Contents

[**Giai đoạn 4: Giám sát và ghi nhật ký** 2](#_Toc202378201)

[**Nhiệm vụ 4.1: Sử dụng CloudTrail để ghi lại các cuộc gọi API của Amazon S3** 2](#_Toc202378202)

[**Bước 1: Tạo CloudTrail Trail** 2](#_Toc202378203)

[**Bước 2: Tạo file CSV để test** 4](#_Toc202378204)

[**Bước 3: Tạo bảng Athena để đọc log từ CloudTrail** 5](#_Toc202378205)

[**Bước 4: Truy vấn log upload file với Athena** 5](#_Toc202378206)

[**Nhiệm vụ 4.2: Sử dụng CloudWatch Logs để theo dõi nhật ký an toàn** 8](#_Toc202378207)

[**Bước 1: Tạo CloudWatch Log Group** 8](#_Toc202378208)

[**Bước 2: Kết nối với EC2 qua EC2 Instance Connect** 9](#_Toc202378209)

[**Bước 3: Cài đặt CloudWatch Agent và collectd** 9](#_Toc202378210)

[**Bước 4: Tải file cấu hình cho CloudWatch Agent** 10](#_Toc202378211)

[**Bước 5: Khởi động CloudWatch Agent** 11](#_Toc202378212)

[**Bước 7: Theo dõi trực tiếp file log /var/log/secure** 13](#_Toc202378213)

[**Bước 8: SSH vào instance từ AWS Cloud9 để tạo log** 13](#_Toc202378214)

[**Bước 9: Đăng nhập thất bại (tạo log failed)** 15](#_Toc202378215)

[**Bước 10: Kiểm tra log trong CloudWatch** 15](#_Toc202378216)

[**Nhiệm vụ 4.3: Tạo báo động CloudWatch để gửi thông báo về các sự cố bảo mật** 16](#_Toc202378217)

[**Bước 1: Tạo Metric Filter cho Log Group** 16](#_Toc202378218)

[**Bước 2: Tạo CloudWatch Alarm từ Metric Filter** 17](#_Toc202378219)

[**Bước 3: Xác nhận email để nhận thông báo từ SNS** 19](#_Toc202378220)

[**Bước 4: Mô phỏng tấn công SSH sai** 20](#_Toc202378221)

[**Bước 5: Kiểm tra CloudWatch Logs và Alarm** 21](#_Toc202378222)

[**Nhiệm vụ 4.4: Cấu hình AWS Config để đánh giá cài đặt bảo mật và khắc phục cấu hình tài nguyên AWS** 22](#_Toc202378223)

[**Bước 1: Tạo bucket compliance** 22](#_Toc202378224)

[**Bước 2: Bật ACL cho bucket ghi log** 22](#_Toc202378225)

[**Bước 3: Cấu hình AWS Config** 22](#_Toc202378226)

[**Giai đoạn 5: Kết thúc phiên của bạn** 27](#_Toc202378227)

# **Giai đoạn 4: Giám sát và ghi nhật ký**

Nhóm lãnh đạo tại AnyCompany Financial đã nhận được báo cáo về một vụ vi phạm bảo mật mới tại một trong những đối thủ cạnh tranh lớn nhất của mình. Công ty muốn đảm bảo rằng mình đã sẵn sàng phát hiện và ứng phó với mọi sự cố bảo mật trong tương lai. Giám đốc CNTT đã yêu cầu bạn triển khai giải pháp giám sát và ghi nhật ký để phát hiện các sự cố bảo mật để công ty có thể ứng phó kịp thời.

Giải pháp cần thực hiện những điều sau:

Theo dõi tất cả các lệnh gọi API đến thùng S3.

Giám sát nhật ký ứng dụng.

Thông báo cho các thành viên trong nhóm trong trường hợp xảy ra sự cố bảo mật.

Giám sát cấu hình tài nguyên AWS và tự động sửa đổi các cấu hình không tuân thủ.

Bảng sau đây mô tả các tác vụ mà bạn sẽ triển khai trong giai đoạn này.

**Chi tiết tác vụ được đánh số**

1 Tạo một dấu vết trong AWS CloudTrail để ghi lại các lệnh gọi API của Amazon S3.

2 Cấu hình Nhật ký CloudWatch để giám sát nhật ký xác thực của phiên bản WebServer.

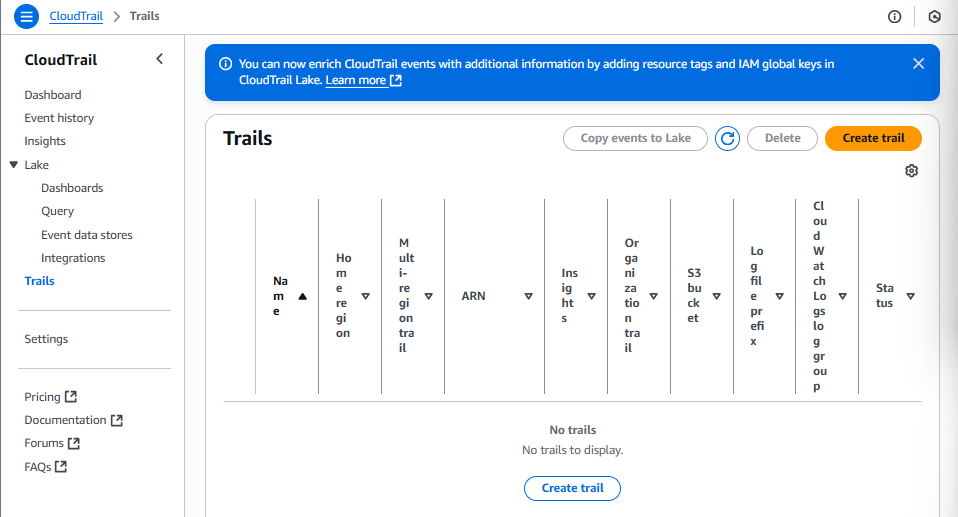
3 Tạo báo động CloudWatch để thông báo cho các thành viên trong nhóm khi có nỗ lực truy cập vào phiên bản WebServer.

4 Sử dụng AWS Config để đảm bảo rằng các thùng S3 đã bật ghi nhật ký đối tượng khi chúng được tạo.

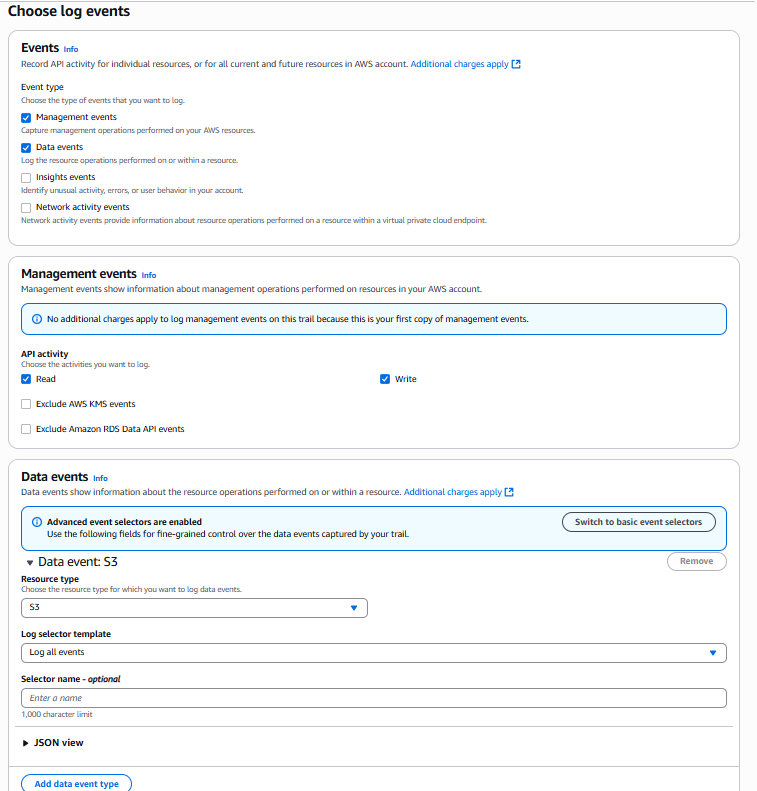
## **Nhiệm vụ 4.1: Sử dụng CloudTrail để ghi lại các cuộc gọi API của Amazon S3**

### **Bước 1: Tạo CloudTrail Trail**

1. Vào **AWS CloudTrail Console**.
2. Ở góc trái, nhấn nút **menu (☰)** → chọn **Trails** → **Create trail** (❗ **Không nhấn “Create trail” trên trang chính**, vì nó sẽ đưa bạn đến chế độ "Quick trail" không phù hợp).



1. Cấu hình trail như sau:
   * **Trail name:** data-bucket-reads-writes
   * **Storage location:** chọn **bucket S3 có sẵn là cloudtrail-logs**
   * **Log file SSM-KMS encryption:** bỏ chọn **Enabled**
   * **Additional settings ->** bỏ tích ở tất cả
   * **Event logging:**
     + Bật **Management events**
     + Bật **Data events**
       - Chọn **S3** → **Log all current and future buckets**



Next->

### **Bước 2: Tạo file CSV để test**

1. Trên máy tính, tạo file tên: **customer-data.csv**
2. Dán nội dung sau vào file và lưu lại:

***CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone***

***1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MD,301-555-0158***

***2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163***

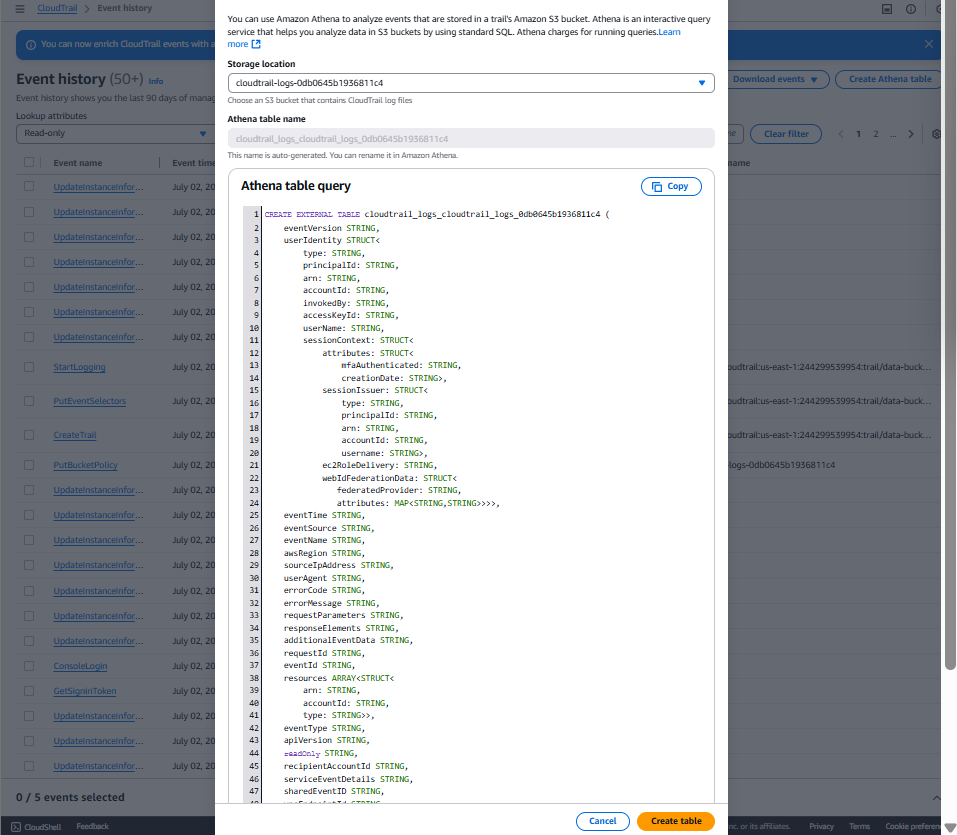
***3,John,Stiles,9/20/2016,1980 8th St.,Nowhere,NY,914-555-0122***

***4,Li,Juan,6/29/2011,1323 22nd Ave.,Anytown,NY,914-555-0149***

1. Đăng nhập AWS Console → vào **Amazon S3** → chọn bucket tên **data-bucket** → nhấn **Upload** → chọn file customer-data.csv.
2. Sau khi upload, **mở (preview)** file đó trong S3 Console → hành động này sẽ tạo log trong CloudTrail.

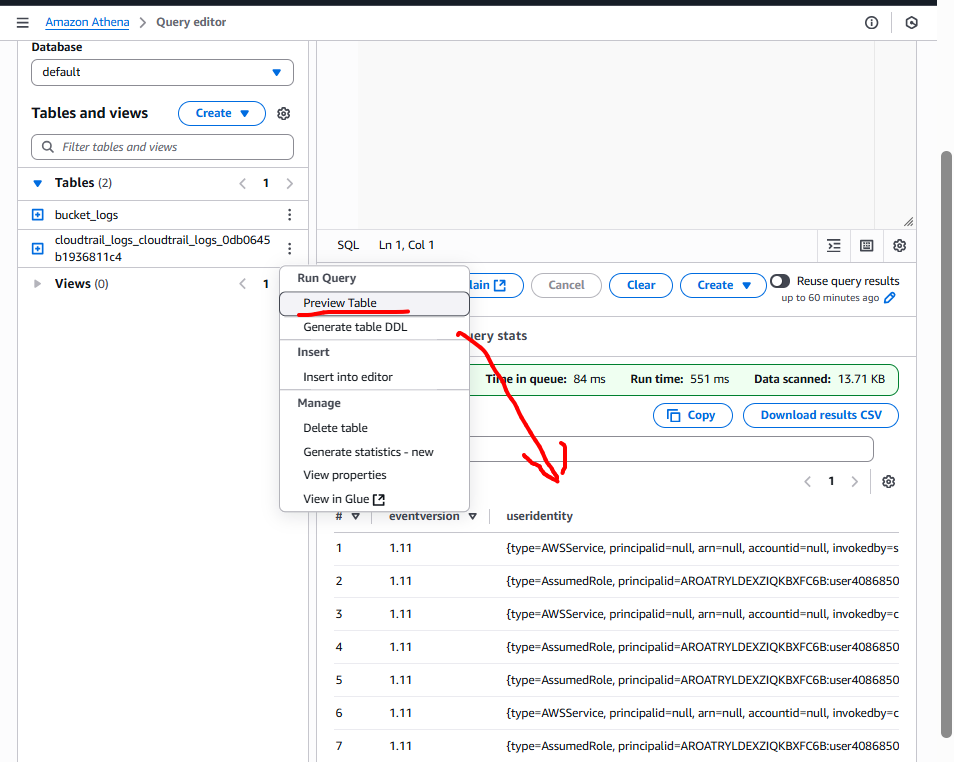
### **Bước 3: Tạo bảng Athena để đọc log từ CloudTrail**

1. Vào **CloudTrail Console** .
2. Ở phần dưới cùng, chọn tab **Event history** → nhấn **Create Athena table**.
3. Cấu hình:
   * **S3 bucket for logs**: cloudtrail-logs
   * Khu vực lưu trữ: chọn cloudtrail-logs
4. Nhấn **Create table** → nó sẽ tạo câu lệnh SQL với CREATE EXTERNAL TABLE trong Athena → **Chạy truy vấn này** để tạo bảng.



### **Bước 4: Truy vấn log upload file với Athena**

1. Vào **Athena Console**
2. Trong phần **Tables**, chọn bảng cloudtrail\_logs → nhấn **Preview table**.
3. Chờ vài phút để dữ liệu được gửi từ CloudTrail (thường ~5 phút).



1. Nếu thấy có kết quả, dán truy vấn dưới đây vào tab mới:

***SELECT eventtime, useridentity.principalid, requestparameters, eventname***

***FROM cloudtrail\_logs***

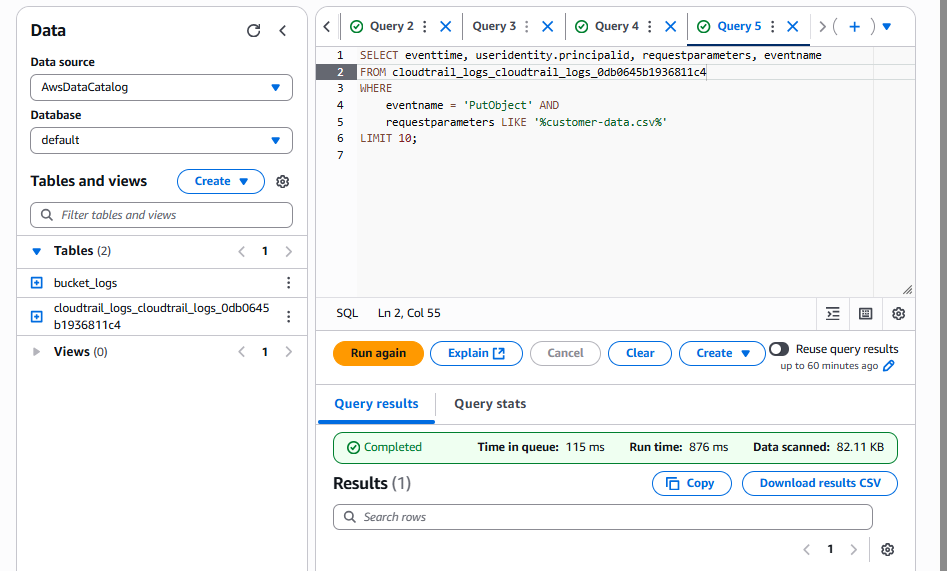
***WHERE***

***eventname = 'PutObject' AND***

***requestparameters LIKE '%customer-data.csv%'***

***LIMIT 10;***

**\*\* Thay cloudtrail\_logs *bằng* cloudtrail\_logs *vừa tạo***

******

📌 **Giải thích:**

* eventname = 'PutObject' → truy tìm hành động upload file.
* requestparameters LIKE '%customer-data.csv%' → lọc các thao tác liên quan đến file bạn upload.

**Challenge cuối cùng: Truy vấn hành động tải/mở file**

👉 Truy vấn để tìm hành động **đọc/tải file** (GetObject), bao gồm:

* **Thời gian**
* **Địa chỉ IP người dùng**
* **Trình duyệt được sử dụng**

***SELECT eventtime, sourceipaddress, useragent, eventname***

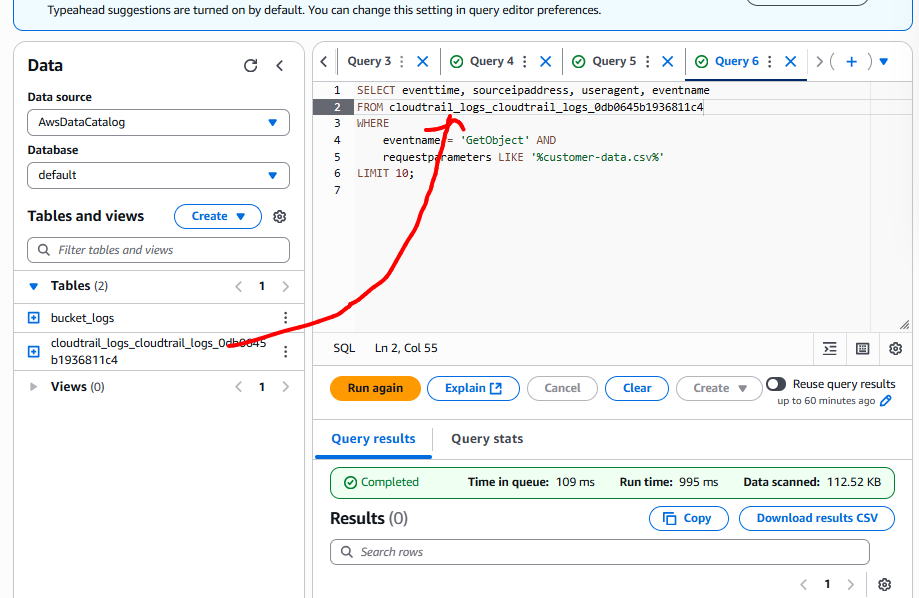
***FROM cloudtrail\_logs***

***WHERE***

***eventname = 'GetObject' AND***

***requestparameters LIKE '%customer-data.csv%'***

***LIMIT 10;***

******

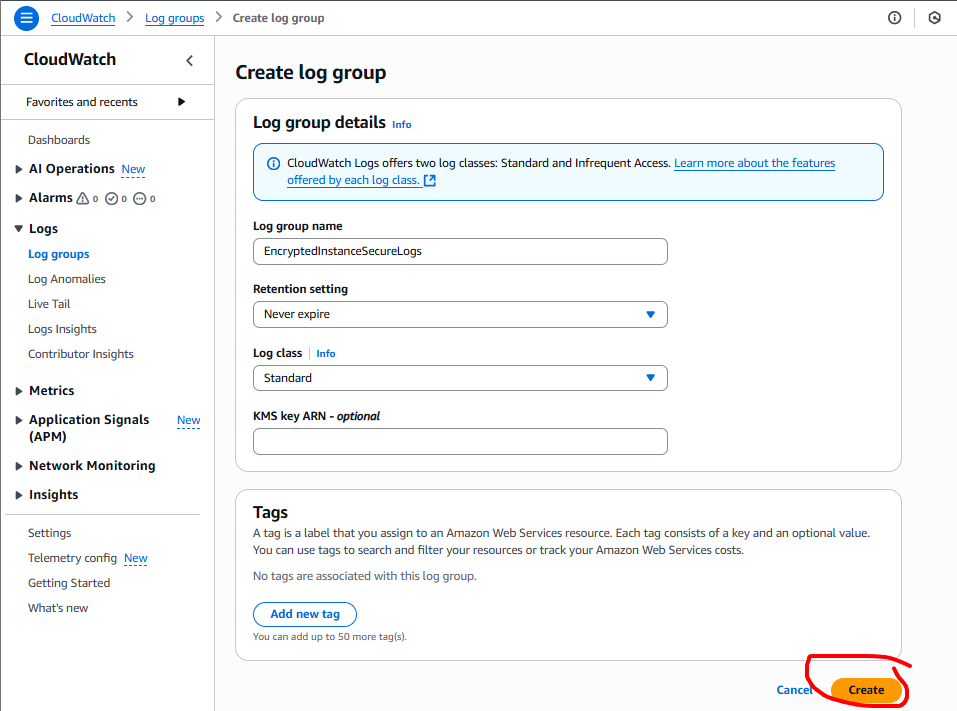
📌 **Giải thích:**

* eventname = 'GetObject': truy cập đọc hoặc tải file từ S3.
* sourceipaddress: địa chỉ IP của người thực hiện.
* useragent: trình duyệt hoặc công cụ được sử dụng (có thể là trình duyệt web, aws-cli, sdk...).

## **Nhiệm vụ 4.2: Sử dụng CloudWatch Logs để theo dõi nhật ký an toàn**

### **Bước 1: Tạo CloudWatch Log Group**

1. Vào **AWS Console**.
2. Mở dịch vụ **CloudWatch > Logs > Log groups**.
3. Tạo mới log group tên: ***EncryptedInstanceSecureLogs***
   * Giữ nguyên các thiết lập mặc định.



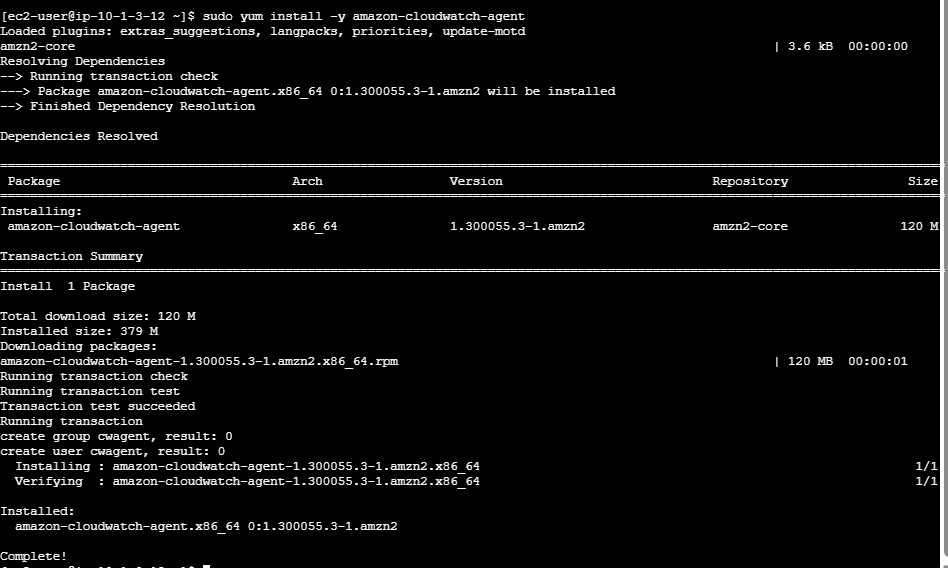
### **Bước 2: Kết nối với EC2 qua EC2 Instance Connect**

1. Vào EC2 Console, chọn instance ***EncryptedInstance***
2. Nhấn nút **Connect > EC2 Instance Connect**, sau đó nhấn **Connect**.

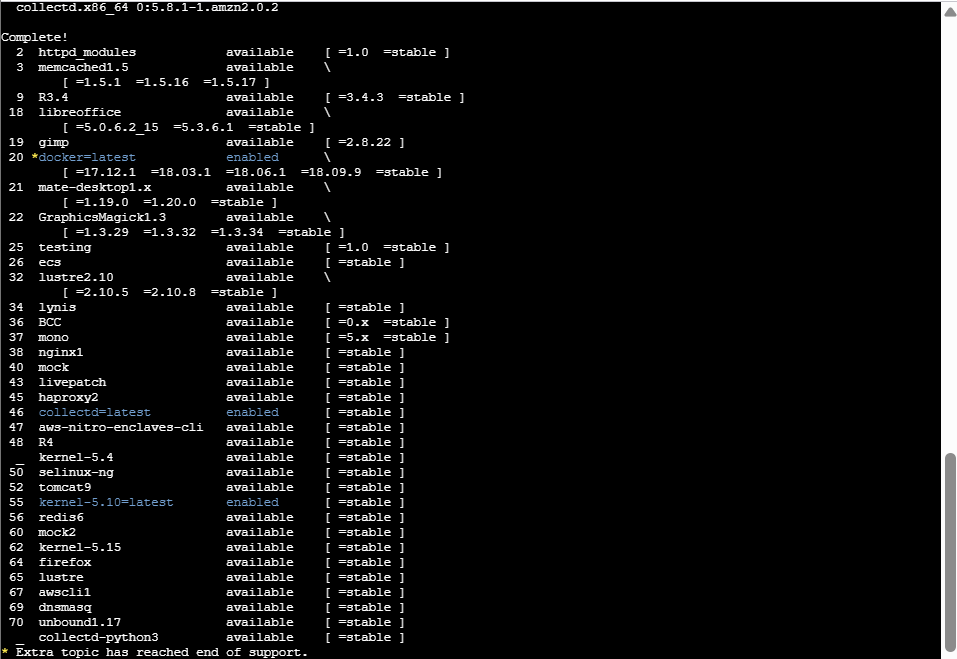
### **Bước 3: Cài đặt CloudWatch Agent và collectd**

Chạy các lệnh sau trong cửa sổ EC2 Instance Connect:

***sudo yum install -y amazon-cloudwatch-agent***

******

***sudo amazon-linux-extras install -y collectd***

******

### **Bước 4: Tải file cấu hình cho CloudWatch Agent**

***sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAP6-91948/capstone-6-security/s3/config.json -P /opt/aws/amazon-cloudwatch-agent/bin/***

******

Hiển thị nội dung file:

***sudo cat /opt/aws/amazon-cloudwatch-agent/bin/config.json***

******

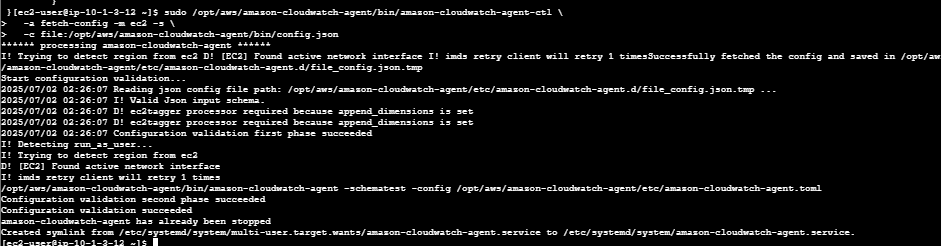
👉 **Phân tích**: File cấu hình này giúp CloudWatch Agent thu thập log từ file /var/log/secure và gửi về EncryptedInstanceSecureLogs.

### **Bước 5: Khởi động CloudWatch Agent**

***sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \***

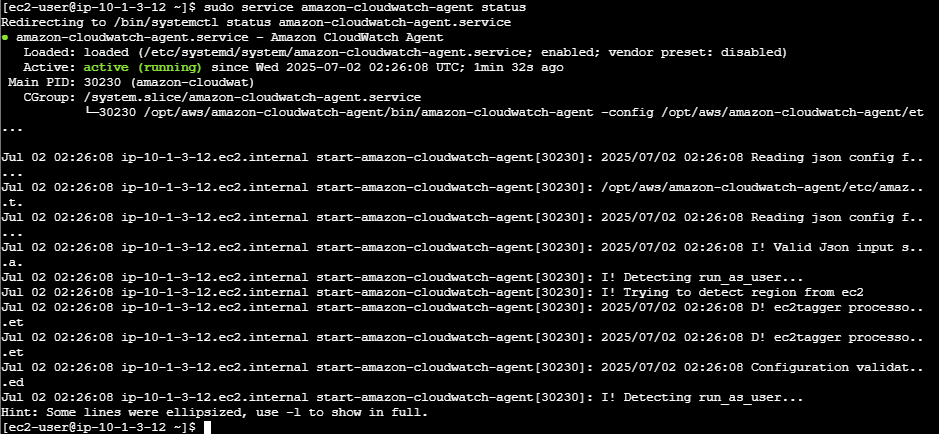
***-a fetch-config -m ec2 -s \***

***-c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json***



Kiểm tra trạng thái:

***sudo service amazon-cloudwatch-agent status***

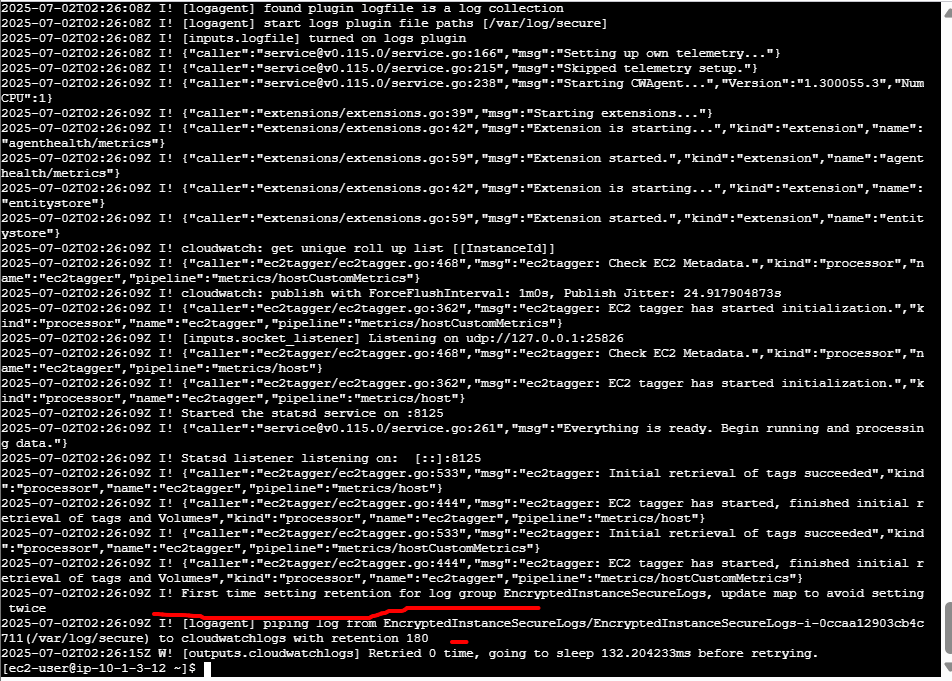


**🔹 Bước 6: Kiểm tra agent có gửi log thành công chưa**

***sudo cat /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log***

Tìm dòng như sau:

[logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-...(/var/log/secure) to cloudwatchlogs...



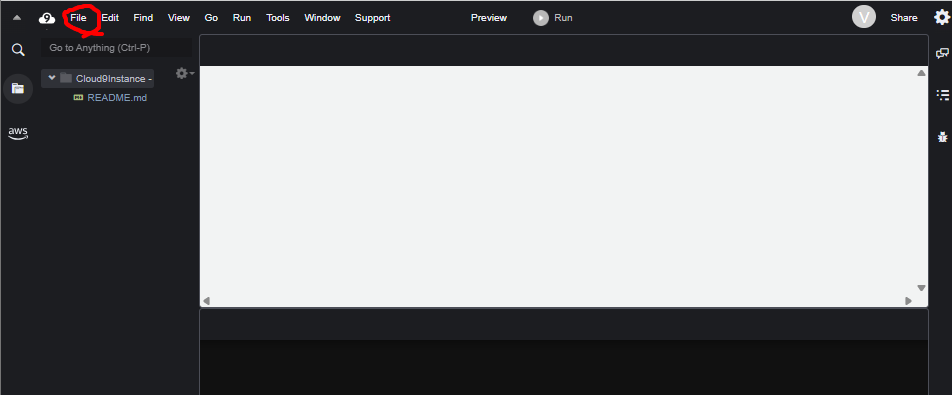
### **Bước 7: Theo dõi trực tiếp file log /var/log/secure**

***sudo tail -f /var/log/secure***

**Giữ cửa sổ EC2 Instance Connect mở để quan sát log ghi lại khi có truy cập SSH.**

### **Bước 8: SSH vào instance từ AWS Cloud9 để tạo log**

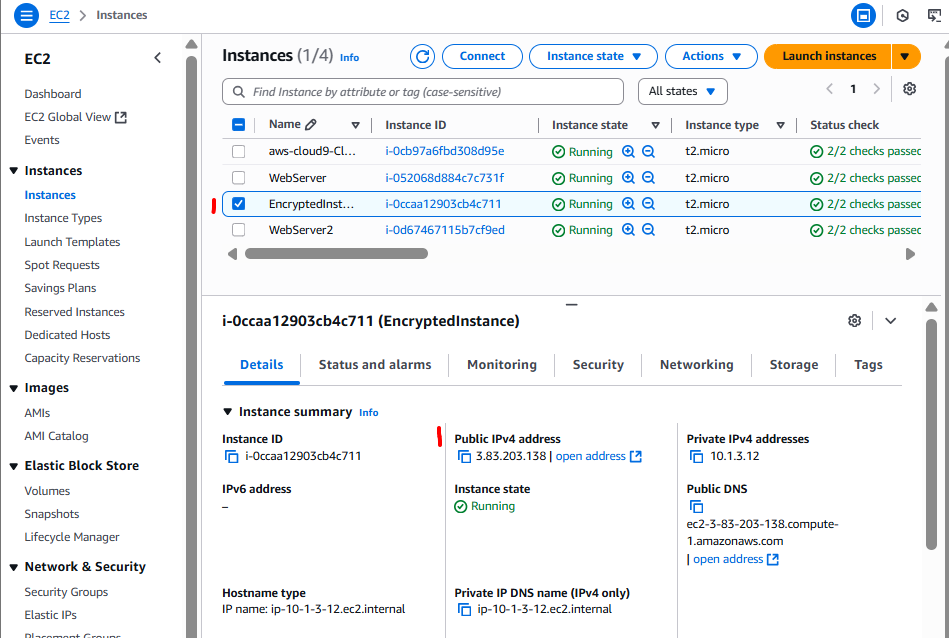
1. Trên máy tính cá nhân, tải về file PEM (labsuser.pem) từ liên kết trong phần hướng dẫn bài lab.
2. Mở **AWS Cloud9 IDE**.
3. Vào **File > Upload Local Files**, tải lên file labsuser.pem.



Sau đó, chạy:

***chmod 400 labsuser.pem***

***ssh -i labsuser.pem ec2-user@<EncryptedInstance-public-IP>***

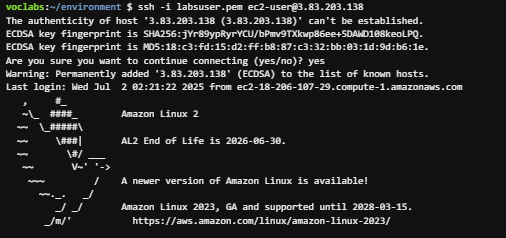


ssh -i labsuser.pem ec2-user@3.83.203.138

✅ Nhập yes khi được hỏi.

🎯 Kết quả:

* Đăng nhập thành công → file /var/log/secure sẽ c như:



### **Bước 9: Đăng nhập thất bại (tạo log failed)**

Trong Cloud9, ngắt kết nối:

***exit***

Thử đăng nhập bằng user sai:

***ssh -i labsuser.pem ubuntu@<EncryptedInstance-public-IP>***

ở đây sẽ là ssh -i labsuser.pem ubuntu@3.83.203.138

❌ Sẽ bị từ chối với lỗi Permission denied.



🎯 Kết quả:

* /var/log/secure ghi lại:

Invalid user ubuntu from ...

### **Bước 10: Kiểm tra log trong CloudWatch**

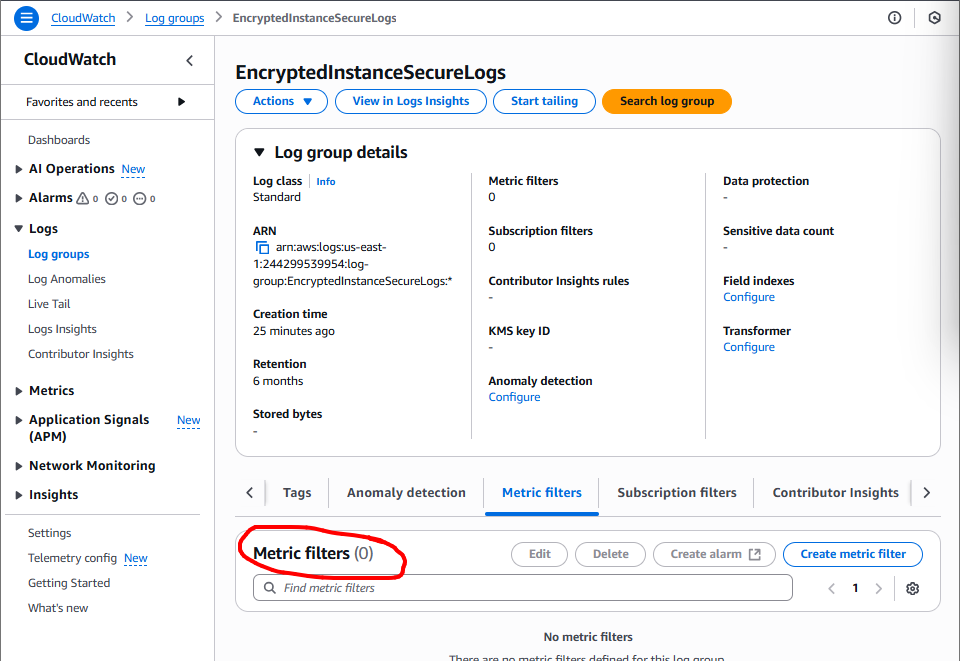
1. Quay lại **AWS Console > CloudWatch > Logs > Log groups**.
2. Chọn log group: EncryptedInstanceSecureLogs.
3. Mở **log stream mới nhất**.
4. Xem các dòng log như:
   * Accepted publickey for ec2-user from ...
   * Invalid user ubuntu from ...

📌 *Lưu ý*: Bạn có thể thấy nhiều dòng failed login khác từ Internet. Đây là hiện tượng phổ biến.

## **Nhiệm vụ 4.3: Tạo báo động CloudWatch để gửi thông báo về các sự cố bảo mật**

### **Bước 1: Tạo Metric Filter cho Log Group**

1. Vào **CloudWatch Console**:  
   Truy cập **Log Groups**, chọn log group có tên:  
   ***EncryptedInstanceSecureLogs***
2. Tạo một **Metric Filter** (Bộ lọc số liệu):

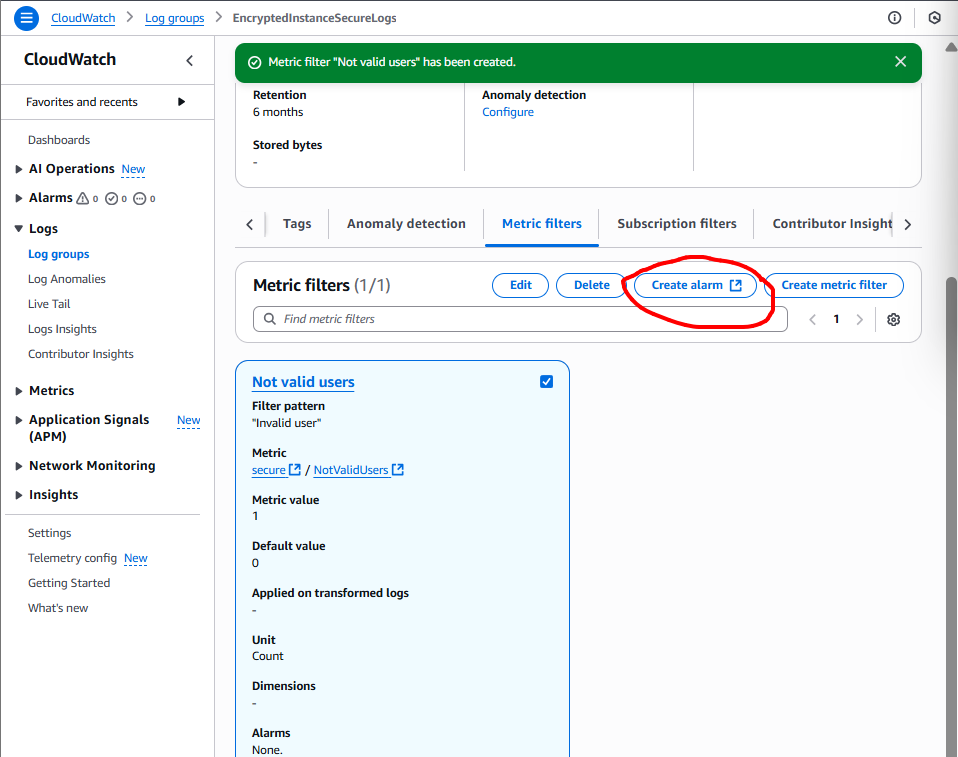


* + **Filter pattern**: ***"Invalid user"*** *(ghi đúng cả dấu ngoặc kép)*
  + **Filter name**: Not valid users
  + **Metric namespace**: secure
  + **Metric name**: NotValidUsers
  + **Metric value**: 1
  + **Default value**: 0
  + **Unit**: Count

📘 **Giải thích**: Filter này sẽ quét log tìm dòng chứa "Invalid user" – tức là đăng nhập SSH sai – và tăng số liệu lên 1 lần mỗi khi phát hiện.

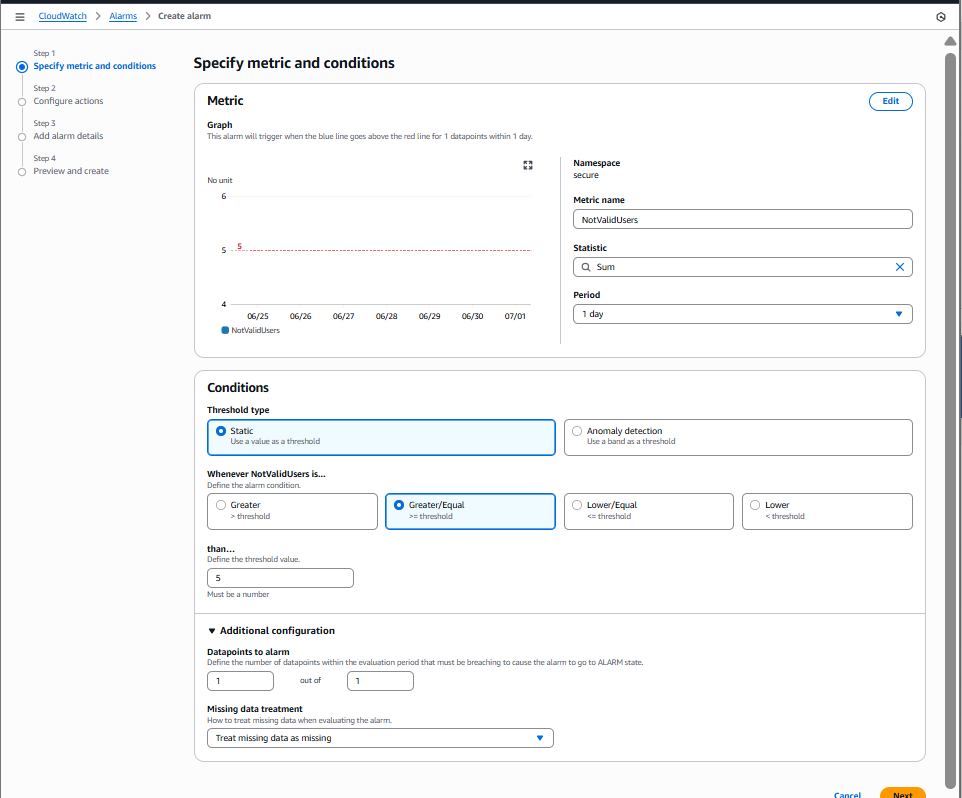
### **Bước 2: Tạo CloudWatch Alarm từ Metric Filter**

1. Trong cùng log group EncryptedInstanceSecureLogs, chuyển sang tab **Metric filters**.
2. Tích chọn filter tên Not valid users.
3. Nhấn **Create Alarm** để tạo cảnh báo mới với cấu hình sau:



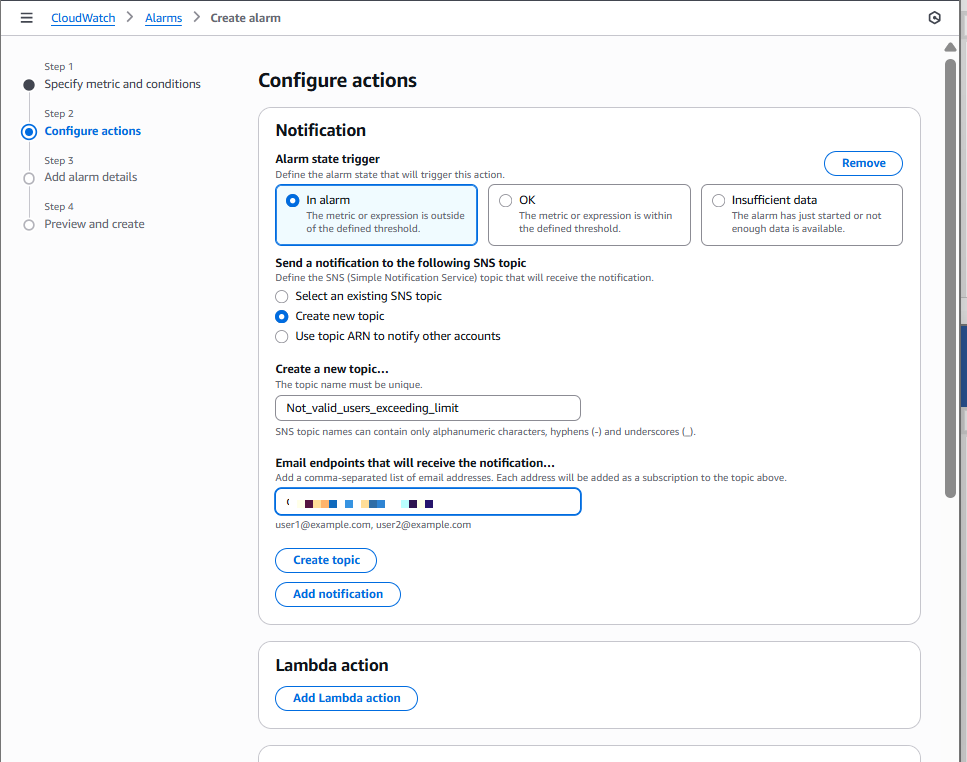
Step 1

* + **Threshold type**: Static
  + **Whenever metric is**: Greater/Equal
  + **Than...**: 5
  + **Period**: 1 day (86400 seconds)
  + Bấm **Next**



Step 2 Create new SNS topic:

* + Topic name: Not\_valid\_users\_exceeding\_limit
  + Email endpoints: Nhập email mà bạn có thể kiểm tra được(nên nhập email cá nhân hoặc Email trường để nhận
  + Ấn create Topic



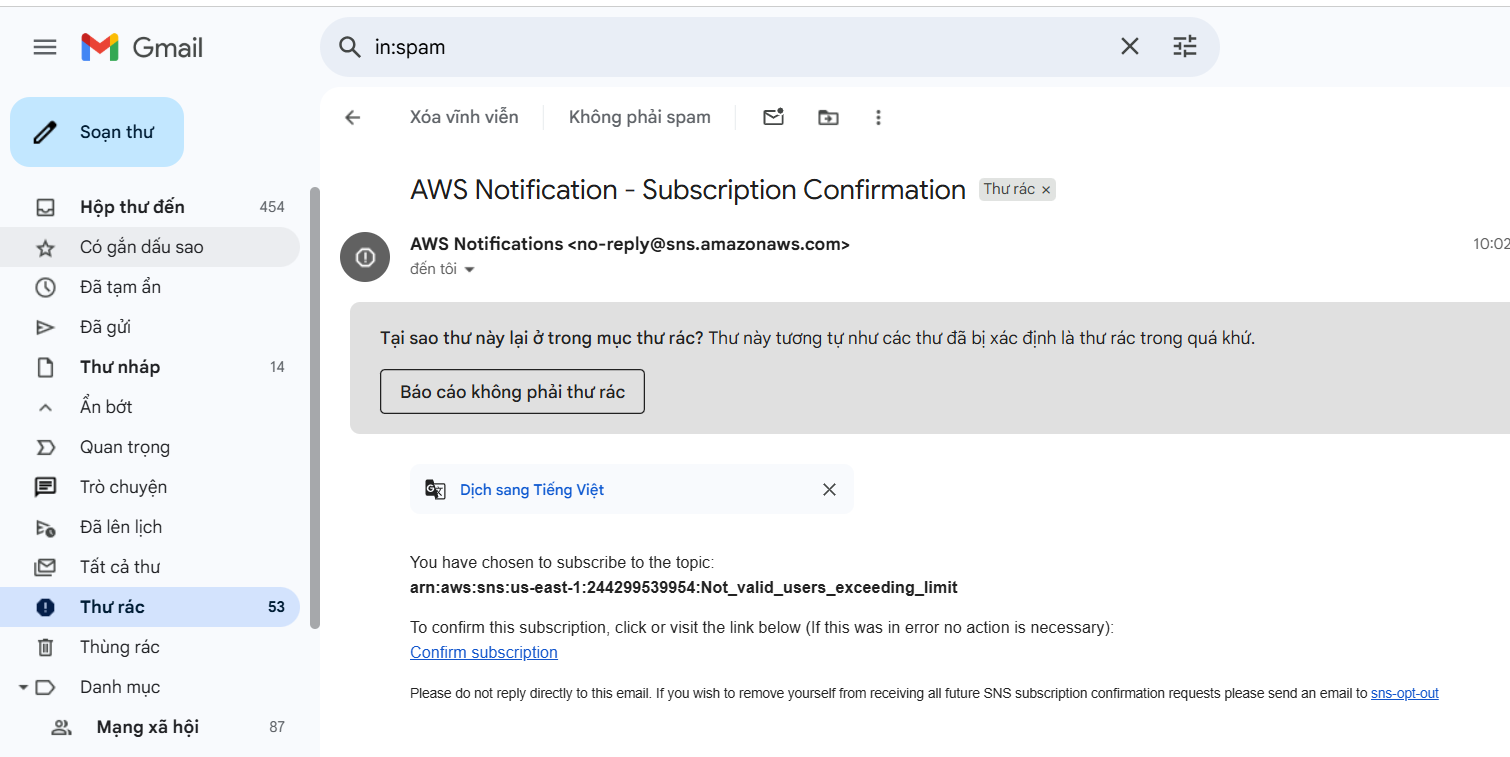
Step 3 **Alarm name**:

* + ***Not valid users exceeding limit on EncryptedInstance***
  + Description : ***Not valid access attempts over SSH to the EncryptedInstance server have exceeded 4 in the last 24 hours***

Step 4 Next và gmail xác nhận

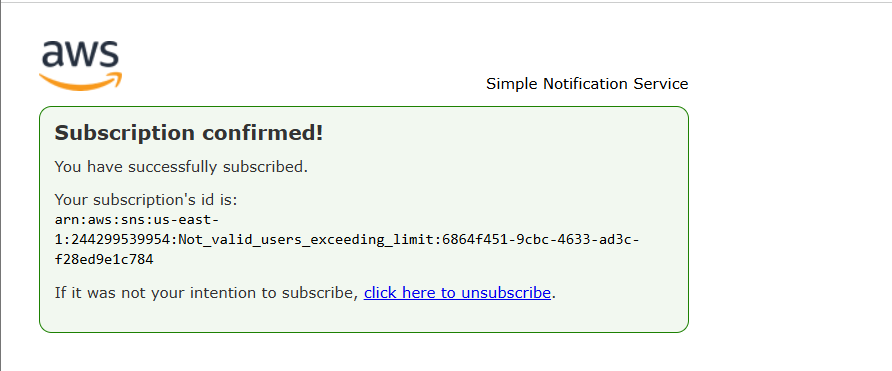
### **Bước 3: Xác nhận email để nhận thông báo từ SNS**

1. Truy cập hộp thư của bạn (email đã nhập ở bước trên).
2. Tìm email từ **AWS Notifications**.



1. Nhấn vào nút **“Confirm subscription”** để kích hoạt nhận thông báo từ SNS.

🛑 **Không xác nhận thì CloudWatch Alarm sẽ KHÔNG gửi thông báo được.**



### **Bước 4: Mô phỏng tấn công SSH sai**

1. Quay lại **Cloud9 IDE**, mở terminal.
2. Thực hiện ít nhất **5 lần thử đăng nhập SSH sai** ( nhiều hơn càng tốt) vào EncryptedInstance (dùng sai user).

Ví dụ lệnh (thay public\_ip bằng IP của EncryptedInstance):

***ssh invaliduser@<EncryptedInstance\_Public\_IP>***

**Ví dụ: 7 lệnh**

**ssh testuser1@3.83.203.138**

**ssh admin123@3.83.203.138**

**ssh ubuntu@3.83.203.138**

**ssh hacker@3.83.203.138**

**ssh fakeuser@3.83.203.138**

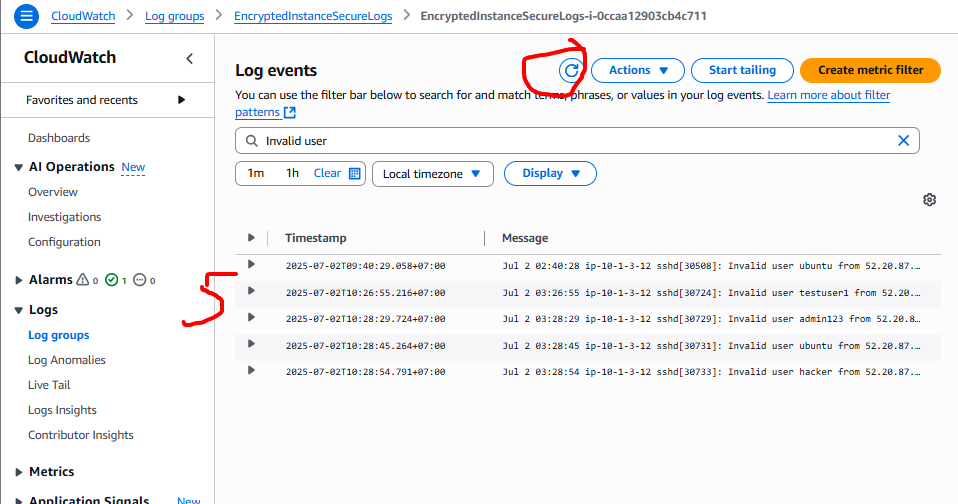
**ssh root123@3.83.203.138**

**ssh guest@3.83.203.138**

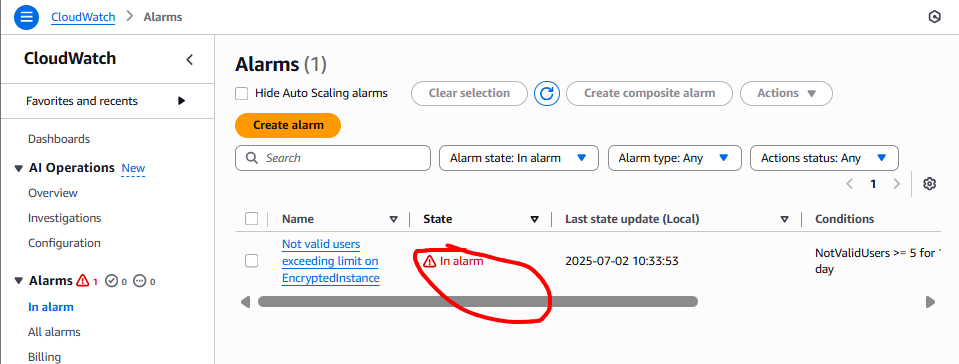
Lặp lại lệnh này ít nhất 5 lần với cùng user sai.

### **Bước 5: Kiểm tra CloudWatch Logs và Alarm**

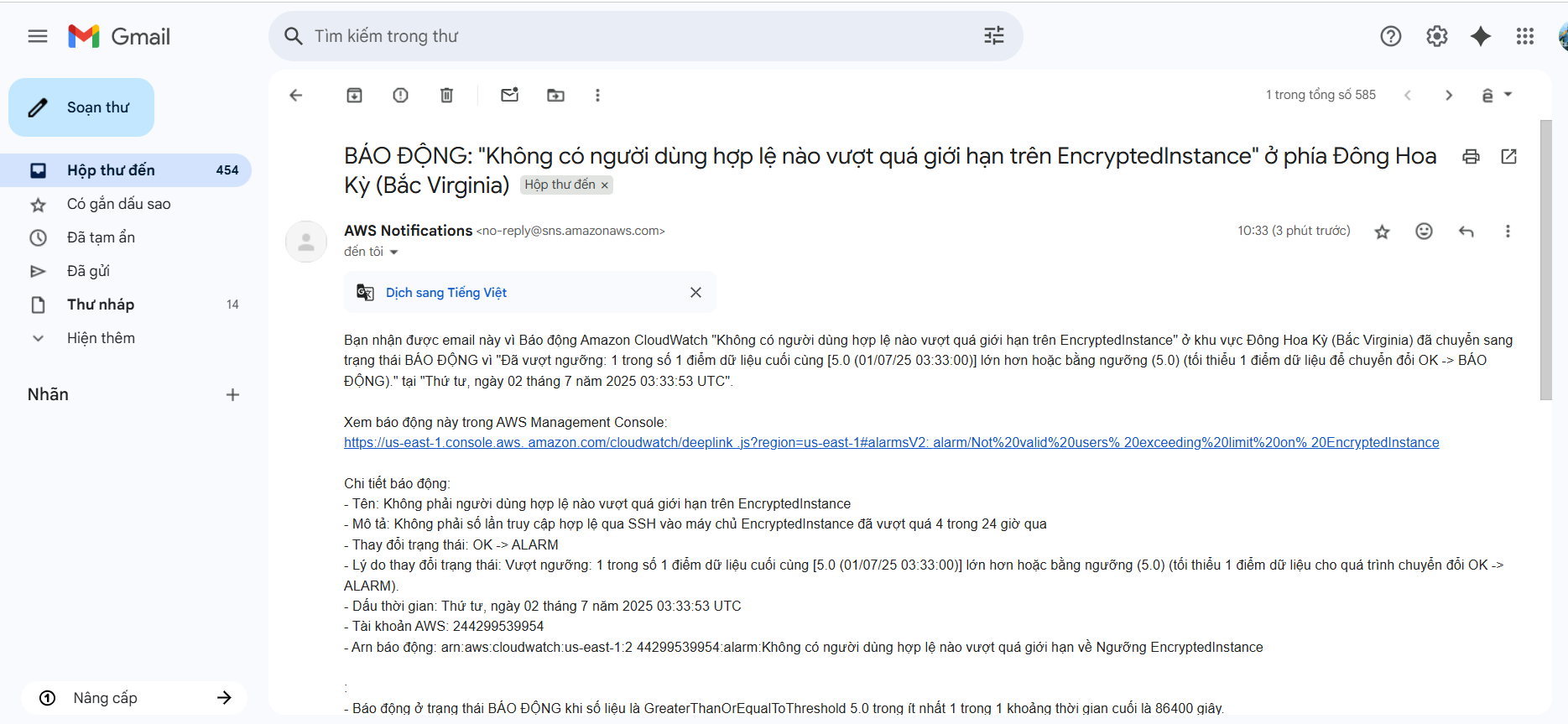
1. Vào lại **CloudWatch Console**, vào EncryptedInstanceSecureLogs.
2. Mở log stream mới nhất, lọc theo từ khóa Invalid user.
3. Đảm bảo có ít nhất **5 log events** trong 24 giờ gần nhất.



🟢 Nếu đủ điều kiện, trạng thái Alarm sẽ chuyển sang **“In Alarm”**.



1. Kiểm tra **hộp thư email** – bạn sẽ thấy một email thông báo rằng ngưỡng cảnh báo đã bị vượt.



## **Nhiệm vụ 4.4: Cấu hình AWS Config để đánh giá cài đặt bảo mật và khắc phục cấu hình tài nguyên AWS**

### **Bước 1: Tạo bucket compliance**

1. Truy cập **Amazon S3 console**.
2. Tạo bucket mới tên là compliance-bucket-<unique-ID> (dùng cùng unique-ID như các bucket khác trong lab).
3. Khu vực (region): us-east-1.
4. Bật **ACLs**: Trong phần cấu hình **Object Ownership**, chọn **ACLs enabled**.

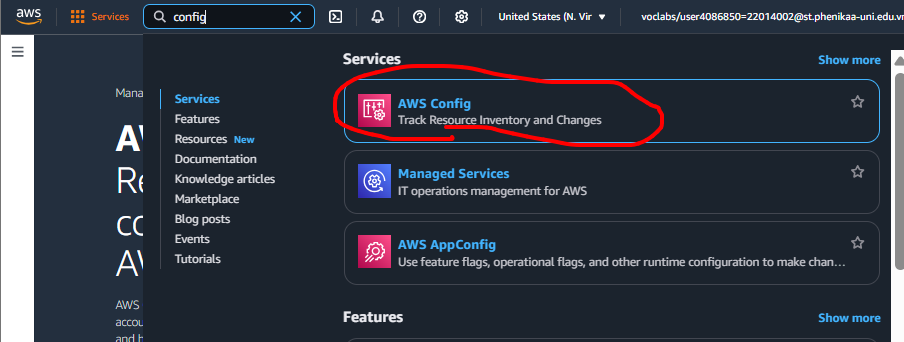
### **Bước 2: Bật ACL cho bucket ghi log**

* Vào **S3 > Buckets > s3-objects-access-log**
* Chuyển sang tab **Permissions**
* Tìm mục **Object Ownership** → Nhấn **Edit**
* Chọn **ACLs enabled**
* Mục **Object Ownership** :
  + Chọn **Bucket owner preferred**

→ **Save changes**

### **Bước 3: Cấu hình AWS Config**

1. Truy cập **AWS Config console** > Nhấn **Get started** trên thanh tìm kiếm

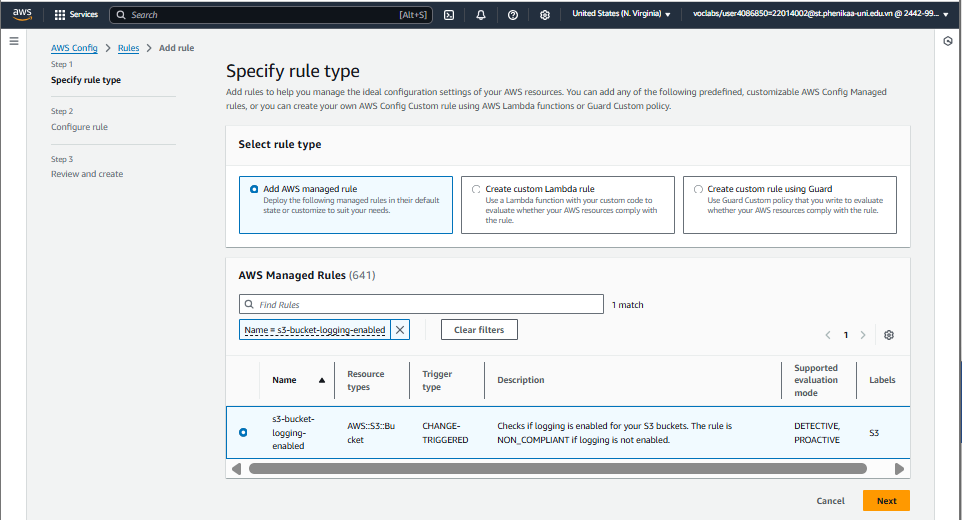


1. Thiết lập như sau:

* Recording strategy: **All resource types with customizable overrides**
* Default settings: **Continuous recording**
* IAM role for AWS Config: **AWSConfigRole**
* Amazon S3 bucket: **Choose a bucket from your account**
* Chọn bucket có dạng ***aws-config-…………***
* Step2: Rules ko phải tick gì cả
* Ấn Confirm

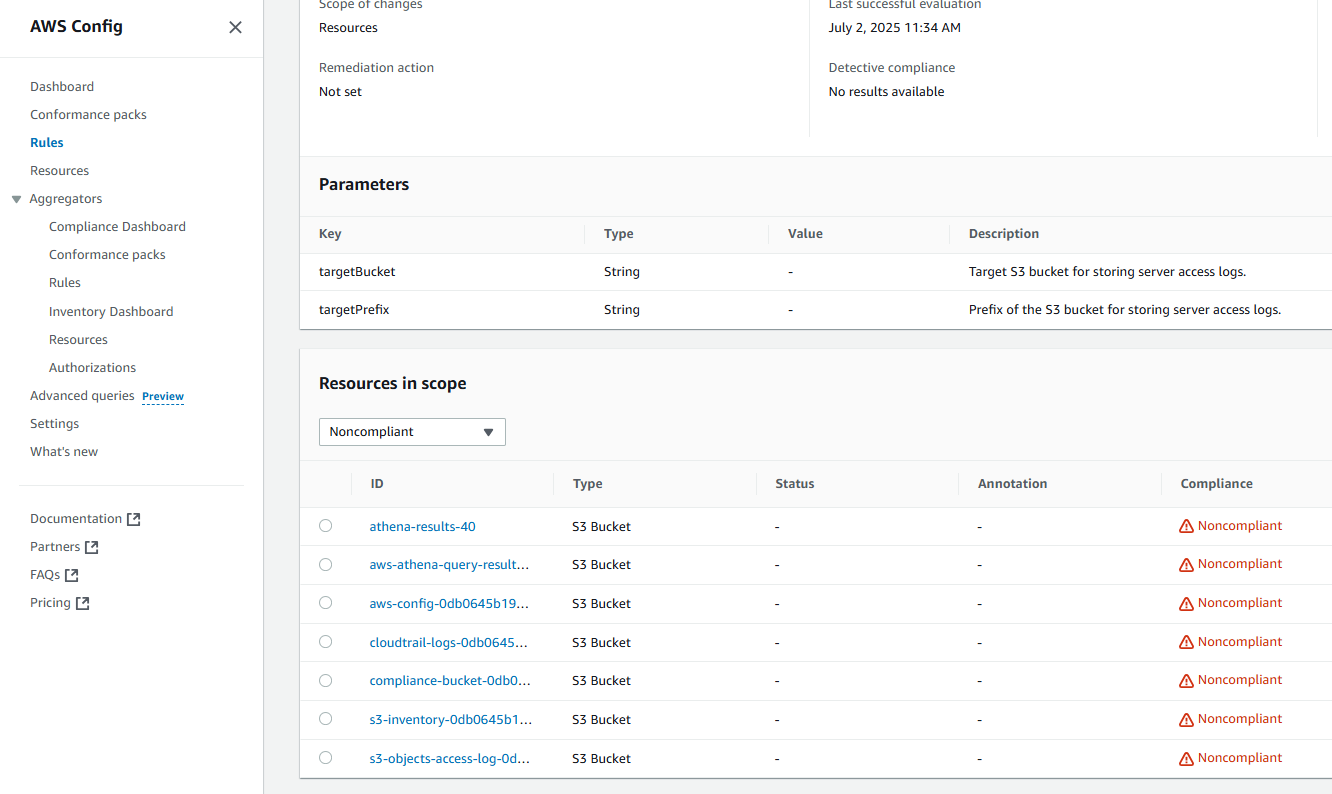
**Bước 4: Thêm rule kiểm tra log S3**

1. Trong AWS Config console, chọn **Rules > Add Rule**.
2. Tìm và chọn rule tên s3-bucket-logging-enabled.
3. Giữ các tùy chọn mặc định > **Add Rule**.

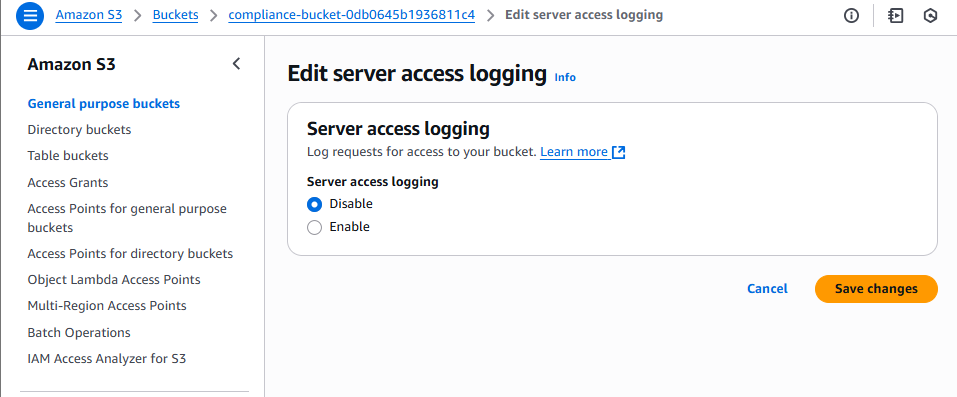


**Bước 5: Kiểm tra compliance**

1. Chờ khoảng vài phút (tối đa 15 phút), vào lại rule s3-bucket-logging-enabled.
2. Kiểm tra phần **Resources in scope**.
3. Bucket compliance-bucket-<unique-ID> sẽ bị đánh dấu **Noncompliant** vì chưa bật server access logging.



* Xác minh bucket compliance-bucket-<uniqueID> bị đánh dấu là **Noncompliant**.
* Trong S3 -> Click ID bucket → [Manage Resource] → tab **Properties** → xác nhận **Server access logging: Disabled**.

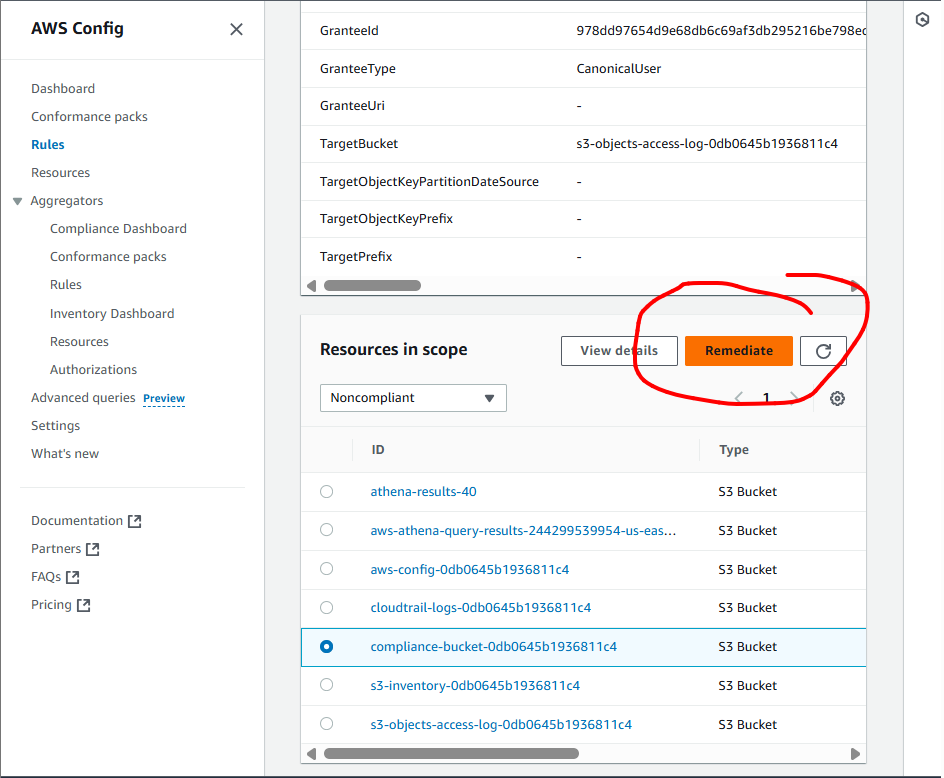


**Bước 6: Cấu hình remediation thủ công**

1. Trong **rule (aws config)** s3-bucket-logging-enabled, chọn **Actions > Manage remediation**.
2. Cấu hình như sau:
   * **Remediation method**: Manual remediation.
   * **Remediation action**: AWS-ConfigureS3BucketLogging.
   * Các tham số:
     + **BucketName**: compliance-bucket-<unique-ID>.
     + **GrantedPermission**: FULL\_CONTROL.
     + **GranteeType**: CanonicalUser.
     + **GranteeId**: (Lấy từ Permissions > ACL của compliance-bucket, là mã Canonical ID của bạn).
     + **TargetBucket**: s3-objects-access-log-<unique-ID>.
     + **AutomationAssumeRole**: ARN của SSMAutomationRole (vào IAM > Roles > SSMAutomationRole > copy ARN).
   * Nhấn **Save changes**.

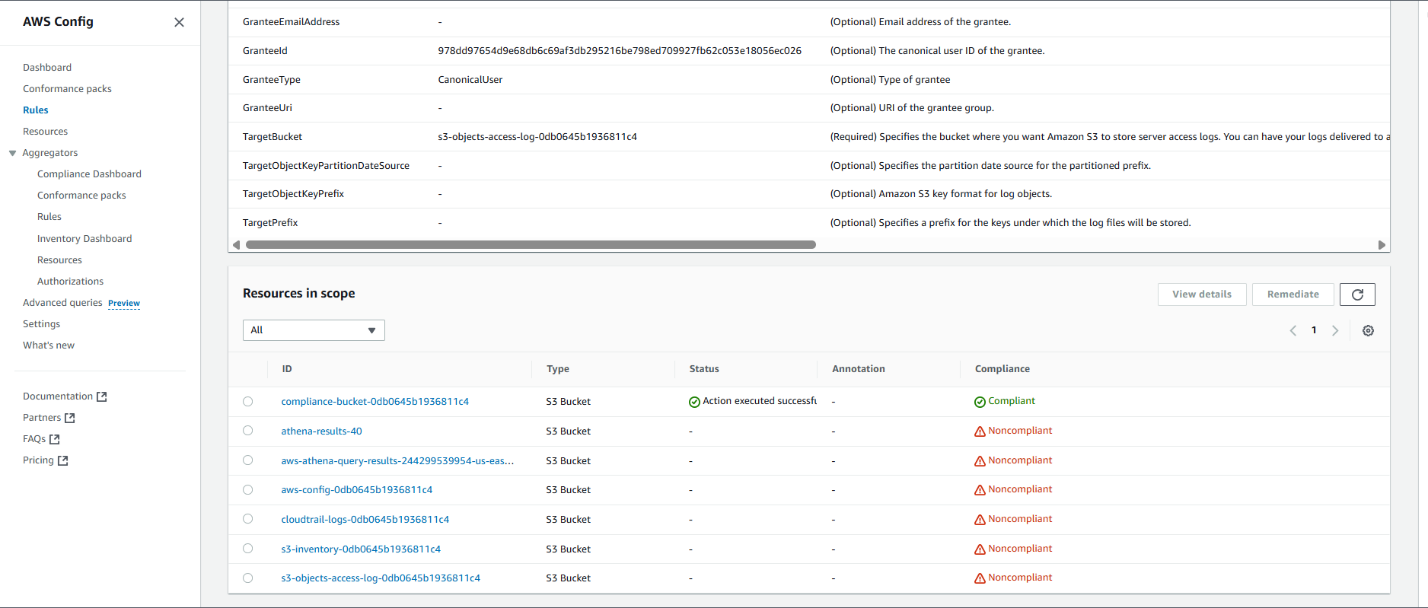
**Bước 7: Thực thi remediation**

1. Trong rule s3-bucket-logging-enabled, ở phần **Resources in scope**, chọn compliance-bucket.
2. Nhấn **Remediate**.



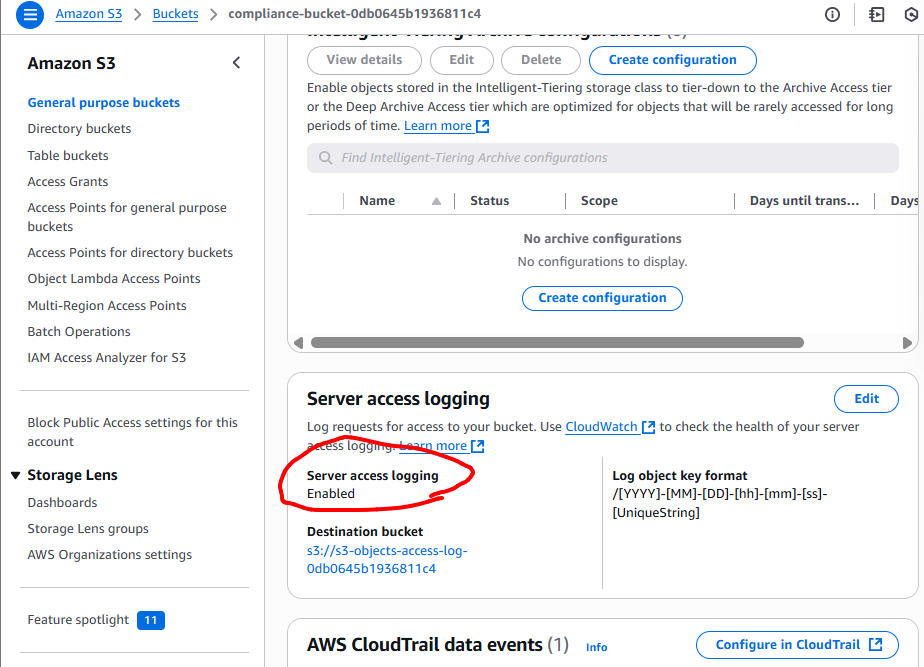
1. Trạng thái chuyển sang “Action execution queued” > Nhấn refresh để theo dõi.
2. Trạng thái sẽ chuyển thành **Action executed successfully**.

🔧 Nếu bị lỗi, vào **Systems Manager > Automation** để xem chi tiết lỗi và cách khắc phục.



**Bước 8: Xác nhận bucket đã bật logging**

1. Vào lại compliance-bucket > Tab **Properties**.
2. Tìm phần **Server access logging** → Bây giờ sẽ thấy **đã bật** nhờ bước remediation trên.



# **Giai đoạn 5: Kết thúc phiên của bạn**

Nhắc nhở: Đây là môi trường phòng thí nghiệm tồn tại lâu dài. Dữ liệu được lưu giữ cho đến khi bạn sử dụng ngân sách được phân bổ hoặc đến ngày kết thúc khóa học (tùy theo điều kiện nào xảy ra trước).

Để giữ nguyên ngân sách khi bạn hoàn thành trong ngày hoặc khi bạn hoàn thành việc làm bài tập trong thời gian hiện tại, hãy thực hiện như sau:

Ở đầu trang này, hãy chọn Kết thúc phòng thí nghiệm, sau đó chọn Có để xác nhận rằng bạn muốn kết thúc phòng thí nghiệm.

Một bảng thông báo cho biết phòng thí nghiệm đang kết thúc.

Lưu ý: Việc chọn Kết thúc phòng thí nghiệm trong môi trường này sẽ không xóa tài nguyên bạn đã tạo. Chúng vẫn ở đó vào lần tiếp theo bạn chọn Bắt đầu phòng thí nghiệm (ví dụ: vào một ngày khác).

Để đóng bảng, hãy chọn Đóng ở góc trên bên phải