d44e3b06e29c27f82419e
CloudWatch
Favorites and recents
Ingestion
Dashboards
Alarms 0 0 0
In alarm
All alarms
Billing
AI Operations
GenAI Observability
Application Signals (APM) New
Infrastructure Monitoring
Logs
Log Management New
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Actions
Start tailing
Create metric filter
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display
Back to top

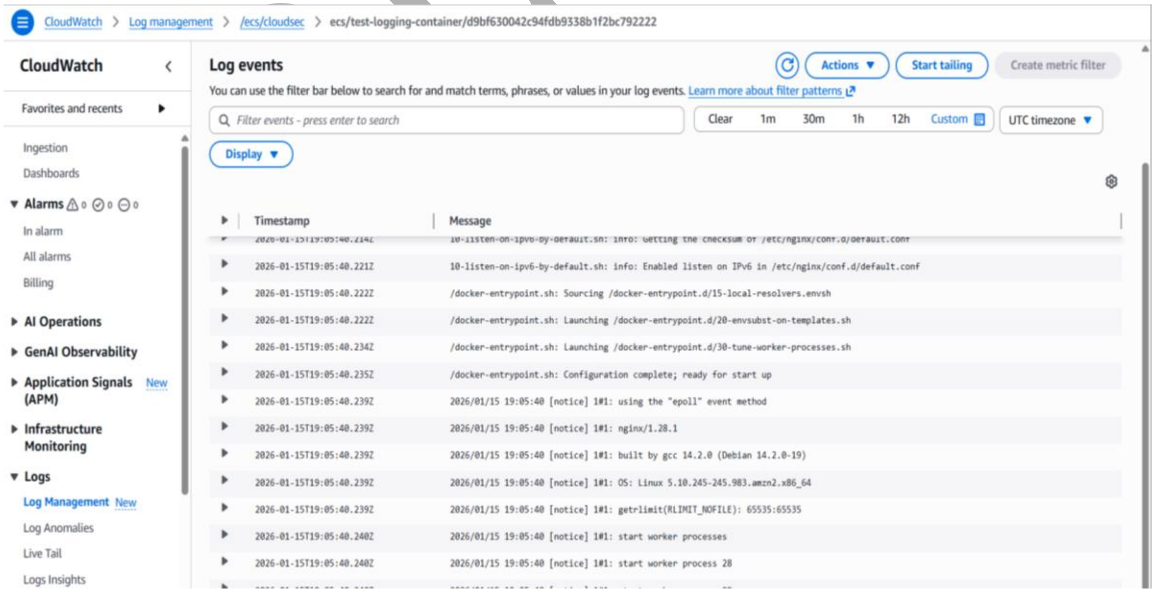
```
Timestamp                  Message
2026-01-15T18:20:37.669Z   END RequestId: bac6f639-8fa5-49d1-8c9c-d30d849c8aab
2026-01-15T18:20:37.669Z   REPORT RequestId: bac6f639-8fa5-49d1-8c9c-d30d849c8aab Duration: 38.07 ms Billed Duration: 39 ms Memory Size: 128 MB Max Memory Use…
2026-01-15T18:22:48.077Z   START RequestId: 176329b2-b0c3-4428-ab46-d821c67c2a2a Version: $LATEST
2026-01-15T18:22:48.130Z   END RequestId: 176329b2-b0c3-4428-ab46-d821c67c2a2a
2026-01-15T18:22:48.130Z   REPORT RequestId: 176329b2-b0c3-4428-ab46-d821c67c2a2a Duration: 52.01 ms Billed Duration: 53 ms Memory Size: 128 MB Max Memory Use…
2026-01-15T18:23:56.161Z   START RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0 Version: $LATEST

START RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0 Version: $LATEST

2026-01-15T18:23:56.194Z   END RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0

END RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0

2026-01-15T18:23:56.194Z   REPORT RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0 Duration: 33.01 ms Billed Duration: 34 ms Memory Size: 128 MB Max Memory Use…

REPORT RequestId: fcf351bb-c644-4e67-b81f-13a3a53038e0  Duration: 33.01 ms     Billed Duration: 34 ms  Memory Size: 128 MB    Max Memory Used: 45 MB

No newer events at this moment. Auto retry paused. Resume
```

9.2 ECS Container Logging

ECS Fargate workloads were configured using the awslogs driver.

Application logs were verified in dedicated CloudWatch log groups.

This ensured container workloads were centrally monitored.


CloudWatch > Log management > /ecs/cloudsec > ecs/test-logging-container/d9bf630042c94fdb9338b1f2bc792222
CloudWatch
Favorites and recents
Ingestion
Dashboards
Alarms 0 0 0
In alarm
All alarms
Billing
AI Operations
GenAI Observability
Application Signals (APM) New
Infrastructure Monitoring
Logs
Log Management New
Log Anomalies
Live Tail
Logs Insights
Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Actions
Start tailing
Create metric filter
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display

```
Timestamp                  Message
2026-01-15T19:05:40.214Z   10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
2026-01-15T19:05:40.221Z   10-listen-on-ipv6-by-default.sh: info: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
2026-01-15T19:05:40.222Z   /docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
2026-01-15T19:05:40.222Z   /docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
2026-01-15T19:05:40.234Z   /docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
2026-01-15T19:05:40.235Z   /docker-entrypoint.sh: Configuration complete; ready for start up
2026-01-15T19:05:40.239Z   2026/01/15 19:05:40 [notice] 1#1: using the "epoll" event method
2026-01-15T19:05:40.239Z   2026/01/15 19:05:40 [notice] 1#1: nginx/1.28.1
2026-01-15T19:05:40.239Z   2026/01/15 19:05:40 [notice] 1#1: built by gcc 14.2.0 (Debian 14.2.0-19)
2026-01-15T19:05:40.239Z   2026/01/15 19:05:40 [notice] 1#1: OS: Linux 5.10.245-245.983.amzn2.x86_64
2026-01-15T19:05:40.239Z   2026/01/15 19:05:40 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 65535:65535
2026-01-15T19:05:40.240Z   2026/01/15 19:05:40 [notice] 1#1: start worker processes
2026-01-15T19:05:40.240Z   2026/01/15 19:05:40 [notice] 1#1: start worker process 28
```

10. Durability and Backup Strategy

All logs delivered through Firehose are backed up to S3.

Lifecycle policies archive data to Glacier for long-term retention.

This provides durability, disaster recovery, and compliance support.

11. Governance and Documentation

All logging configurations, access policies, and retention standards were documented.

This supported:

- Audit reviews
- Compliance reporting
- Incident investigations
- Operational continuity

12. Outcomes and Impact

This implementation delivered:

- Centralized security visibility
- Improved incident response capability
- Compliance-aligned log retention
- Secure SIEM deployment
- Reliable log delivery
- Reduced operational blind spots

13. Conclusion

I designed and implemented a secure, scalable, and compliant centralized logging and observability platform on AWS.

Through automated log collection, secure analytics, and structured retention policies, this solution supports enterprise security monitoring, investigations, and regulatory requirements.