# Kết nối dữ liệu điện toán với dịch vụ Amazon OpenSearch và Amazon Managed Grafana

*Source: https://aws.amazon.com/blogs/big-data/correlate-telemetry-data-with-amazon-opensearch-service-and-amazon-managed-grafana/*

*Ngày: 03 tháng 4 năm 2025*

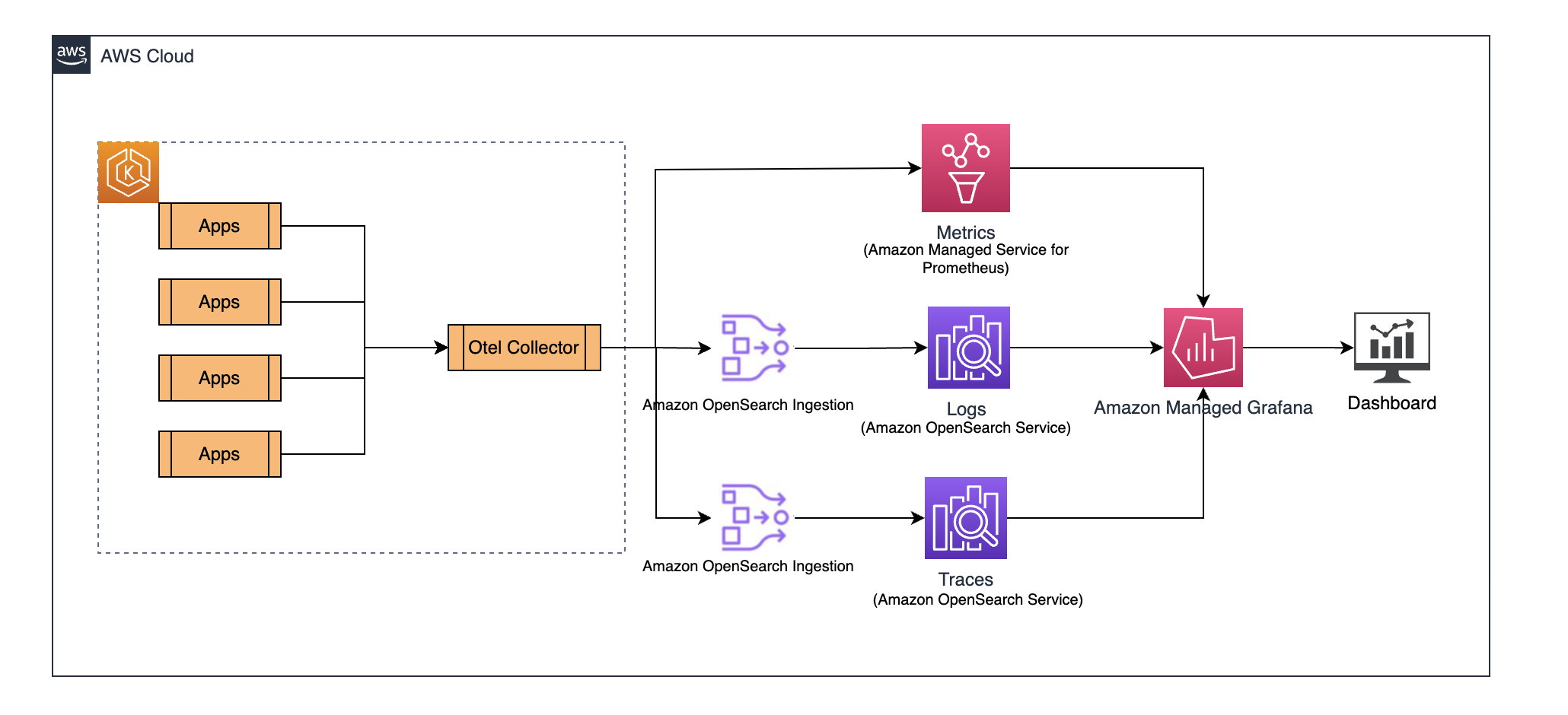
Việc khắc phục các vấn đề trong một ứng dụng doanh nghiệp lớn, phức tạp và phân tán liên quan đến những thách thức như theo dõi các yêu cầu trên nhiều dịch vụ, xác định những nút thắt hiệu suất trên toàn bộ hàng, và hiểu các thất bại hàng loạt giữa các dịch vụ phụ thuộc Các khách hàng thường cần phải làm việc với dữ liệu riêng biệt để xác định nguyên nhân cơ bản của vấn đề. Bằng cách tương quan các tín hiệu khác nhau như nhật ký, dấu vết, métrics và các chỉ số hiệu suất khác, bạn có thể có được một cái nhìn có giá trị về nguyên nhân gây ra pr Oblem, nơi nào và tại sao.

Amazon OpenSearch Service là một dịch vụ quản lý để triển khai, vận hành và tìm kiếm dữ liệu quy mô trong AWS. Amazon Managed Grafana là một dịch vụ trực quan hóa dữ liệu an toàn để truy vấn dữ liệu hoạt động từ nhiều nguồn, bao gồm cả OpenSearch Service.

Trong bài viết này, chúng tôi sẽ cho bạn thấy cách sử dụng các dịch vụ này để tương quan các tín hiệu quan sát khác nhau cải thiện phân tích nguyên nhân gốc rễ, do đó dẫn đến thời gian trung bình để giải quyết (MTTR) giảm. quy mô để giám sát chủ động các ứng dụng doanh nghiệp để tránh một vấn đề trước khi chúng xảy ra.

## Hình tổng quan của giải pháp

Bảng đồ họa sau đây cho thấy kiến trúc giải pháp để thu thập và tương quan các tín hiệu viễn thông doanh nghiệp khác nhau trên quy mô.



Trong lõi kiến trúc này là các ứng dụng bao gồm các dịch vụ vi mô (được đại diện bởi hộp cam) chạy trên Amazon Elastic Kubernetes Service (Amazon EKS). etrics, logs và traces. Dữ liệu này được xuất khẩu vào bộ sưu tập OpenTelemetry, phục vụ như một cửa ngõ agnostic nhà cung cấp trung tâm để thu thập dữ liệu này một cách đồng nhất.

Trong bài viết này, chúng tôi sử dụng một ứng dụng demo OpenTelemetry như một ứng dụng doanh nghiệp mẫu. Khách hàng doanh nghiệp lớn thường tách dữ liệu tín hiệu quan sát của họ thành các cửa hàng khác nhau để có thể mở rộng, cách ly lỗi, kiểm soát truy cập và dễ dàng sử dụng để hỗ trợ các chức năng này, chúng tôi khuyên bạn nên sử dụng Amazon OpenSearch Ingestion để tạo ra một đường ống dữ liệu không máy chủ, có thể mở rộng và được quản lý đầy đủ. o gửi dữ liệu số liệu đến Amazon Managed Service cho Prometheus.

Chúng tôi sử dụng Amazon Managed Grafana như một nền tảng hình ảnh hóa dữ liệu và phân tích để truy vấn và hình ảnh hóa dữ liệu này. Chúng tôi cũng cho thấy cách sử dụng mối tương quan như một công cụ có giá trị để có được thông tin sâu sắc từ các tín hiệu này lan rộng trên các cửa hàng dữ liệu khác nhau.

Các phần sau mô tả xây dựng kiến trúc này trên quy mô.

## Các điều kiện tiên quyết

Thực hiện các bước tiên quyết sau:

1. Cung cấp và cấu hình không gian làm việc Amazon Managed Prometheus để nhận số liệu từ bộ sưu tập OpenTelemetry.
2. Tạo hai miền dịch vụ OpenSearch chuyên dụng (hoặc sử dụng các tên miền hiện có) để thu nhập nhật ký và dấu vết từ bộ sưu tập OpenTelemetry.
3. Tạo một không gian làm việc Amazon Managed Grafana và cấu hình các nguồn dữ liệu để kết nối với Amazon Managed Prometheus và OpenSearch Service.
4. Thiết lập một cluster EKS để triển khai các ứng dụng và bộ sưu tập OpenTelemetry.

## Tạo các đường ống OpenSearch Ingestion

Trước khi thiết lập các đường ống tiêu thụ, bạn cần tạo ra các chính sách và vai trò cần thiết của AWS Identity and Access Management (IAM). sử dụng các chính sách này.

### Tạo một chính sách tiêu thụ

Thực hiện các bước sau đây để tạo ra chính sách IAM:

1. Mở máy điều khiển IAM.
2. Chọn Chính sách trong hộp điều hướng, sau đó chọn Tạo chính sách.
3. Trên tab JSON, nhập chính sách sau này vào trình chỉnh sửa:

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "es:DescribeDomain",  
            "Resource": "arn:aws:es:\*:{accountId}:domain/\*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "es:ESHttpGet", "es:HttpHead", "es:HttpDelete", "es:HttpPatch", "es:HttpPost", "es:HttpPut" ],  
            "Resource": "arn:aws:es:us-east-1:{accountId}:domain/otel-traces"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "es:ESHttpGet", "es:HttpHead", "es:HttpDelete", "es:HttpPatch", "es:HttpPost", "es:HttpPut" ],  
            "Resource": "arn:aws:es:us-east-1:{accountId}:domain/otel-logs"  
        }  
        }  
    ]  
}  
  
// Replace {accountId} with your own values

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "es:DescribeDomain",  
            "Resource": "arn:aws:es:\*:{accountId}:domain/\*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "es:ESHttpGet", "es:HttpHead", "es:HttpDelete", "es:HttpPatch", "es:HttpPost", "es:HttpPut" ],  
            "Resource": "arn:aws:es:us-east-1:{accountId}:domain/otel-traces"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "es:ESHttpGet", "es:HttpHead", "es:HttpDelete", "es:HttpPatch", "es:HttpPost", "es:HttpPut" ],  
            "Resource": "arn:aws:es:us-east-1:{accountId}:domain/otel-logs"  
        }  
        }  
    ]  
}  
  
// Replace {accountId} with your own values

1. Chọn Next, chọn Next một lần nữa, và đặt tên chính sách domain của bạn.
2. Chọn Create Policy.
3. Tạo một chính sách khác với tên osis-policy và sử dụng JSON sau:

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "osis:Ingest",  
            "Resource": "arn:aws:osis:us-east-1:{accountId}:pipeline/osi-pipeline-otellogs"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "osis:Ingest",  
            "Resource": "arn:aws:osis:us-east-1:{accountId}:pipeline/osi-pipeline-oteltraces"  
        }  
    ]  
}  
// Replace {accountId} with your own values

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "osis:Ingest",  
            "Resource": "arn:aws:osis:us-east-1:{accountId}:pipeline/osi-pipeline-otellogs"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "osis:Ingest",  
            "Resource": "arn:aws:osis:us-east-1:{accountId}:pipeline/osi-pipeline-oteltraces"  
        }  
    ]  
}  
// Replace {accountId} with your own values

### Tạo một vai trò đường ống

Thực hiện các bước sau đây để tạo ra vai trò đường ống:

1. Trên bảng điều khiển IAM, chọn Roles trong bảng điều hướng, sau đó chọn Create role.
2. Chọn chính sách tin tưởng tùy chỉnh và nhập chính sách sau này vào trình chỉnh sửa:

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "eks.amazonaws.com",  
                    "osis-pipelines.amazonaws.com"  
                ],  
                "AWS": "{nodegroup\_arn}"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}  
  
// Replace {nodegroup\_arn} with your own values

{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "eks.amazonaws.com",  
                    "osis-pipelines.amazonaws.com"  
                ],  
                "AWS": "{nodegroup\_arn}"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}  
  
// Replace {nodegroup\_arn} with your own values

1. Chọn Next, sau đó tìm kiếm và chọn chính sách chính sách và chính sách miền mà bạn vừa tạo.
2. Chọn Next và đặt tên vai PipelineRole.
3. Chọn Create role.

osis-policy

domain-policy

PipelineRole

### Cho phép truy cập cho vai trò đường ống trong các miền dịch vụ OpenSearch

Để cho phép truy cập cho vai trò đường ống trong các miền dịch vụ OpenSearch, hoàn thành các bước sau:

1. Mở máy điều khiển OpenSearch Service.
2. Chọn miền của bạn (hoặc nhật ký hoặc dấu vết).
3. Chọn URL bảng điều khiển OpenSearch
4. Đăng nhập với giấy chứng nhận của bạn.

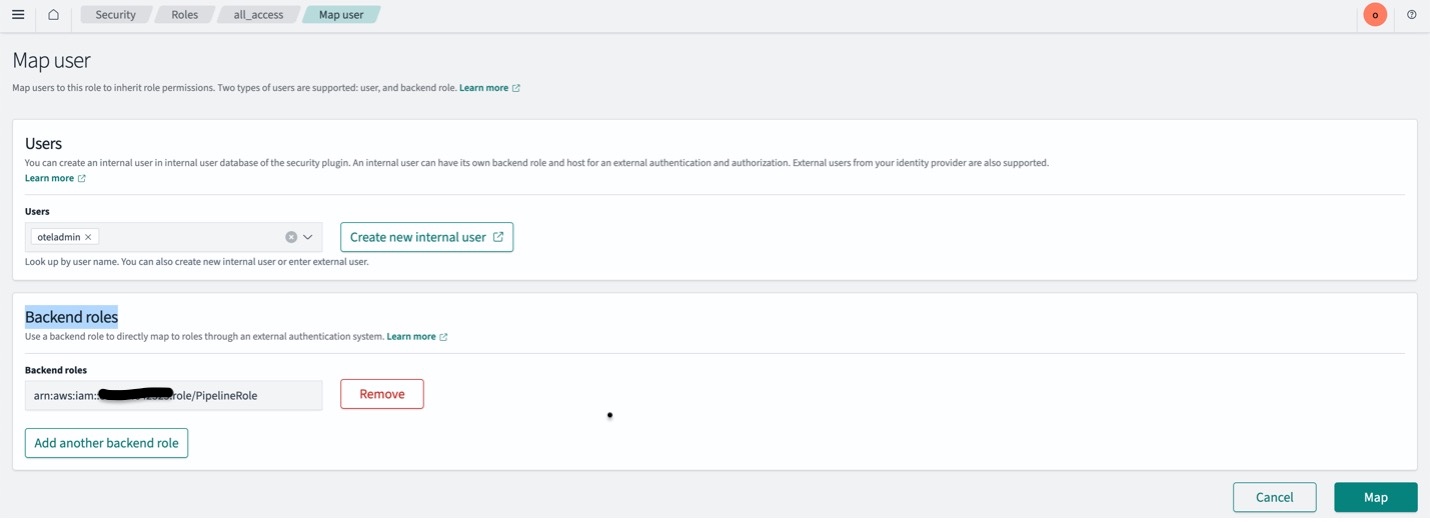
Sau đó, hoàn thành các bước sau đây cho mỗi miền dịch vụ OpenSearch (logbo và các tên miền theo dõi).

1. Trong bảng điều khiển OpenSearch, đi đến an ninh
2. Chọn Roles và sau đó all\_access.

Quy trình này chỉ sử dụng vai trò all\_access cho mục đích minh chứng. Điều này cho phép quyền hành chính đầy đủ cho vai trò đường ống, vi phạm nguyên tắc quyền tối thiểu và có thể gây ra rủi ro an ninh. Đối với môi trường sản xuất, bạn có thể sử dụng các công cụ này để tạo ra các thông tin về các công cụ. nên tạo ra một vai trò tùy chỉnh với tối thiểu các quyền được yêu cầu cho việc hấp thụ dữ liệu, giới hạn quyền chỉ số và hoạt động cụ thể, xem xét việc triển khai các mô hình chỉ số và kiểm soát truy cập dựa trên thời gian, và thường xuyên kiểm tra bản đồ vai trò và cho phép Để biết chi tiết về việc tạo các vai trò tùy chỉnh với các quyền thích hợp, hãy xem Bảo mật trong dịch vụ Amazon OpenSearch.

1. Chọn Maped users và sau đó quản lý bản đồ.
2. Trên trang người dùng Map, dưới vai trò Backend, cập nhật vai trò backend với Amazon Resource Name (ARN) cho vai trò PiplelineRole.
3. Chọn Map.

PiplelineRole



### Tạo một đường ống cho các nhật ký

Thực hiện các bước sau đây để tạo ra một đường ống cho các nhật ký:

1. Mở máy điều khiển OpenSearch Service.
2. Chọn đường ống nước.
3. Chọn tạo đường ống.
4. Định nghĩa cấu hình đường ống bằng cách nhập các thông tin sau:

version: "2"  
otel-logs-pipeline:  
  source:  
    otel\_logs\_source:  
      path: "/v1/logs"  
  sink:  
    - opensearch:  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:  
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
          serverless: false  
        index: "observability-otel-logs%{yyyy-MM-dd}"  
         
 # To get the values for the placeholders:  
 # 1. {OpenSearch\_domain\_endpoint}: You can find the domain endpoint by navigating to the Amazon Managed Opensearch managed clusters in the AWS Management Console, and then clicking on the domain.  
 # After obtaining the necessary values, replace the placeholders in the configuration with the actual values.

version: "2"  
otel-logs-pipeline:  
  source:  
    otel\_logs\_source:  
      path: "/v1/logs"  
  sink:  
    - opensearch:  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:  
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
          serverless: false  
        index: "observability-otel-logs%{yyyy-MM-dd}"  
         
 # To get the values for the placeholders:  
 # 1. {OpenSearch\_domain\_endpoint}: You can find the domain endpoint by navigating to the Amazon Managed Opensearch managed clusters in the AWS Management Console, and then clicking on the domain.  
 # After obtaining the necessary values, replace the placeholders in the configuration with the actual values.

### Tạo một đường ống để tìm ra dấu vết

Thực hiện các bước sau đây để tạo ra một đường ống dẫn để tìm thấy dấu vết:

1. Mở máy điều khiển OpenSearch Service.
2. Chọn đường ống nước.
3. Chọn tạo đường ống.
4. Định nghĩa cấu hình đường ống bằng cách nhập các thông tin sau:

version: "2"  
entry-pipeline:  
  source:  
    otel\_trace\_source:  
      path: "/v1/traces"  
  processor:  
    - trace\_peer\_forwarder:  
  sink:  
    - pipeline:  
        name: "span-pipeline"  
    - pipeline:  
        name: "service-map-pipeline"  
span-pipeline:  
  source:  
    pipeline:  
      name: "entry-pipeline"  
  processor:  
    - otel\_traces:  
  sink:  
    - opensearch:  
        index\_type: "trace-analytics-raw"  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:                   
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
service-map-pipeline:  
  source:  
    pipeline:  
      name: "entry-pipeline"  
  processor:  
    - service\_map:  
  sink:  
    - opensearch:  
        index\_type: "trace-analytics-service-map"  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:                   
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
           
 # To get the values for the placeholders:  
 # 1. {OpenSearch\_domain\_endpoint}: You can find the domain endpoint by navigating to the Amazon Managed Opensearch managed clusters in the AWS Management Console, and then clicking on the domain.  # 2. {accountId}: This is your AWS account ID. You can find your account ID by clicking on your username in the top-right corner of the AWS Management Console and selecting "My Account" from the dropdown menu.  
 # After obtaining the necessary values, replace the placeholders in the configuration with the actual values.

version: "2"  
entry-pipeline:  
  source:  
    otel\_trace\_source:  
      path: "/v1/traces"  
  processor:  
    - trace\_peer\_forwarder:  
  sink:  
    - pipeline:  
        name: "span-pipeline"  
    - pipeline:  
        name: "service-map-pipeline"  
span-pipeline:  
  source:  
    pipeline:  
      name: "entry-pipeline"  
  processor:  
    - otel\_traces:  
  sink:  
    - opensearch:  
        index\_type: "trace-analytics-raw"  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:                   
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
service-map-pipeline:  
  source:  
    pipeline:  
      name: "entry-pipeline"  
  processor:  
    - service\_map:  
  sink:  
    - opensearch:  
        index\_type: "trace-analytics-service-map"  
        hosts: ["{OpenSearch\_domain\_endpoint}"]  
        aws:                   
          sts\_role\_arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
          region: "us-east-1"  
           
 # To get the values for the placeholders:  
 # 1. {OpenSearch\_domain\_endpoint}: You can find the domain endpoint by navigating to the Amazon Managed Opensearch managed clusters in the AWS Management Console, and then clicking on the domain.  # 2. {accountId}: This is your AWS account ID. You can find your account ID by clicking on your username in the top-right corner of the AWS Management Console and selecting "My Account" from the dropdown menu.  
 # After obtaining the necessary values, replace the placeholders in the configuration with the actual values.

## Cài đặt ứng dụng demo OpenTelemetry trong Amazon EKS

Sử dụng cụ thể EKS bạn đã thiết lập trước đó cùng với AWS CloudShell hoặc công cụ khác để hoàn thành các bước sau:

1. Mở Console quản lý AWS.
2. Chọn biểu tượng CloudShell trong thanh điều hướng trên cùng, hoặc trực tiếp vào máy điều khiển CloudShell.
3. Chờ cho môi trường shell khởi động nó được cài đặt sẵn với công cụ giao diện dòng lệnh AWS (AWS CLI) phổ biến.

Bây giờ bạn có thể hoàn thành các bước sau để cài đặt ứng dụng.

1. Khả năng sao chép kho demo OpenTelemetry:

git clone https://github.com/aws-samples/sample-correlation-opensearch-repository

git clone https://github.com/aws-samples/sample-correlation-opensearch-repository

1. Di chuyển đến thư mục Kubernetes:

cd deployment\_files

cd deployment\_files

1. Dùng ứng dụng demo bằng cách sử dụng kubectl áp dụng:

kubectl apply -f .

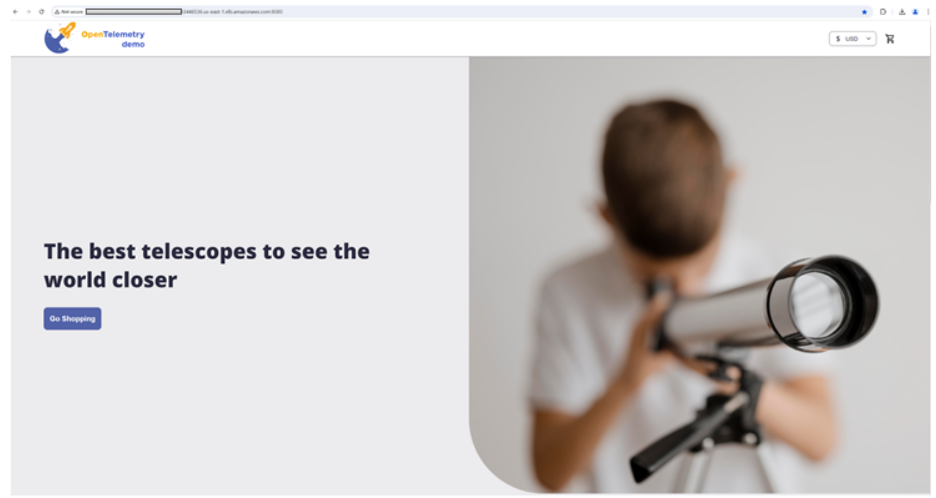
kubectl apply -f .

1. Sử dụng một bộ cân bằng tải để phơi bày dịch vụ đầu cuối để bạn có thể truy cập URL web ứng dụng nguồn:

kubectl expose deployment opentelemetry-demo-frontendproxy --type=LoadBalancer --name=frontendproxy

kubectl expose deployment opentelemetry-demo-frontendproxy --type=LoadBalancer --name=frontendproxy

1. Sau khi bạn đã triển khai ứng dụng, truy cập ứng dụng đầu tiên bằng cách sử dụng bộ cân bằng tải trên cổng 8080. Sử dụng trình duyệt của bạn để truy cập http://<LoadBalancerIP>:8080/ để mở ứng dụng nguồn cho OpenTelemetry.



Bằng cách làm theo các bước này, bạn có thể cài đặt và truy cập thành công các ứng dụng demo trên cluster EKS của mình.

## Cài đặt các nhà xuất khẩu OpenTelemetry Collector cho các nhật ký, dấu vết và số liệu

OpenTelemetry Collector là một công cụ quản lý việc nhận, xử lý và xuất dữ liệu viễn thông từ ứng dụng của bạn sang kho mục tiêu.

Trong bước này, chúng tôi gửi nhật ký và dấu vết đến Dịch vụ OpenSearch và số liệu đến Amazon Managed Prometheus. là phần, chúng tôi bao gồm các bước để cấu hình bộ sưu tập OpenTelemetry trong môi trường EKS. Sau đó chúng tôi triển khai ứng dụng demo và khám phá các nhà xuất khẩu OpenTelemetry sử dụng Giải pháp quản lý AWS thay vì phiên bản nguồn mở.

Thực hiện các bước sau:

1. Mở ConfigMap config-config otel-collector-in your preferred editor:

kubectl edit configmap opentelemetry-demo-otelcol -n otel-demo

kubectl edit configmap opentelemetry-demo-otelcol -n otel-demo

1. Cập nhật phần xuất khẩu với cấu hình sau (giải ý các URL nhập nhật ký của dịch vụ Prometheus và OpenSearch)

exporters:  
     logging: {}  
     otlphttp/logs:  
       logs\_endpoint: "<AWS\_OPENSEARCH\_LOG\_INGESTION\_URL>/v1/logs"  
       auth:  
         authenticator: sigv4auth  
       compression: none  
     otlphttp/traces:  
       traces\_endpoint: "<AWS\_OPENSEARCH\_TRACE\_INGESTION\_URL>/v1/traces"  
       auth:  
         authenticator: sigv4auth  
       compression: none  
     prometheusremotewrite:  
        endpoint: "<AWS\_MANAGED\_PROMETHEUS\_ENDPOINT>"  
        auth:  
          authenticator: sigv4auth

exporters:  
     logging: {}  
     otlphttp/logs:  
       logs\_endpoint: "<AWS\_OPENSEARCH\_LOG\_INGESTION\_URL>/v1/logs"  
       auth:  
         authenticator: sigv4auth  
       compression: none  
     otlphttp/traces:  
       traces\_endpoint: "<AWS\_OPENSEARCH\_TRACE\_INGESTION\_URL>/v1/traces"  
       auth:  
         authenticator: sigv4auth  
       compression: none  
     prometheusremotewrite:  
        endpoint: "<AWS\_MANAGED\_PROMETHEUS\_ENDPOINT>"  
        auth:  
          authenticator: sigv4auth

1. Tìm phần mở rộng và cập nhật ARN vai trò IAM trong cấu hình sigv4auth:

sigv4auth:  
 assume\_role:  
 arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
 sts\_region: "us-east-1"  
 region: "us-east-1"  
 service: "osis"  
 # {accountId}: replace accountID with your account id

sigv4auth:  
 assume\_role:  
 arn: "arn:aws:iam::{accountId}:role/osi-pipeline-role"  
 sts\_region: "us-east-1"  
 region: "us-east-1"  
 service: "osis"  
 # {accountId}: replace accountID with your account id

1. Sau khi cập nhật ConfigMap, khởi động lại việc triển khai OpenTelemetry Collector:

kubectl rollout restart deployment opentelemetry-demo-otelcol -n otel-demo

kubectl rollout restart deployment opentelemetry-demo-otelcol -n otel-demo

Với những thay đổi này, bộ sưu tập OpenTelemetry sẽ gửi dữ liệu theo dõi đến miền dịch vụ OpenSearch, dữ liệu métrics đến dịch vụ quản lý AWS cho điểm cuối Prometheus và dữ liệu nhật ký đến miền dịch vụ OpenSearch.

## Cài đặt Amazon quản lý Grafana

Trước khi bạn có thể hình dung nhật ký và dấu vết của mình, bạn cần phải cấu hình OpenSearch Service như một nguồn dữ liệu trong không gian làm việc Amazon Managed Grafana của bạn.

### Cài đặt nguồn dữ liệu OpenSearch Service

Thực hiện các bước sau đây để cấu hình nguồn dữ liệu của OpenSearch Service:

1. Mở máy điều khiển Amazon Managed Grafana.
2. Chọn không gian làm việc của bạn và chọn URL không gian làm việc để truy cập vào bản đồ Grafana của bạn.
3. Nhập vào phiên bản Amazon quản lý Grafana của bạn.
4. Từ menu bên, chọn biểu tượng cấu hình (gear).
5. Trong menu Cài đặt, chọn Quên dữ liệu.
6. Chọn Add nguồn dữ liệu.
7. Trên trang Thêm nguồn dữ liệu, chọn OpenSearch Service từ danh sách các nguồn dữ liệu có sẵn.
8. Trong trường Name, nhập một tên mô tả cho nguồn dữ liệu.
9. Trong trường URL, nhập URL (OpenSearch Service domain endpoint) của tên miền OpenSearch Service của bạn, bao gồm giao thức và số cổng.
10. Nếu cụm OpenSearch của bạn được cấu hình với xác thực, cung cấp các thông tin tin xác thực cần thiết trong User và Password
11. Nếu bạn muốn sử dụng một mẫu chỉ mục cụ thể cho nguồn dữ liệu, bạn có thể chỉ định nó trong trường tên Index (ví dụ, logstash-\*).
12. Điều chỉnh bất kỳ cài đặt khác nếu cần thiết, chẳng hạn như tên trường Thời gian và khoảng thời gian Thời gian.
13. Chọn Save & Test để xác minh kết nối với cụm OpenSearch của bạn.

logstash-\*

Nếu thử nghiệm thành công, bạn nên thấy thông báo màu xanh lá cây với thông điệp Sản lượng dữ liệu đang hoạt động.

1. Chọn Save để lưu cấu hình nguồn dữ liệu.
2. Lặp lại các bước tương tự cho các tên miền OpenSearch log và traces.

### Thiết lập nguồn dữ liệu Prometheus

Thực hiện các bước sau đây để cấu hình nguồn dữ liệu Prometheus:

1. Mở máy điều khiển Amazon Managed Grafana.
2. Chọn không gian làm việc của bạn và chọn URL không gian làm việc để truy cập vào bản đồ Grafana của bạn.
3. Nhập vào phiên bản Amazon quản lý Grafana của bạn.
4. Từ menu bên, chọn biểu tượng cấu hình (gear).
5. Trong menu Cài đặt, chọn Quên dữ liệu.
6. Chọn Add nguồn dữ liệu.
7. Trên trang Thêm nguồn dữ liệu, chọn Amazon Managed Prometheus từ danh sách các nguồn dữ liệu có sẵn.
8. Trong trường Name, nhập một tên mô tả cho nguồn dữ liệu.
9. Các trường AWS Author Provider và Default Region nên được tự động lấp đầy dựa trên cấu hình không gian làm việc Amazon Managed Grafana của bạn.
10. Trong trường Workspace, nhập ID hoặc tên đếm của không gian làm việc Amazon quản lý Prometheus của bạn.
11. Chọn Save & Test để xác minh kết nối với không gian làm việc Amazon Managed Prometheus của bạn.

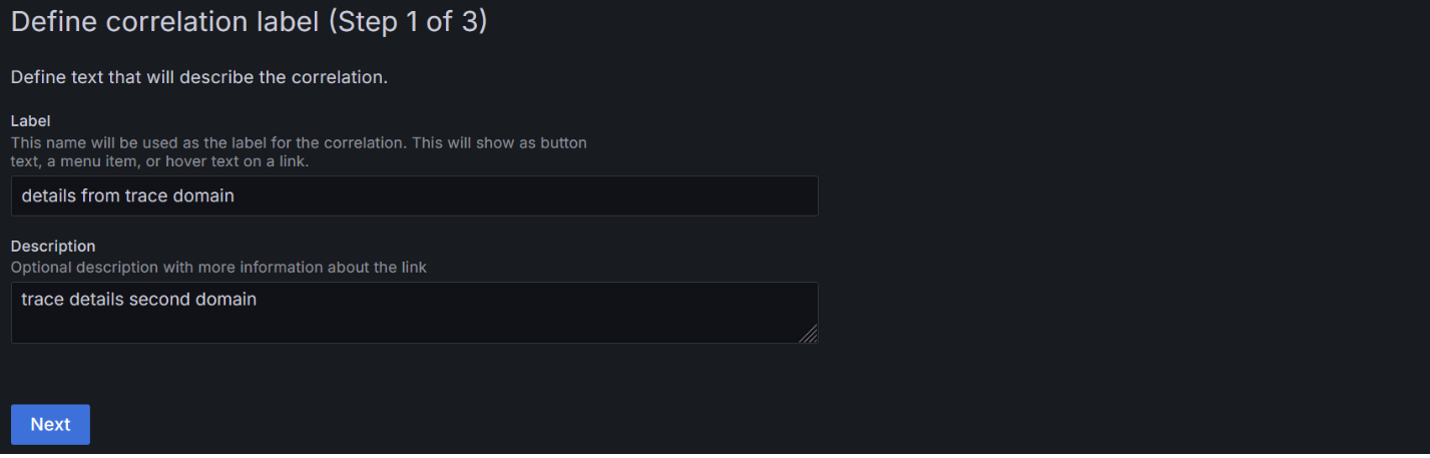
Nếu thử nghiệm thành công, bạn nên thấy thông báo màu xanh lá cây với thông điệp Sản lượng dữ liệu đang hoạt động.

1. Chọn Save để lưu cấu hình nguồn dữ liệu.

## Tạo liên kết trong Amazon quản lý Grafana

Để thiết lập kết nối giữa các nhật ký và dữ liệu theo dõi của bạn, bạn cần thiết lập mối tương quan dữ liệu trong Amazon Managed Grafana. Điều này cho phép bạn điều hướng liền mạch giữa các nhật ký và các dấu vết liên quan. Thực hiện các bước này trong công việc của bạn Amazon Managed Grafana không gian:

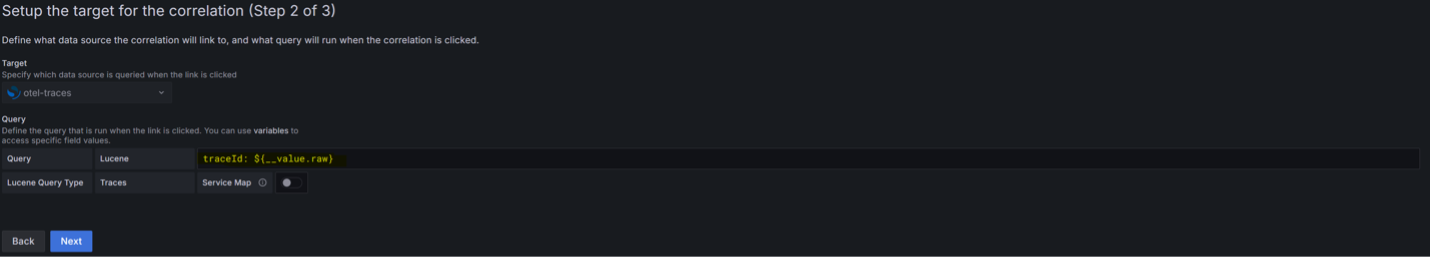
1. Mở máy điều khiển Amazon Managed Grafana.
2. Chọn không gian làm việc của bạn và chọn URL không gian làm việc để truy cập vào bản đồ Grafana của bạn.
3. Trong cổng thông tin Amazon quản lý Grafana, trong menu Quản trị, chọn Plugins và Data, và chọn Correlation.



1. Trong mục Cài đặt mục tiêu cho trang tương quan, trong mục tiêu, chọn nguồn dữ liệu dấu vết của bạn (OpenSearch Service, ví dụ, otel-traces) từ danh sách thả xuống và xác định truy vấn sẽ được thực hiện khi liên kết được theo dõi. Bạn có thể sử dụng variable les để truy vấn các giá trị trường cụ thể. ví dụ, traceId: ${\_\_value.raw}.

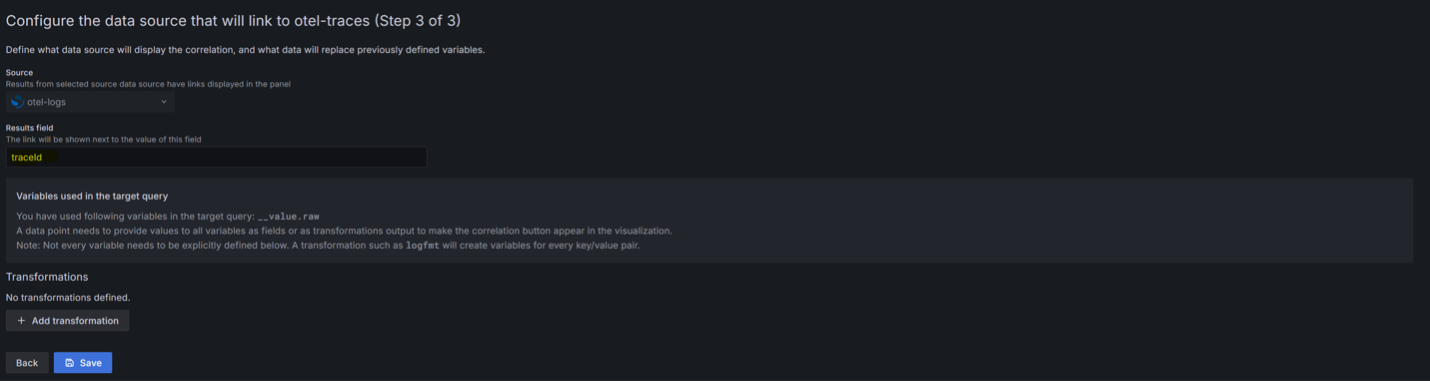
otel-traces

traceId: ${\_\_value.raw}

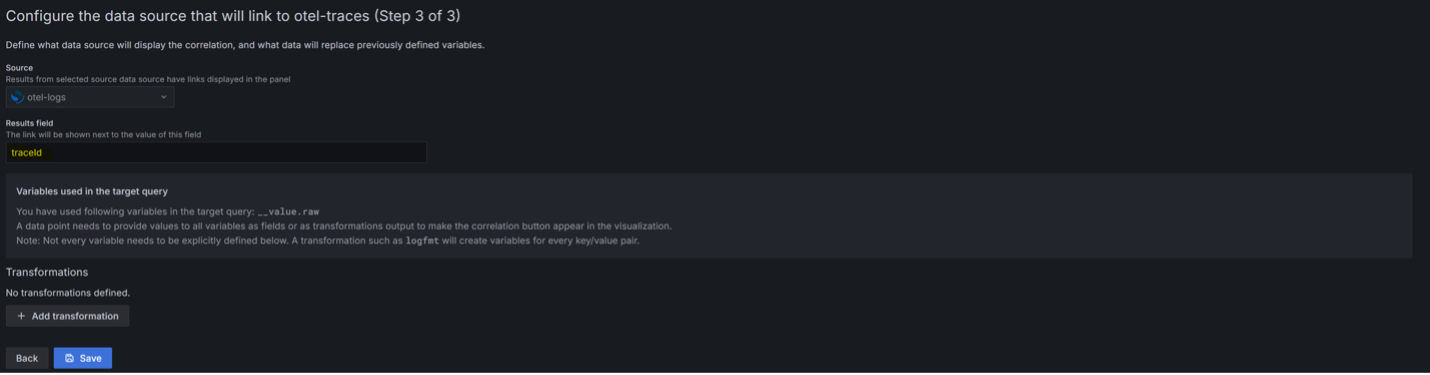


1. Trong mục đặt mục tiêu cho trang tương quan, chọn nguồn dữ liệu nhật ký từ danh sách thả xuống, và nhập tên trường để được liên kết hoặc tương quan với nguồn dữ liệu dấu vết trong nguồn dữ liệu OpenSearch Service. ví dụ, traceID.

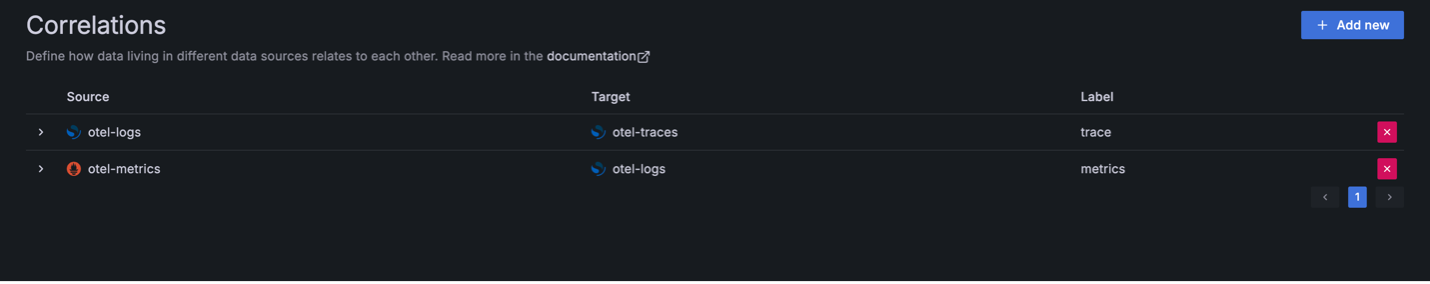
traceID



1. Chọn Save để hoàn thành cấu hình tương quan.

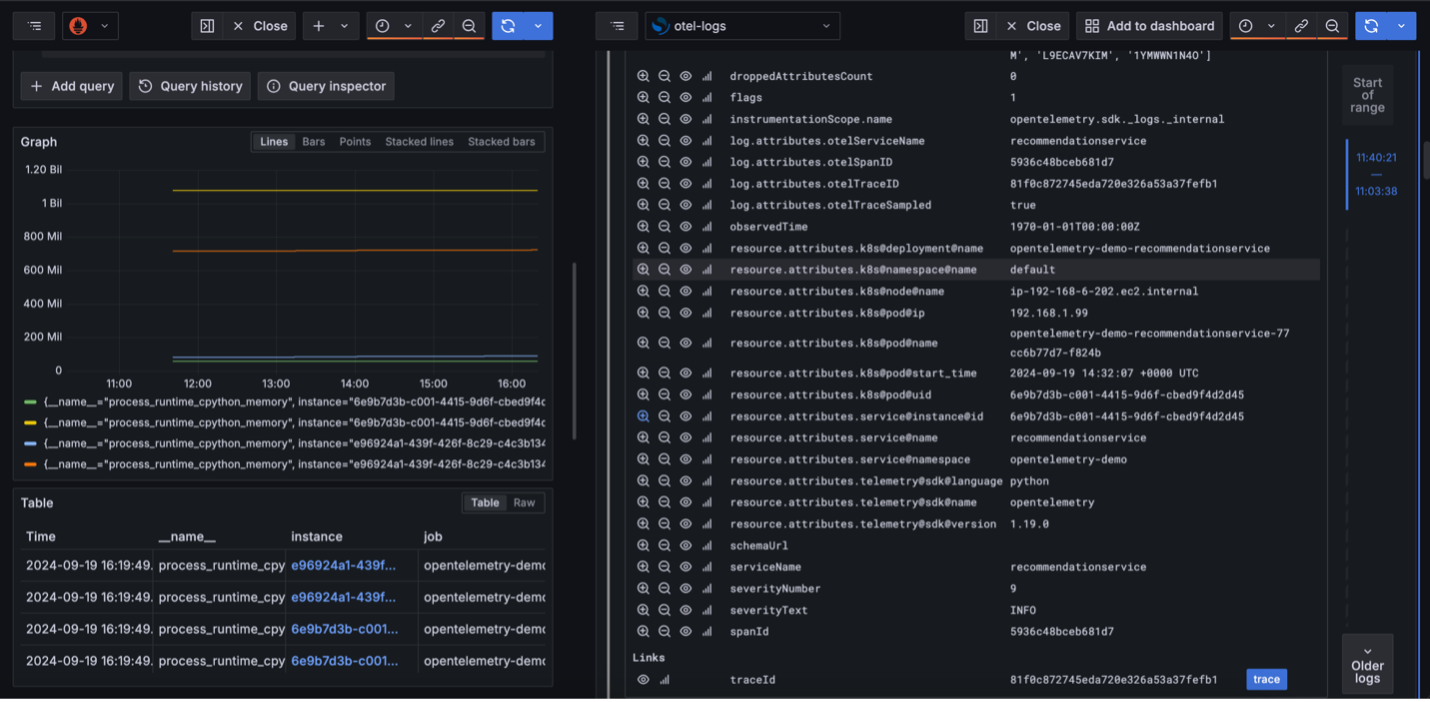


1. Lặp lại các bước để tạo mối tương quan giữa các métrics trên Prometheus với các bản ghi trong OpenSearch Service.

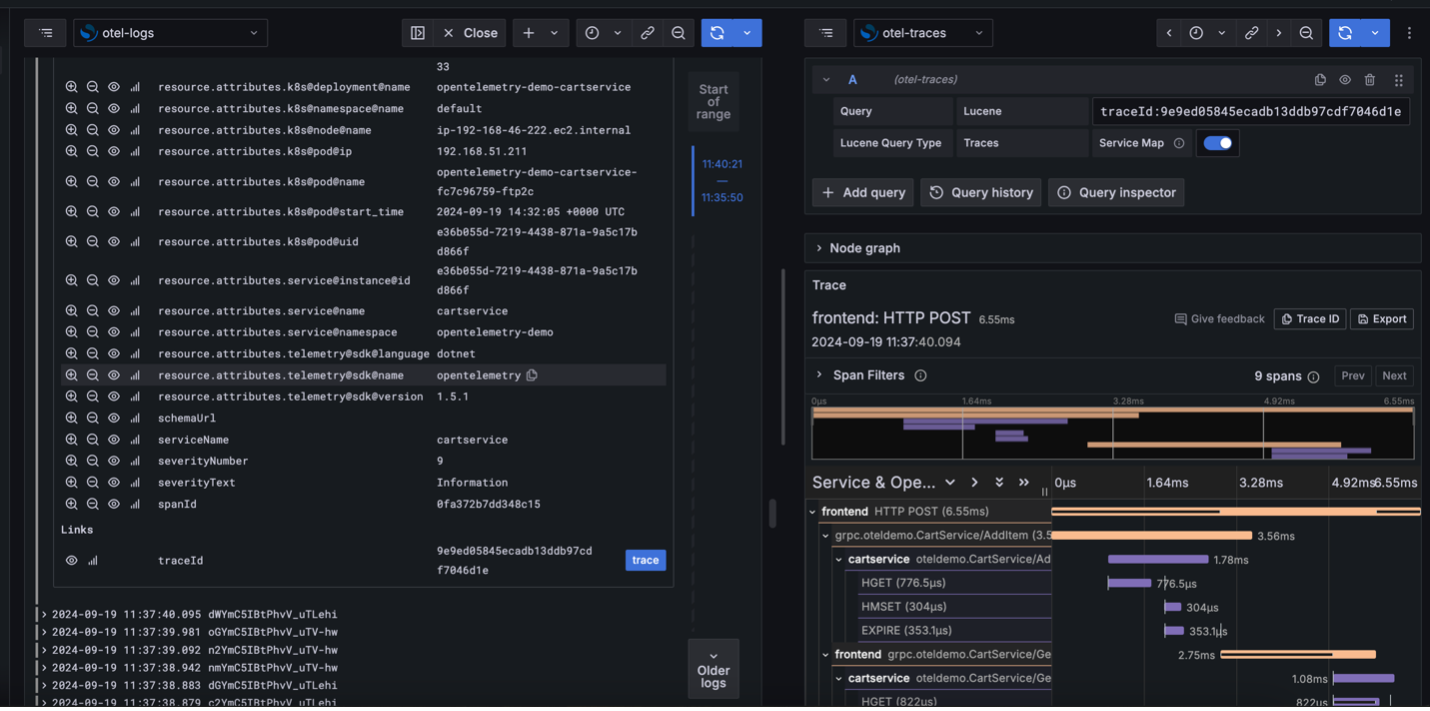


## Thiết lập kết quả

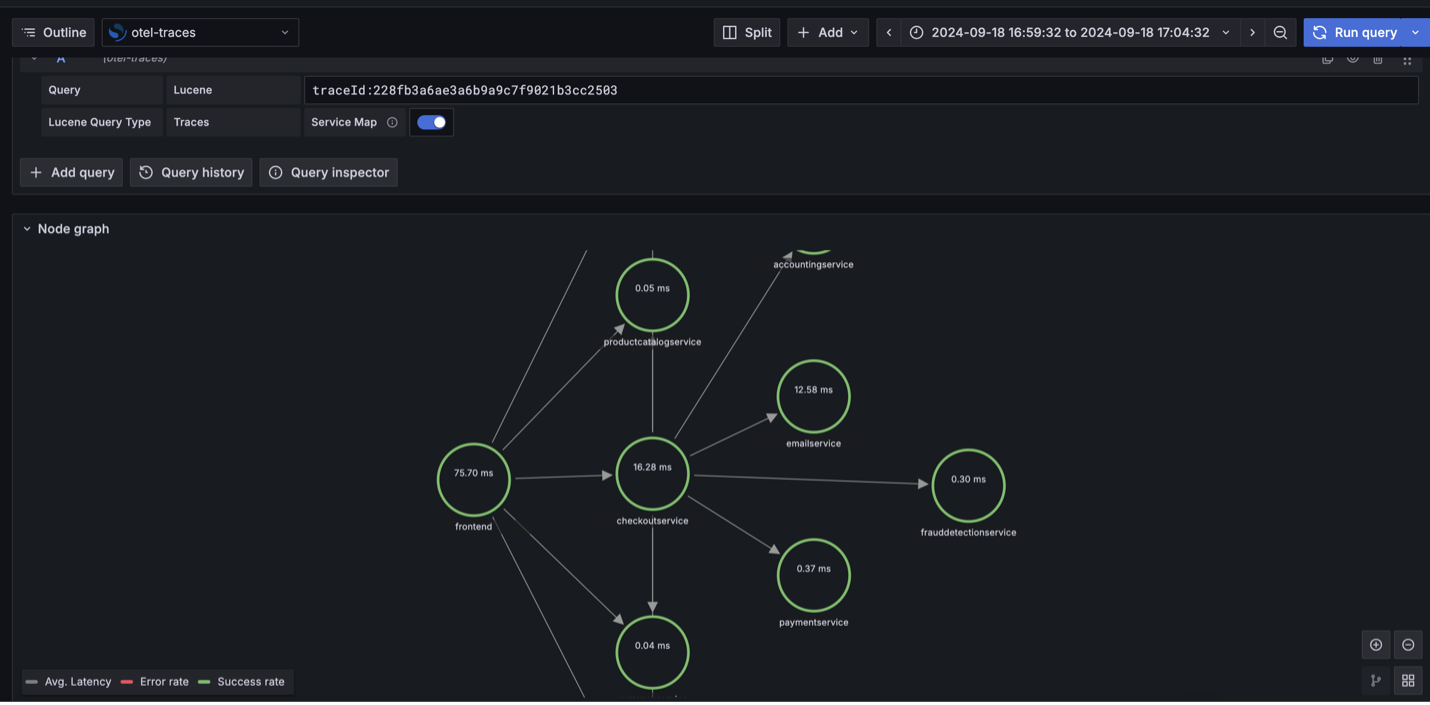
Trong Amazon Managed Grafana, sử dụng nguồn dữ liệu Prometheus, tìm thấy ví dụ mong muốn để tương quan. ID ví dụ sẽ được hiển thị như một liên kết. Hãy theo liên kết để mở các chi tiết nhật ký tương ứng trong một bảng ở phía bên phải của trang.



Với các nhật ký để kết hợp dấu vết được cấu hình, bạn có thể truy cập thông tin dấu vết trực tiếp từ trang nhật ký. Chọn dấu vết trên bảng chi tiết nhật ký để xem dữ liệu dấu vết tương ứng.



Bức ảnh màn hình sau đây cho thấy hình ảnh biểu đồ nút cho thấy dòng chảy tương quan: métrics trường hợp đến nhật ký đến dấu vết.



## Làm sạch

Xóa cơ sở hạ tầng cho giải pháp này khi không được sử dụng để tránh gây ra chi phí không cần thiết.

## Kết luận

Trong bài viết này, chúng tôi đã chỉ ra cách sử dụng tương quan như một công cụ hữu ích để có được cái nhìn sâu sắc về dữ liệu có thể quan sát được lưu trữ trong các cửa hàng khác nhau.

Việc tách các nhật ký và dấu vết thành các miền riêng cung cấp những lợi ích sau đây:

* Việc phân bổ và quy mô tài nguyên tốt hơn dựa trên các mô hình tải trọng công việc khác nhau
* Tối ưu hóa hiệu suất độc lập cho mỗi loại dữ liệu
* Theo dõi và quản lý chi phí đơn giản
* Kiểm soát an ninh được tăng cường với các chính sách truy cập riêng biệt

Bạn có thể sử dụng giải pháp này như một tham chiếu để xây dựng một giải pháp quan sát có thể mở rộng cho doanh nghiệp của bạn để phát hiện, điều tra và khắc phục các vấn đề nhanh hơn. Khả năng này, khi được sử dụng trong suốt thế hệ tiếp theo trí tuệ nhân tạo và học máy (AI/ML), giúp không chỉ phản ứng chủ động mà còn dự đoán và ngăn ngừa các vấn đề trước khi chúng xảy ra. Bạn có thể tìm hiểu thêm về AI/ML với AWS.

### Về tác giả

Balaji Mohan là một cố vấn phân phối cấp cao chuyên về ứng dụng và hiện đại hóa dữ liệu cho đám mây. Phương pháp kinh doanh đầu tiên của ông cung cấp chuyển đổi liền mạch, phù hợp công nghệ với mục tiêu tổ chức. Sử dụng kiến trúc tập trung trên đám mây , ông cung cấp các giải pháp có thể mở rộng, nhanh nhẹn và hiệu quả về chi phí, thúc đẩy đổi mới và tăng trưởng.



Senthil Ramasamy là một cố vấn cơ sở dữ liệu cao cấp tại Amazon Web Services. Ông làm việc với khách hàng AWS để cung cấp hướng dẫn và hỗ trợ kỹ thuật về các dịch vụ cơ sở dữ liệu, giúp họ chuyển đổi cơ sở dữ liệu sang AWS Cloud và cải thiện giá trị của giải pháp của họ khi sử dụng AWS.



Muthu Pitchaimani là một chuyên gia tìm kiếm với dịch vụ Amazon OpenSearch. Ông xây dựng các ứng dụng tìm kiếm và giải pháp quy mô lớn. Muthu quan tâm đến các chủ đề mạng và an ninh, và có trụ sở tại Austin, Texas.



Lập nhận xét...