# Tự động hóa báo cáo kiểm tra AWS Private CA và cảnh báo hết hạn chứng chỉ

bởi Santosh Vallurupalli và Manthan Raval vào ngày 09 tháng 4 năm 2025 trong [Nâng cao (300),](https://aws.amazon.com/blogs/security/category/learning-levels/advanced-300/" \o "View all posts in Advanced (300)) [Trình quản lý chứng chỉ AWS](https://aws.amazon.com/blogs/security/category/security-identity-compliance/aws-certificate-manager/" \o "View all posts in AWS Certificate Manager), Cơ [quan quản lý chứng chỉ riêng AWS](https://aws.amazon.com/blogs/security/category/security-identity-compliance/aws-private-certificate-authority/" \o "View all posts in AWS Private Certificate Authority), [Bảo mật, Danh tính và Tuân thủ](https://aws.amazon.com/blogs/security/category/security-identity-compliance/" \o "View all posts in Security, Identity, & Compliance), Hướng [dẫn kỹ thuật Nhận](https://aws.amazon.com/blogs/security/category/post-types/technical-how-to/" \o "View all posts in Technical How-to) [xét liên kết](https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/" \l "Comments) [vĩnh viễn](https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/) [Chia sẻ](https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/)

Các tổ chức ngày nay phụ thuộc nhiều vào các kênh liên lạc an toàn và đáng tin cậy và chứng chỉ kỹ thuật số đóng một vai trò quan trọng trong việc bảo mật cơ sở hạ tầng bên trong và bên ngoài bằng cách thiết lập niềm tin và cho phép giao tiếp được mã hóa. Mặc dù chứng chỉ công khai thường được sử dụng để bảo mật các ứng dụng internet, nhưng nhiều tổ chức thích chứng chỉ riêng cho tài nguyên nội bộ để duy trì tính bảo mật và cho phép cấu hình tùy chỉnh mà chứng chỉ công khai không hỗ trợ. [Tổ chức cấp chứng chỉ riêng AWS (AWS Private CA)](https://aws.amazon.com/private-ca" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) cung cấp giải pháp toàn diện để tạo và quản lý hệ thống phân cấp chứng chỉ riêng trong cơ sở hạ tầng khóa công khai (PKI) của tổ chức. AWS xử lý các công việc nặng nhọc về quản lý tổ chức cấp chứng chỉ (CA), cho phép các tổ chức cấp chứng chỉ cho các trường hợp sử dụng khác nhau, bao gồm tạo các kênh giao tiếp được mã hóa, xác thực máy khách và ký mã bằng mật mã. Các chứng chỉ này vẫn được tin cậy trong tổ chức, giúp đảm bảo an ninh nội bộ mà không để lộ chúng trên internet công cộng.

AWS Certificate Manager (ACM) và AWS Private CA cung cấp các công cụ mạnh mẽ để cấp và quản lý chứng chỉ liền mạch trong AWS. Tuy nhiên, khi khối lượng công việc phát triển—bao gồm các vi dịch vụ gốc đám mây, môi trường bộ chứa và triển khai biên lai—cấu hình chứng chỉ mặc định có thể không đáp ứng mọi nhu cầu. Ví dụ: chứng chỉ TLS riêng được yêu cầu bằng ACM đi kèm với thời hạn hiệu lực cố định là 13 tháng, ACM tự động theo dõi và gia hạn. Nhưng điều gì sẽ xảy ra nếu tổ chức của bạn yêu cầu chứng chỉ có thời hạn hiệu lực tùy chỉnh, chẳng hạn như chứng chỉ tồn tại ngắn hạn cho vùng chứa tạm thời hoặc chứng chỉ có thời hạn kéo dài cho hệ thống tại chỗ của bạn? Đây là kịch bản phổ biến đối với các doanh nghiệp sử dụng kiến trúc hiện đại. Bạn có thể đạt được lợi thế đáng kể bằng cách tạo và cập nhật chứng chỉ của mình thông qua [Giao diện dòng lệnh AWS (AWS CLI)](https://aws.amazon.com/cli" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) hoặc [AWS SDK](https://docs.aws.amazon.com/AmazonS3/latest/API/sdk-general-information-section.html" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank). Những công cụ mạnh mẽ này mang lại tính linh hoạt nâng cao và tích hợp liền mạch với quy trình làm việc hiện có.

Nâng cao hiệu quả này hơn nữa, bạn có thể tối ưu hóa việc quản lý chứng chỉ của mình bằng cách bỏ qua Bảng điều khiển quản lý AWS, sử dụng AWS CLI hoặc SDK để tạo chứng chỉ theo chương trình thông qua quy trình PKI tùy chỉnh của họ.

Bạn có thể sử dụng cách tiếp cận thân thiện với tự động hóa này để duy trì toàn quyền kiểm soát vòng đời chứng chỉ của mình, mặc dù cần lưu ý rằng ACM vốn không theo dõi thời hạn của các chứng chỉ được cấp bằng API [acm-pca:IssueCertificate](https://docs.aws.amazon.com/privateca/latest/APIReference/API_IssueCertificate.html" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) và không được yêu cầu bằng ACM. Việc thiếu giám sát về thời hạn chứng chỉ có thể dẫn đến gián đoạn hoạt động và ảnh hưởng đến khả năng truy cập của các ứng dụng của bạn. AWS Private CA cung cấp một tùy chọn mạnh mẽ để giải quyết lỗ hổng này: tùy chọn Tạo báo cáo kiểm tra. Tùy chọn này tạo báo cáo chi tiết về các chứng chỉ do hệ thống phân cấp chứng chỉ của bạn cấp—bao gồm cả ngày hết hạn của chúng—bất kể chúng được tạo như thế nào. Tuy nhiên, với việc các tổ chức quản lý số lượng lớn chứng chỉ trên nhiều hệ thống phân cấp chứng chỉ, việc tạo và xem xét báo cáo thủ công trở nên không thực tế và không bền vững.

Trong bài đăng trên blog này, chúng tôi hướng dẫn bạn quy trình tự động hóa tùy chỉnh khai thác báo cáo kiểm tra AWS Private CA để chủ động theo dõi thời hạn chứng chỉ. Giải pháp này sử dụng [Amazon EventBridge](https://aws.amazon.com/eventbridge" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank), [AWS Lambda](https://aws.amazon.com/lambda" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank), [Amazon Simple Storage Service (Amazon S3),](https://aws.amazon.com/s3/" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) [Amazon Simple Notification Service (Amazon SNS)](https://aws.amazon.com/sns" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) và [AWS Security Hub](https://aws.amazon.com/security-hub" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) để tạo báo cáo hàng ngày, xem xét các chứng chỉ sắp hết hạn, thông báo cho các bên liên quan và tạo kết quả nhật ký để có khả năng hiển thị tập trung. Chúng tôi cũng đã bao gồm một mẫu [AWS CloudFormation](https://aws.amazon.com/cloudformation" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) để triển khai giải pháp này trong môi trường AWS của bạn, hoàn chỉnh với hướng dẫn từng bước. Cách tiếp cận này có thể giúp đảm bảo rằng bạn luôn trước khi hết hạn chứng chỉ.

## Thách thức: Quản lý chứng chỉ vượt ra ngoài mặc định

Để hiểu tại sao giải pháp này lại quan trọng, chúng ta hãy khám phá nhu cầu quản lý chứng chỉ ngày càng phát triển.

Các chứng chỉ được yêu cầu bằng ACM được cấp bởi CA riêng của bạn thông qua bảng điều khiển mặc định là thời hạn hiệu lực 13 tháng; một nền tảng trung gian hợp lý cho nhiều khối lượng công việc. ACM theo dõi các chứng chỉ này, giám sát thời hạn của chúng và thậm chí tự động hóa việc gia hạn. Cách tiếp cận không cần thực hiện này hoạt động tốt cho các ứng dụng đám mây tiêu chuẩn, nhưng môi trường CNTT hiện đại hiếm khi đạt tiêu chuẩn vì các yêu cầu đa dạng của các trường hợp sử dụng trong thế giới thực.

Hãy xem xét các ví dụ thực tế sau:

* **Chứng chỉ tồn tại ngắn:** trong môi trường container chạy trên EKS hoặc [Amazon Elastic Container Service (Amazon ECS),](https://aws.amazon.com/eks" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) chứng chỉ có thời hạn hiệu lực là vài giờ hoặc vài ngày ngày càng phổ biến. Các lưới dịch vụ như [Istio](https://istio.io/latest/about/service-mesh/" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) hoặc [Linkerd](https://linkerd.io/" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) dựa vào các chứng chỉ tồn tại trong thời gian ngắn để bảo mật giao tiếp giữa các pod, giảm bề mặt mối đe dọa nếu khóa bị xâm phạm. Chứng chỉ 13 tháng có thể không tối ưu cho trường hợp sử dụng này.
* **Chứng chỉ tồn tại lâu dài:** Mặt khác, một số khối lượng công việc — thường được tìm thấy trong môi trường truyền thống hoặc hạn chế tài nguyên — được hưởng lợi từ các chứng chỉ có thời hạn hiệu lực kéo dài. Ví dụ: các hệ thống được triển khai ở các vị trí có quyền truy cập mạng không đáng tin cậy hoặc bị hạn chế có thể yêu cầu chứng chỉ có tuổi thọ cao hơn để giảm thiểu những thách thức của việc gia hạn thường xuyên, điều này có thể làm gián đoạn hoạt động hoặc yêu cầu can thiệp thủ công. Tương tự như vậy, cơ sở hạ tầng chạy các ứng dụng quan trọng với tự động hóa tối thiểu có thể nghiêng về chứng chỉ nhiều năm để giảm gánh nặng quản trị và duy trì bảo mật nhất quán theo thời gian. Trong những trường hợp như vậy, chứng chỉ có tuổi thọ cao cung cấp một giải pháp đáng tin cậy, cân bằng nhu cầu bảo mật với sự đơn giản trong hoạt động và giảm thiểu tần suất các tác vụ bảo trì.

Để giải quyết những nhu cầu này, nhiều tổ chức chuyển sang quy trình tích hợp và phân phối liên tục (CI/CD) của riêng họ và tự động hóa tùy chỉnh bằng cách sử dụng AWS Private CA và ACM. Sử dụng AWS CLI hoặc SDK, bạn có thể sử dụng AWS Private CA để cấp chứng chỉ có thời hạn hiệu lực tùy chỉnh phù hợp với yêu cầu khối lượng công việc của chúng.

## Mở rộng giám sát chứng chỉ ngoài các dịch vụ tích hợp ACM

Ngay cả khi chứng chỉ không được yêu cầu bằng ACM, bạn có thể tùy chọn nhập lại chứng chỉ vào ACM. Sau khi các chứng chỉ đã được nhập, ACM bắt đầu theo dõi và giám sát chúng. Tuy nhiên, bạn có thể linh hoạt quyết định nhập chứng chỉ nào. Các chứng chỉ không được nhập vào ACM sẽ không được dịch vụ theo dõi. Các chứng chỉ này sẽ không xuất hiện trong bảng điều khiển ACM, các sự kiện hết hạn của chúng sẽ không kích hoạt [Amazon CloudWatch Logs](https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/Welcome.html" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) và ACM không hỗ trợ việc gia hạn được quản lý của các chứng chỉ này.

Nếu không có chế độ xem tập trung, bạn phải theo dõi ngày hết hạn theo cách thủ công, một tác vụ nhanh chóng trở nên không thể quản lý được khi khối lượng chứng chỉ tăng lên. Chứng chỉ hết hạn có thể dẫn đến thời gian ngừng hoạt động (ví dụ: cân bằng tải từ chối lưu lượng truy cập). Đây là lúc khả năng tạo báo cáo kiểm tra từ AWS Private CA có thể giúp bạn. Nó cung cấp danh sách đầy đủ tất cả các chứng chỉ do CA của bạn cấp, bao gồm số sê-ri, ngày cấp và ngày hết hạn. Tuy nhiên, việc tạo báo cáo này theo cách thủ công bằng bảng điều khiển và xem lại báo cáo hàng ngày không thể mở rộng.

Trong phần sau, chúng tôi hướng dẫn bạn cách thiết lập một giải pháp tự động, có thể mở rộng hơn sẽ thông báo cho bạn khi cần gia hạn chứng chỉ.

## Điều kiện tiên quyết

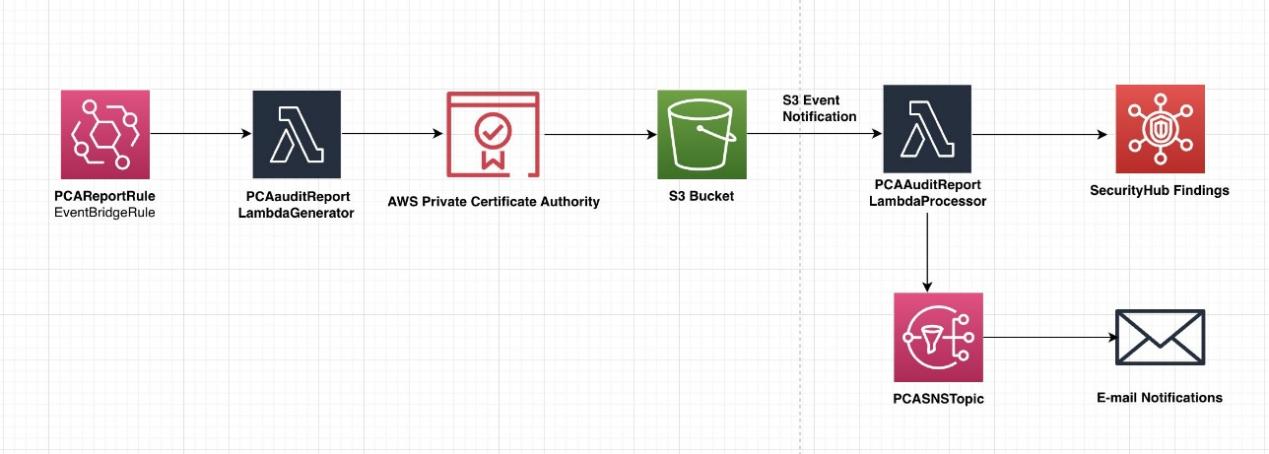
Đối với hướng dẫn này, bạn cần có những điều sau:

* Tài khoản AWS
* CA riêng từ AWS Private CA
* Chứng chỉ được tạo bên ngoài được nhập vào ACM

## Tổng quan về giải pháp

Giải pháp tạo kiểm tra này cung cấp một cách tiếp cận tự động, có thể mở rộng và tích hợp để tạo và phân tích báo cáo kiểm tra cho các chứng chỉ do AWS Private CA cấp. Nó sử dụng các dịch vụ AWS để giám sát trạng thái chứng chỉ, phát hiện sắp hết hạn và thông báo cho quản trị viên trong khi tích hợp các phát hiện vào Security Hub để giám sát bảo mật tập trung. Giải pháp giúp đảm bảo nhận thức kịp thời các chứng chỉ hết hạn; tăng cường tuân thủ và bảo mật hoạt động.

Hình sau đây cho thấy kiến trúc giải pháp. Quá trình bắt đầu với quy tắc EventBridge () kích hoạt tạo báo cáo kiểm tra theo lịch trình do người dùng xác định (ví dụ: hàng ngày). Quy tắc này gọi hàm đầu tiên trong số hai hàm Lambda: . Chức năng này tương tác với AWS boto3 SDK để tạo báo cáo kiểm tra, nắm bắt chi tiết về các chứng chỉ đã cấp. Báo cáo được định dạng dưới dạng tệp CSV (với hỗ trợ JSON tùy chọn có thể định cấu hình trong hàm Lambda) và được lưu trữ trong vùng lưu trữ S3 được chỉ định. Để mô phỏng cảnh báo hết hạn cho mục đích trình diễn, chứng chỉ có thể được cấp với thời hạn hiệu lực dưới 30 ngày, trái ngược với hiệu lực mặc định 13 tháng của chứng chỉ AWS Private CA.PCAReportRulePCAauditReportLambdaGenerator



*Hình 1: Kiến trúc giải pháp*

Sau khi báo cáo kiểm tra được tải lên vùng lưu trữ S3, thông báo sự kiện sẽ kích hoạt hàm Lambda thứ hai, . Chức năng này tải xuống báo cáo gần đây nhất, phân tích cú pháp dữ liệu trong tệp CSV và phân tích chi tiết để xác định các chứng chỉ sắp hết hạn trong ngưỡng 30 ngày. Khi xác định chứng chỉ sắp hết hạn, chức năng sẽ gửi thông báo tổng hợp bằng chủ đề Amazon SNS , hỗ trợ đăng ký như email hoặc hàng đợi [Amazon Simple Queue Service (Amazon SQS)](https://aws.amazon.com/sqs" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank) tùy chọn để xử lý thêm. Đồng thời, chức năng tích hợp các phát hiện vào Security Hub, cung cấp chế độ xem tập trung về các chứng chỉ sắp hết hạn để theo dõi tuân thủ và giám sát bảo mật.S3:PutObjectPCAAuditReportLambdaProcessorPCASNSTopic

Kiến trúc được triển khai bằng cách sử dụng mẫu CloudFormation, tự động hóa việc thiết lập các thành phần cốt lõi — EventBridge, hàm Lambda, vùng lưu trữ S3, chủ đề SNS và tích hợp Security Hub — vào một hệ thống gắn kết. Security Hub đóng vai trò là dịch vụ quản lý tình trạng bảo mật đám mây cung cấp cho các tổ chức cái nhìn tổng hợp về cảnh báo bảo mật và trạng thái tuân thủ trên các tài khoản AWS của bạn. Nó hoạt động như một bảng điều khiển trung tâm, nơi dữ liệu bảo mật từ nhiều nguồn và dịch vụ AWS được tổng hợp, cho phép tự động đánh giá tài nguyên theo các tiêu chuẩn bảo mật đã thiết lập đồng thời giúp các nhóm ưu tiên các mối quan tâm về bảo mật trong toàn bộ môi trường của họ. Thiết kế này giúp đảm bảo khả năng mở rộng, tính linh hoạt và can thiệp thủ công tối thiểu, cho phép người dùng sửa đổi các hàm Lambda để hỗ trợ các định dạng báo cáo bổ sung (chẳng hạn như JSON) hoặc điều chỉnh ngưỡng thông báo theo yêu cầu. Cũng cần lưu ý rằng bạn có thể tạo báo cáo sau mỗi 30 phút.

## Triển khai giải pháp

Với các điều kiện tiên quyết và hiểu biết về kiến trúc, bạn đã sẵn sàng triển khai và kiểm tra quy trình tự động hóa và chạy báo cáo kiểm tra theo yêu cầu.

### Triển khai mẫu CloudFormation

1. Để bắt đầu, hãy sao chép kho lưu trữ GitHub sau.

~ $ curl -O https://aws-security-blog-content.s3.us-east-1.amazonaws.com/public/sample/2526-monitor-private-ca-issued-certificates-aws-private-certificate-authority-eventbridge/ACM-PCA-Monitoring-cfn.yml

~ $ ls

ACM-PCA-Monitoring-cfn.yml

Mẫu CloudFormation bao gồm các thông số sau, cho phép bạn tùy chỉnh triển khai:ACM-PCA-Monitoring-cfn.yml

* **CertificateAuthorityArn**: Tên tài nguyên Amazon (ARN) () của CA riêng có sẵn mà báo cáo kiểm tra được tạo ra.<ARN\_of\_your\_PrivateCA>
* **S3BucketName**: Một vùng lưu trữ S3 mới () nơi báo cáo kiểm tra sẽ được lưu trữ.<Name\_of\_s3\_bucket>
* **EventBridgeRuleName**: Tên của quy tắc EventBridge (<) để kích hoạt hàm Lambda (giá trị mặc định: ).Name\_of\_EventBridgeRule>PCAReportRule
* **CronJobExpression**: Một biểu thức cron () để xác định lịch trình tạo báo cáo (giá trị mặc định: ).<Frequency\_of\_running\_evaluation>cron(0 21 \* \* ? \*)
* **SNSName**: Tên của chủ đề Amazon SNS mới () cho cảnh báo hết hạn (giá trị mặc định: ).<Name\_of\_SNS\_Topic>PCASNSTopic
* **SQSName**: Tên của hàng đợi Amazon SQS mới () cho cảnh báo hết hạn (giá trị mặc định).<Name\_of\_SQS>PCASQS
* **EmailAddress**: Địa chỉ email để nhận thông báo ().<Email\_to\_Receive\_alerts>
* **CertificateExpirationThreshold**: Giá trị ngưỡng tính bằng ngày () để theo dõi thời gian hết hạn của chứng chỉ (giá trị mặc định: 30).<Expiration\_threshold\_in\_days>

1. Chạy lệnh sau để tạo ngăn xếp CloudFormation. Quá trình tạo ngăn xếp sẽ mất 2–3 phút để hoàn tất.

aws cloudformation create-stack \

--stack-name PCAMonitoringWorkflow \

--template-body file://ACM-PCA-Monitoring-cfn.yml \

--capabilities CAPABILITY\_NAMED\_IAM \

--parameters '[

{"ParameterKey": "CertificateAuthorityArn", "ParameterValue": "<ARN\_of\_your\_PrivateCA>"},

{"ParameterKey": "S3BucketName", "ParameterValue": "<Name\_of\_s3\_bucket>"},

{"ParameterKey": "EventBridgeRuleName", "ParameterValue": "<Name\_of\_EventBridgeRule>"},

{"ParameterKey": "CronJobExpression", "ParameterValue": "<Frequency\_of\_running\_evaluation>"},

{"ParameterKey": "SNSName", "ParameterValue": "<Name\_of\_SNS\_Topic>"},

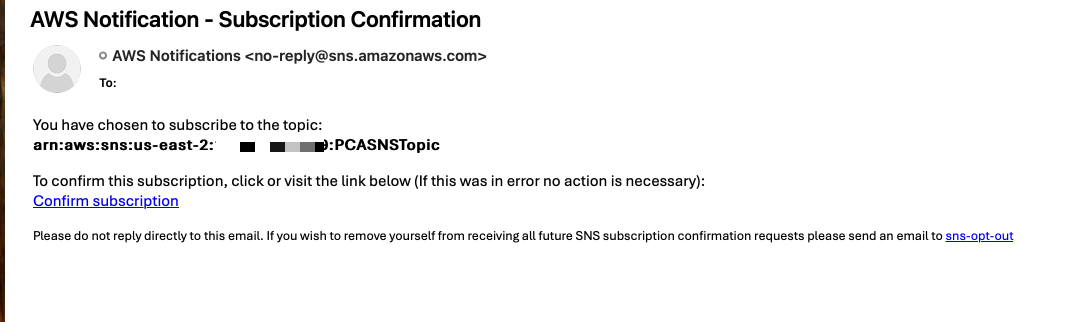
{"ParameterKey": "SQSName", "ParameterValue": "<Name\_of\_SQS>"},

{"ParameterKey": "EmailAddress", "ParameterValue": "<Email\_to\_Receive\_alerts>"},

{"ParameterKey": "CertificateExpirationThreshold", "ParameterValue": "<Expiration\_threshold\_in\_days>"}

]'

1. Khi quá trình tạo ngăn xếp hoàn tất, bạn sẽ nhận được email yêu cầu bạn xác nhận đăng ký chủ đề SNS được chỉ định từ bước trước.



*Hình 2: Mẫu email thông báo do Amazon SNS gửi*

### Kiểm tra quy trình tự động hóa

1. Kiểm tra quy trình tự động hóa bằng cách tạo chứng chỉ riêng sẽ kích hoạt hệ thống cảnh báo hết hạn của bạn. Để thực hiện việc này, bạn sẽ tạo một chứng chỉ riêng bằng cách sử dụng CA riêng của mình với thời gian hết hạn ngắn có chủ ý. Chứng chỉ sẽ hết hạn trước ngưỡng bạn đặt trong mẫu CloudFormation (mặc định là 30 ngày). Ví dụ: nếu bạn giữ ngưỡng mặc định 30 ngày, mã sau sẽ tạo chứng chỉ hết hạn sau 20 ngày, mã này sẽ kích hoạt hệ thống thông báo:

#Generate a Private Key

~ $ % openssl genrsa -out private-key.pem 2048

#List the private key

~ $ % ls

private-key.pem

#Generate a Certificate Signing Request (CSR)

~ $ % openssl req -new -key private-key.pem -out csr.pem -subj "/C=US/ST=Ohio/L=Columbus/O=MyOrg/OU=IT/CN=mydomain.com"

#Issue a Certificate

~ $ % aws acm-pca issue-certificate --certificate-authority-arn <specify\_arn\_of\_PrivateCA> --csr "$(cat csr.pem | base64 | tr -d '\n')" --signing-algorithm "SHA256WITHRSA" --validity Value=20,Type="DAYS"

{

"CertificateArn": "arn:aws:acm-pca:us-east-2:XXXXXX:certificate-authority/7574de75-e5fd-47d0-a4e2-3afc3c0ba4b3/certificate/87980cc7a1cca819dd9082e6cd360c65"

}

#Retrieve the Issued Certificate

~ $ % aws acm-pca get-certificate --certificate-authority-arn <specify\_arn\_of\_PrivateCA> --certificate-arn <specify\_arn\_of\_Certificate\_generated\_above> --output text > certificate.pem

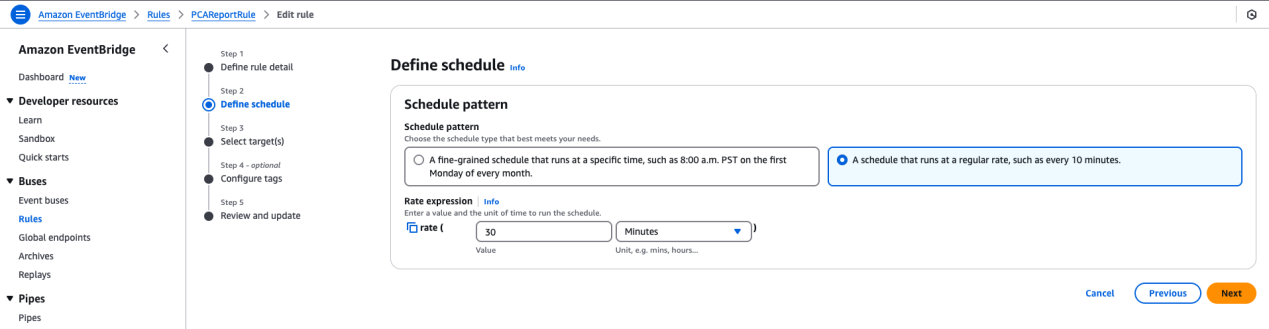
**Lưu ý**: Bạn sẽ nhận được cảnh báo cho tất cả các chứng chỉ sắp hết hạn, ngay cả đối với các chứng chỉ được yêu cầu bằng ACM, hỗ trợ gia hạn có quản lý. Bạn có thể so sánh ARN của chứng chỉ sắp hết hạn với danh sách các chứng chỉ được yêu cầu trong bảng điều khiển ACM hoặc với kết quả của API [acm:ListCertificates](https://docs.aws.amazon.com/acm/latest/APIReference/API_ListCertificates.html" \t "https://aws.amazon.com/blogs/security/automating-aws-private-ca-audit-reports-and-certificate-expiration-alerts/_blank).

Với cơ sở hạ tầng báo cáo kiểm tra được triển khai và chứng chỉ kiểm tra được tạo trong ngưỡng hết hạn của bạn, bước tiếp theo là kích hoạt quy trình tự động hóa để tạo và xử lý báo cáo kiểm tra.

### Chạy báo cáo kiểm tra theo yêu cầu

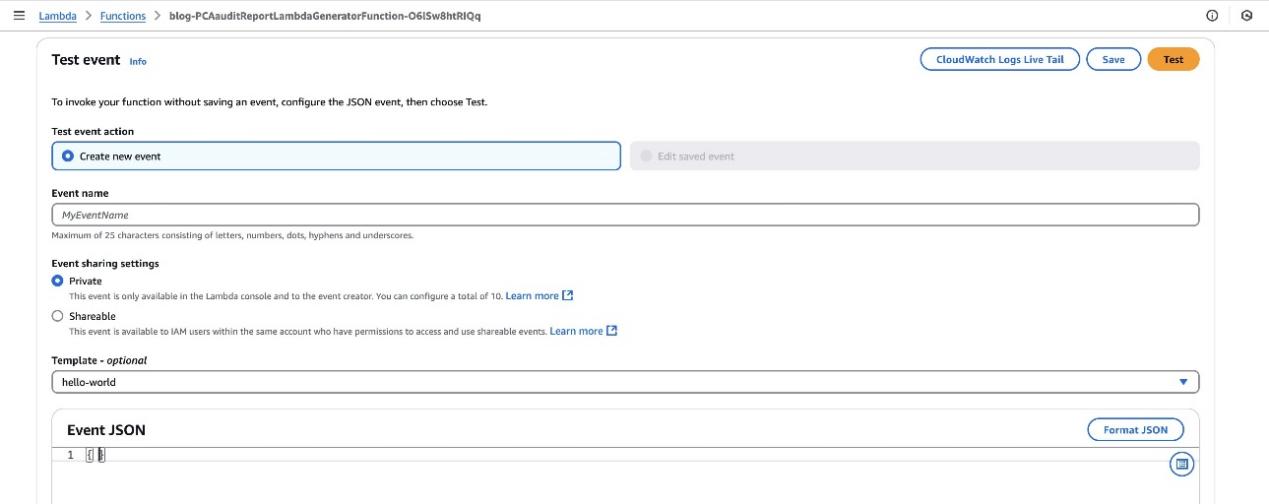
Để kiểm tra quy tắc EventBridge, bạn sẽ tạm thời sửa đổi nó để chạy 30 phút một lần. Khi thử nghiệm xong, bạn có thể hoàn nguyên về lịch trình ban đầu mà bạn đã chỉ định trong các tham số mẫu CloudFormation.PCAReportRule

1. Trong bảng điều khiển Amazon EventBridge, chọn **Quy tắc** trong ngăn điều hướng. Chọn **PCAReportRule** rồi chọn **Chỉnh sửa quy tắc**.
2. Chọn **Xác định lịch trình**.
3. Trong **Mẫu lịch trình**, chọn **Lịch trình chạy với tốc độ thông thường...**
4. Trong **Biểu thức tỷ lệ**, đối với **Giá trị,** nhập 30 và đối với **Đơn vị**, chọn **Phút**.
5. Chọn **Tiếp theo**.



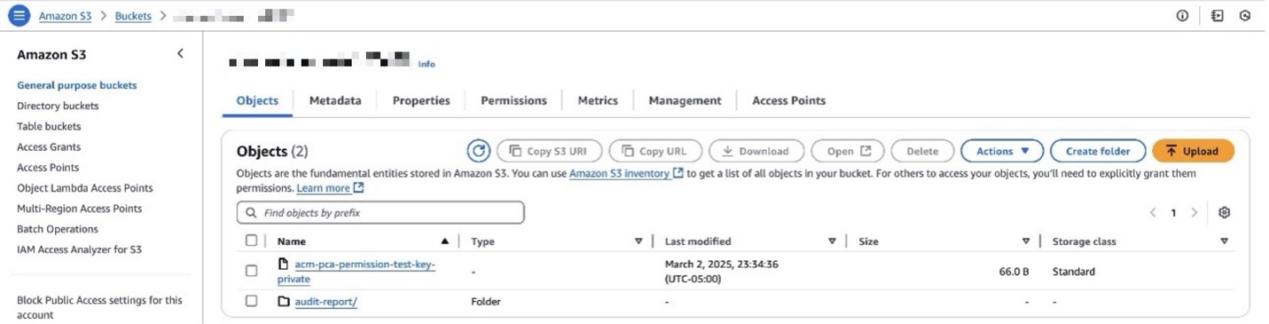
*Hình 3: Chỉnh sửa lịch trình của PCAReportRule cho thử nghiệm*

1. Để kiểm tra ngay lập tức, bạn cũng có thể kích hoạt quy trình làm việc này từ bảng điều khiển Lambda.
2. Trong bảng điều khiển Lambda, chọn **Chức năng** trong ngăn điều hướng, sau đó chọn hàm Lambda.PCAauditReportLambdaGenerator
3. Chọn **tab Kiểm tra,** giữ nguyên giá trị mặc định cho **JSON sự kiện**.
4. Chọn **Kiểm tra ở** đầu cửa sổ.



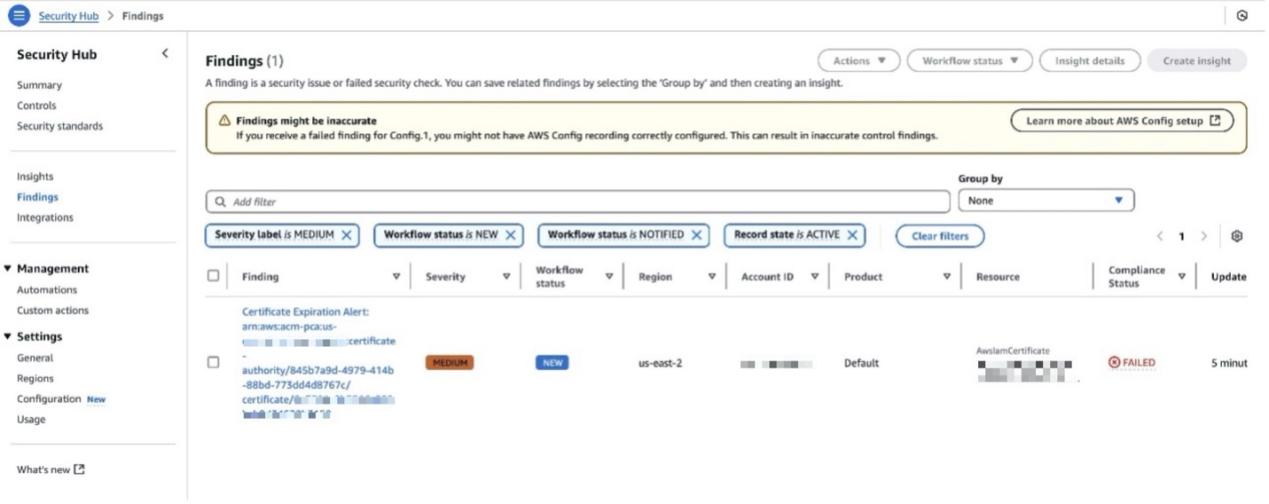
*Hình 4: Sử dụng bảng điều khiển để kích hoạt kiểm tra*

1. Hàm Lambda này tạo báo cáo kiểm tra AWS Private CA và lưu vào vùng lưu trữ S3 được chỉ định ở tiền tố. Để xác minh điều này, hãy điều hướng đến bảng điều khiển Amazon S3 và chọn **Vùng lưu trữ** từ ngăn điều hướng.audit-report
2. Chọn vùng lưu trữ mà bạn đã tạo khi chạy mẫu CloudFormation và xác minh các báo cáo trong thư mục.audit-report



*Hình 5: Báo cáo kiểm toán được lưu vào bucket S3 được chỉ định*

1. Khi báo cáo kiểm tra được tải lên vùng lưu trữ S3, báo cáo sẽ tự động kích hoạt hàm Lambda thông qua thông báo sự kiện S3. Chức năng này phân tích báo cáo kiểm toán để xác định bất kỳ chứng chỉ nào sắp hết hạn. Nếu phát hiện chứng chỉ sẽ hết hạn trong ngưỡng quy định (30 ngày theo mặc định), chức năng sẽ tự động tạo các phát hiện chi tiết trong Security Hub cho mục đích theo dõi và giám sát. Những phát hiện này bao gồm các chi tiết quan trọng như ARN chứng chỉ, ngày hết hạn và mức độ nghiêm trọng.PCAAuditReportLambdaProcessor
2. Vì bạn đã tạo chứng chỉ thử nghiệm hết hạn sau 20 ngày (nằm trong ngưỡng kiểm tra), quy trình tự động hóa sẽ phát hiện điều này và tạo ra các phát hiện tương ứng trong Security Hub. Để xem kết quả, hãy truy cập bảng điều khiển Security Hub và chọn **Kết quả tìm kiếm** trong ngăn điều hướng.



*Hình 6: Xem kết quả báo cáo kiểm tra trong Security Hub*

1. Sau khi tạo kết quả Security Hub, hàm Lambda sẽ gửi cảnh báo chi tiết về hết hạn chứng chỉ thông qua Amazon SNS. Bạn sẽ nhận được thông báo qua email theo địa chỉ bạn đã cung cấp trong tham số CloudFormation. Email sẽ chứa thông tin quan trọng về các chứng chỉ sắp hết hạn, bao gồm ARN và ngày hết hạn chính xác. Dưới đây là ví dụ về định dạng thông báo qua email



*Hình 7: Mẫu email thông báo do Amazon SNS gửi*

## Kết thúc

Quản lý chứng chỉ là rất quan trọng để duy trì tính bảo mật trên các khối lượng công việc hiện đại và AWS Private CA đóng một vai trò quan trọng trong việc cấp chứng chỉ có thời hạn hiệu lực tùy chỉnh. Giải pháp trong bài viết này cung cấp một cách tiếp cận mạnh mẽ, tự động để quản lý vòng đời chứng chỉ bằng cách tích hợp liền mạch một số dịch vụ AWS.

Giải pháp này kết hợp Amazon EventBridge để thực thi báo cáo kiểm tra theo lịch trình, AWS Lambda để xử lý và phân tích tự động, Amazon S3 để lưu trữ an toàn các báo cáo kiểm tra, Amazon SNS để gửi thông báo ngay lập tức và AWS Security Hub để giám sát và theo dõi tập trung. Tích hợp mạnh mẽ này tạo ra một quy trình tự động hóa toàn diện chủ động theo dõi thời hạn chứng chỉ và cung cấp cảnh báo kịp thời trên các triển khai đám mây, kết hợp và biên của bạn.

Bằng cách triển khai mẫu CloudFormation này, bạn có thể:

* Tự động hóa việc tạo và xử lý báo cáo kiểm tra AWS Private CA theo lịch trình
* Nhận thông báo ngay lập tức khi chứng chỉ đạt đến ngưỡng hết hạn
* Duy trì khả năng hiển thị tập trung thông qua các phát hiện chi tiết của Security Hub
* Theo dõi vòng đời chứng chỉ trên toàn bộ cơ sở hạ tầng của bạn
* Giúp đảm bảo tuân thủ các chính sách bảo mật của tổ chức
* Giảm thiểu rủi ro gián đoạn dịch vụ do chứng chỉ hết hạn

Giải pháp chuyển đổi quản lý chứng chỉ truyền thống từ quy trình thủ công, dễ xảy ra lỗi thành quy trình làm việc tự động, hợp lý. Nó cung cấp cho các nhóm bảo mật các công cụ cần thiết để chủ động quản lý vòng đời chứng chỉ, duy trì các yêu cầu tuân thủ và phản hồi nhanh chóng các vấn đề tiềm ẩn liên quan đến chứng chỉ. Các thông báo tự động và giám sát tập trung thông qua Security Hub giúp đảm bảo rằng không có chứng chỉ nào bị hết hạn, cho phép các nhóm thực hiện hành động kịp thời trước khi xảy ra gián đoạn dịch vụ.

Kết quả là một hệ thống có thể mở rộng, đáng tin cậy, giúp đơn giản hóa việc quản lý chứng chỉ và củng cố tình trạng bảo mật tổng thể của tổ chức bạn thông qua giám sát nhất quán và chủ động quản lý vòng đời chứng chỉ.

Nếu bạn có phản hồi về bài đăng này, hãy gửi nhận xét trong phần **Bình luận** bên dưới.

### IMG_262

### Santosh Vallurupalli

Santosh là Kiến trúc sư giải pháp cấp cao tại AWS. Santosh chuyên về mạng, bộ chứa và di chuyển, đồng thời thích giúp đỡ khách hàng trong hành trình áp dụng đám mây và xây dựng các giải pháp Cloud Native cho các vấn đề khó khăn. Khi không làm việc, anh thích đi du lịch, xem Formula1 và xem "The Office" ở chế độ lặp lại.

### IMG_263

### Manthan Raval

Manthan là Kiến trúc sư giải pháp chính tại AWS chuyên về ngành công nghiệp trò chơi, nơi ông giúp khách hàng kiến trúc các giải pháp đám mây an toàn, hiệu suất cao và có thể mở rộng. Manthan hợp tác chặt chẽ với các công ty trò chơi để chuyển đổi hoạt động của họ thông qua đổi mới đám mây. Ông đã hướng dẫn nhiều tổ chức trong hành trình chuyển đổi đám mây của họ, phát triển các kiến trúc mạnh mẽ để thúc đẩy giá trị kinh doanh. Anh ấy chia sẻ kiến thức của mình thông qua các buổi nói trước đám đông, hội thảo kỹ thuật và các buổi giáo dục khách hàng trên toàn cầu.