# Cách tăng cường bảo mật đám mây với Pulumi ESC và AWS Secrets Manager

của Marina Novikova , Jason Janiak và Josh Kodroff 30 THÁNG 4 NĂM 2025 trong [AWS Secrets Manager](https://aws.amazon.com/blogs/apn/category/security-identity-compliance/aws-secrets-manager/) , [AWS Systems Manager](https://aws.amazon.com/blogs/apn/category/management-tools/aws-systems-manager/) , [Trung cấp (200)](https://aws.amazon.com/blogs/apn/category/learning-levels/intermediate-200/) , [Giải pháp đối tác](https://aws.amazon.com/blogs/apn/category/post-types/partner-solutions/) , [Bảo mật](https://aws.amazon.com/blogs/apn/category/security-identity-compliance/security/) [Liên kết cố định](https://aws.amazon.com/blogs/apn/how-to-strengthen-cloud-security-with-pulumi-esc-and-aws-secrets-manager/) [Bình luận](https://aws.amazon.com/blogs/apn/how-to-strengthen-cloud-security-with-pulumi-esc-and-aws-secrets-manager/#Comments) [Chia sẻ](https://aws.amazon.com/vi/blogs/apn/how-to-strengthen-cloud-security-with-pulumi-esc-and-aws-secrets-manager/#)

*Bởi Josh Kodroff, Kiến trúc sư thành công khách hàng chính – Pulumi  
Bởi Marina Novikova, Kiến trúc sư giải pháp đối tác cao cấp – AWS  
Bởi Jason Janiak, Kiến trúc sư giải pháp đối tác – AWS*

| *Biểu tượng Pulumi*  Pulumi  Kết nối với Pulumi |
| --- |
|
|

Các tổ chức hiện đại cần quản lý nhiều bí mật, bao gồm khóa Giao diện lập trình ứng dụng (API), mã thông báo hoặc thông tin xác thực. Một số yếu tố góp phần vào việc các tổ chức sử dụng nhiều giải pháp quản lý bí mật. Các yếu tố này bao gồm hệ thống cũ, sáp nhập và mua lại và nhiều yêu cầu pháp lý khác nhau.

Với một điểm kiểm soát duy nhất, các tổ chức có thể thấy được nơi lưu trữ bí mật và ai có quyền truy cập vào chúng, tạo điều kiện thuận lợi cho các nỗ lực kiểm toán và tuân thủ. Sự phức tạp của việc quản lý bí mật tăng theo cấp số nhân khi các tổ chức mở rộng quy mô. Điều này đặc biệt đúng khi thêm nhiều tài khoản AWS hơn và sử dụng môi trường kết hợp.

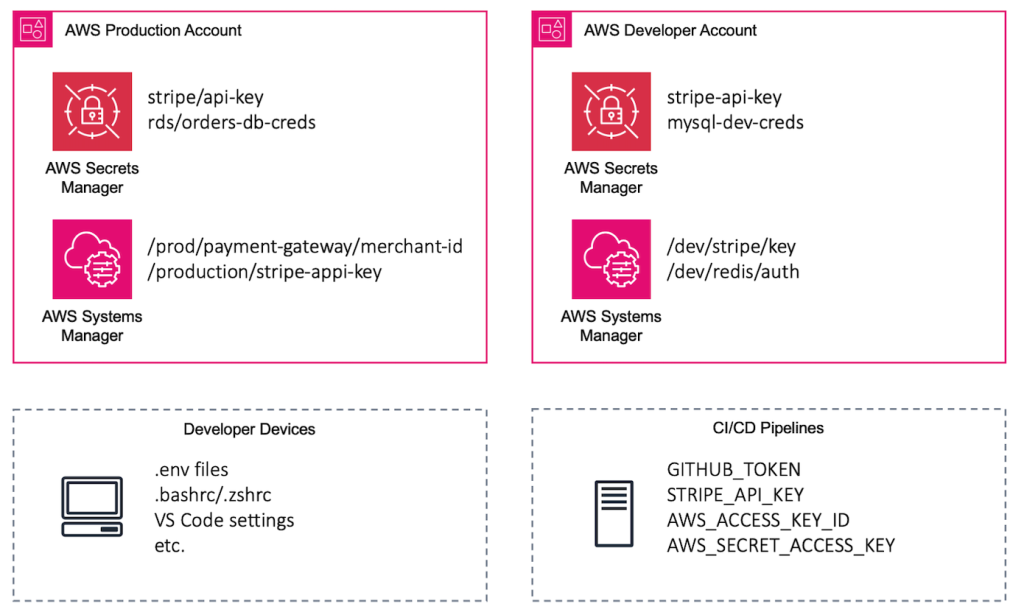
Bài đăng này khám phá cách thống nhất quản lý bí mật cho các tổ chức ở mọi quy mô. Chúng ta sẽ xem xét các công cụ AWS như [AWS Secrets Manager](https://aws.amazon.com/secrets-manager/) và [AWS Systems Manager Parameter Store](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html) , kết hợp với [Pulumi ESC](https://www.pulumi.com/product/secrets-management/) (Môi trường, Bí mật và Cấu hình) để thống nhất [quản lý bí mật](https://www.pulumi.com/what-is/what-is-secrets-management/) .

## **Vấn đề rò rỉ bí mật**

Giải pháp lưu trữ thông tin xác thực trong Secrets Manager có thể phát triển thành một hệ sinh thái bí mật rộng lớn được phân bổ trên khắp các vị trí lưu trữ và hệ thống. Vấn đề thậm chí còn khó khăn hơn nếu dấu chân tài nguyên của tổ chức bạn cũng nằm ngoài AWS, sử dụng các trung tâm dữ liệu khác.

Hãy xem xét một kịch bản doanh nghiệp điển hình với nhiều vị trí bí mật. Thông tin xác thực cơ sở dữ liệu sản xuất có thể được lưu trữ trong Secrets Manager trong một tài khoản. Trong khi đó, các khóa API của bên thứ ba và các bí mật khác nằm trong Systems Manager Parameter Store trong một tài khoản khác. Các nhóm phát triển duy trì các bộ thông tin xác thực của riêng họ trong các tệp .env, cấu hình shell và môi trường phát triển cục bộ. Các bí mật cũng được sao chép trong các cấu hình đường ống CI/CD trên các kho lưu trữ khác nhau.

Hình *1* minh họa ví dụ về một tổ chức có nhiều môi trường phát triển và triển khai AWS, thiết bị dành cho nhà phát triển và đường ống CI/CD.



Hình 1 : *Ví dụ về tổ chức có nhiều môi trường, thiết bị và đường ống*

Sự rò rỉ bí mật này tạo ra một số thách thức quan trọng. Việc phân phối bí mật trên nhiều hệ thống sẽ mở rộng bề mặt tấn công tiềm ẩn và tăng nguy cơ bảo mật . Một quyền truy cập không mong muốn tại bất kỳ điểm nào, chẳng hạn như máy của nhà phát triển, có thể làm tổn hại đến thông tin xác thực nhạy cảm. Khi đến lúc luân chuyển thông tin xác thực, việc theo dõi mọi trường hợp bí mật trở thành một nhiệm vụ khó khăn. [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) cung cấp các khả năng động cho thông tin xác thực tạm thời thông qua [AWS Security Token Service (AWS STS).](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html) Tuy nhiên, một số công cụ vẫn dựa vào các giá trị tĩnh cần luân chuyển định kỳ. Các dịch vụ sử dụng cần có thời gian để chuyển sang các giá trị bí mật mới để tránh thời gian chết. Điều này dẫn đến việc quản lý luân chuyển phức tạp và dễ xảy ra lỗi .

[Việc luân chuyển bí mật với Pulumi ESC](https://www.pulumi.com/blog/esc-secret-rotation-with-iac/) giúp tránh được gánh nặng. Một vấn đề khác làm tăng chi phí hoạt động là dấu vết kiểm toán bị phân mảnh. Trong khi các dịch vụ AWS cung cấp nhật ký truy cập chi tiết, các bí mật được lưu trữ cục bộ trên máy của nhà phát triển hoặc trong các tệp cấu hình không để lại dấu vết kiểm toán. Khi các bí mật được phân tán trên nhiều tài khoản và vùng AWS, việc ghép lại một lịch sử truy cập toàn diện trở nên khó khăn và tốn thời gian.

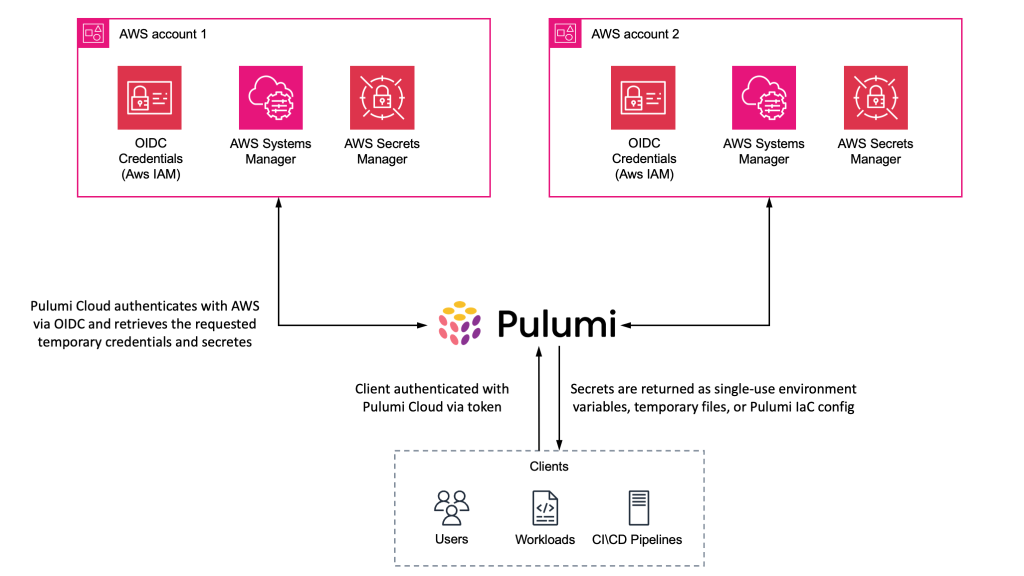
Ngoài ra, để truy cập các bí mật nằm ở nhiều vị trí lưu trữ khác nhau, bạn buộc phải cấp quyền IAM rộng cho các principal (đối tượng được cấp quyền). Điều này dẫn đến việc cấp quyền vượt mức cần thiết và vi phạm nguyên tắc phân quyền tối thiểu (least privilege). Các giải pháp lưu trữ khác nhau lại có mô hình bảo mật và cơ chế kiểm soát truy cập khác nhau. Việc kiểm soát truy cập không đồng nhất khiến cho việc triển khai và duy trì các chính sách bảo mật nhất quán trở nên khó khăn.

Cách tiếp cận phân mảnh này đối với việc quản lý bí mật không chỉ làm tăng rủi ro bảo mật mà còn tạo ra chi phí hoạt động và thách thức về tuân thủ. Các tổ chức hiện đại cần một cách tiếp cận tập trung, an toàn và có thể quản lý được đối với việc xử lý bí mật.

## **Pulumi ESC giúp giải quyết bí mật lan rộng như thế nào**

Pulumi ESC cung cấp giải pháp quản lý bí mật một cách an toàn. Nó hoạt động như một nhà môi giới an toàn giữa các ứng dụng của bạn và nhiều nhà cung cấp bí mật khác nhau. Các nhà cung cấp này bao gồm AWS Secrets Manager, [HashiCorp Vault](https://www.vaultproject.io/) và [các tệp cấu hình Kubernetes](https://kubernetes.io/docs/concepts/configuration/organize-cluster-access-kubeconfig/) . Pulumi ESC cũng hoạt động với [Kubernetes External Secrets Operator](https://external-secrets.io/latest/) .

Hình *2* minh họa cách hoạt động của Pulumi ESC, tiếp theo là mô tả chi tiết hơn trong blog bên dưới.



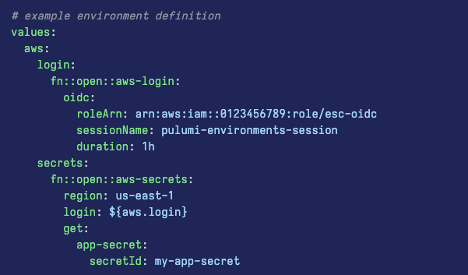
Hình 2 : *Minh họa cách Pulumi ESC hoạt động*

## **Thiết lập ESC**

Việc triển khai bắt đầu bằng việc quản trị viên cấu hình nhà cung cấp OIDC trong IAM. Nó cho phép Pulumi Cloud xác thực an toàn với tài khoản AWS của bạn và thiết lập mối quan hệ đáng tin cậy giữa cơ sở hạ tầng của bạn và hệ thống quản lý bí mật. Bây giờ các kỹ sư có thể tạo môi trường Pulumi ESC và sử dụng vai trò OIDC để truy cập bí mật trong tài khoản AWS.

### **Môi trường ESC Pulumi**

Pulumi ESC là cốt lõi của các môi trường, cấu hình dựa trên YAML, đóng vai trò là nguồn duy nhất đáng tin cậy cho thông tin xác thực tạm thời, bí mật và giá trị cấu hình của bạn. Các môi trường có thể lưu trữ bí mật tĩnh và giá trị cấu hình trực tiếp trong kho lưu trữ an toàn của Pulumi Cloud và tích hợp với các nhà cung cấp danh tính gốc trên đám mây thông qua OIDC, như [IAM](https://www.pulumi.com/docs/esc/integrations/dynamic-login-credentials/aws-login/) . Các trường hợp sử dụng phổ biến khác bao gồm sử dụng tích hợp với các dịch vụ được quản lý như [Secrets Manager](https://www.pulumi.com/docs/esc/integrations/dynamic-secrets/aws-secrets/) và [Systems Manager Parameter Store,](https://www.pulumi.com/docs/esc/integrations/dynamic-secrets/aws-parameter-store/) như được hiển thị trong Hình 3 bên dưới.



Hình 3: *Ví dụ về cấu hình môi trường*

Để biết danh sách đầy đủ các tích hợp được hỗ trợ, hãy xem [Tích hợp Pulumi ESC](https://www.pulumi.com/docs/esc/integrations/) .

Môi trường được thiết kế với tính linh hoạt. Người quản trị có thể cấu hình cách thức bí mật được phân phối đến các ứng dụng: dưới dạng biến môi trường, tệp tạm thời (như tệp Kubernetes KUBECONFIG) hoặc đầu vào trực tiếp cho các chương trình Pulumi Infrastructure as Code.

Để thúc đẩy khả năng tái sử dụng và duy trì các nguyên tắc Không lặp lại chính mình (DRY), môi trường Pulumi ESC có thể nhập các môi trường khác, cho phép tổ chức bí mật và cấu hình theo thứ bậc.

### **Kiểm soát truy cập và bảo mật**

ESC triển khai Kiểm soát truy cập dựa trên vai trò (RBAC) mạnh mẽ thông qua Pulumi Cloud. Người quản trị có thể xác định chính xác những người dùng nào có thể thực hiện các hành động cụ thể (đọc, mở, ghi, xóa) trên mỗi môi trường. Kiểm soát chi tiết này đảm bảo rằng người dùng và dịch vụ chỉ truy cập vào các bí mật mà họ cần, tuân thủ nguyên tắc đặc quyền tối thiểu.

### **Kinh nghiệm của nhà phát triển và CI/CD**

Người dùng cuối, dù là nhà phát triển hay quy trình tự động, đều có thể truy cập bí mật bằng [pulumi CLI](https://www.pulumi.com/docs/iac/cli/) hoặc [esc CLI](https://www.pulumi.com/docs/esc/cli/) chuyên dụng. Đầu tiên, sử dụng [esc open](https://www.pulumi.com/docs/esc/cli/commands/esc_open/) để chỉ định môi trường mở và cho phép xác định lệnh thực thi với bí mật trong môi trường cụ thể này. ESC xử lý phần còn lại.

Đằng sau hậu trường, ESC xác thực người dùng thông qua mã thông báo Pulumi Cloud của họ và xác minh quyền truy cập thông qua RBAC. Tiếp theo, nó lấy các bí mật cần thiết từ nhiều nhà cung cấp khác nhau và tạo ra một môi trường tạm thời để thực hiện lệnh. ESC cũng tự động dọn dẹp sau khi lệnh hoàn tất.

Quá trình này đảm bảo rằng bí mật không bao giờ tồn tại trên máy cục bộ và quyền truy cập được ghi lại và kiểm soát.

## **Vượt ngoài quản lý bí mật cơ bản**

Khả năng của ESC mở rộng ra ngoài quản lý bí mật truyền thống với bốn tính năng chính. Các ứng dụng có thể tích hợp trực tiếp với ESC bằng Pulumi ESC SDK để truy cập bí mật thời gian chạy an toàn mà không cần lưu trữ cục bộ. Nền tảng này tạo ra các phiên bản có tên mới khi môi trường thay đổi, cho phép người dùng sử dụng các phiên bản cụ thể hoặc mới nhất. Tích hợp của ESC với Kubernetes External Secrets Operator cung cấp cho các ứng dụng quyền truy cập hợp nhất vào các bí mật từ nhiều nhà cung cấp khác nhau. Cuối cùng, thông qua tích hợp IAM, ESC cho phép các nhà điều hành xoay vòng các khóa truy cập cho các khối lượng công việc yêu cầu thông tin xác thực lâu dài.

Bằng cách tập trung quản lý bí mật thông qua ESC, các tổ chức có thể duy trì một điểm kiểm soát duy nhất và đảm bảo ghi nhật ký kiểm toán toàn diện trên tất cả các quyền truy cập bí mật. Nó đơn giản hóa việc luân chuyển bí mật và giảm sự phức tạp của quyền IAM trong khi vẫn duy trì các biện pháp kiểm soát truy cập nhất quán trên tất cả các môi trường. Do đó, nó giúp các nhóm đáp ứng các yêu cầu tuân thủ của tổ chức.

Phương pháp quản lý bí mật thống nhất này biến đổi bối cảnh từng phân tán và rủi ro thành một hệ thống được kiểm soát, an toàn và có thể kiểm toán.

## **Boost Insurance: Nâng cao năng suất bảo mật và phát triển với Pulumi ESC**

Boost Insurance là một nhà cung cấp nền tảng có trụ sở tại New York, trao quyền cho các công ty xây dựng, ra mắt và mở rộng các chương trình bảo hiểm sáng tạo. Hoạt động tại giao điểm của công nghệ và bảo hiểm, Boost Insurance cần cơ sở hạ tầng đám mây an toàn, có thể mở rộng để hỗ trợ nhu cầu kinh doanh ngày càng tăng của họ. Khi mở rộng hoạt động đám mây, tổ chức cần một giải pháp để quản lý thông tin xác thực truy cập một cách an toàn trong khi vẫn duy trì năng suất của nhà phát triển và các hoạt động cấu hình nhất quán. Boost Insurance nhận thấy Pulumi ESC đã giải quyết được những nhu cầu này.

“ *Với Pulumi ESC, các nhà phát triển của chúng tôi có được thông tin xác thực AWS động theo yêu cầu. Điều đó loại bỏ nhu cầu về các mã thông báo tồn tại lâu dài và tăng cường bảo mật. ESC cho phép các chương trình Pulumi chia sẻ thông tin xác thực an toàn và truy cập các bí mật trong môi trường đám mây nhất định của chúng. ESC là một công cụ chia sẻ quản lý cấu hình và bí mật tuyệt vời để cho phép tiếp cận DRY đối với quá trình phát triển.* ” Richard Genthner, Phó chủ tịch Bảo mật Cơ sở hạ tầng tại Boost Insurance cho biết.

## **Phần kết luận**

Các tổ chức ngày nay phải đối mặt với sự phức tạp trong việc quản lý bí mật trên cơ sở hạ tầng đám mây của họ. Rủi ro của việc bí mật rò rỉ – từ lỗ hổng bảo mật đến chi phí hoạt động – không phải là lý thuyết. Như đã chứng minh bằng những câu chuyện thành công của khách hàng, những thách thức này là có thật và chúng đòi hỏi các giải pháp thực tế.

Cải thiện khả năng quản lý bí mật của bạn với Pulumi ESC, bất kể quy mô nhóm của bạn. Truy cập blog Pulumi để biết [tài nguyên AWS](https://www.pulumi.com/blog/tag/aws/) và [tham gia hội thảo của chúng tôi](https://www.pulumi.com/resources/#upcoming) để xem các bản trình diễn trực tiếp về các giải pháp AWS.



.

## **Pulumi – Đối tác nổi bật của AWS**

Pulumi là Đối tác công nghệ tiên tiến của AWS và Đối tác năng lực của AWS giúp các nhóm kỹ thuật nền tảng dễ dàng tự động hóa, bảo mật và quản lý mọi triển khai đám mây với cơ sở hạ tầng dưới dạng mã, quản lý bí mật tập trung, thực thi chính sách và khả năng phân tích.

[Liên hệ Pulumi](https://partners.amazonaws.com/contactpartner?partnerId=0010L00001pDtqKQAS&partnerName=Pulumi&source=Blog&campaign=) | [Tổng quan về đối tác](https://partners.amazonaws.com/partners/0010L00001pDtqKQAS/Pulumi) | [AWS Marketplace](https://aws.amazon.com/marketplace/seller-profile?id=b3d56f96-ff1e-4284-9585-5ef58df12266) | [Nghiên cứu tình huống](https://partners.amazonaws.com/partners/0010L00001pDtqKQAS/Pulumi#case-studies)

THẺ: [AWS Secrets Manager](https://aws.amazon.com/blogs/apn/tag/aws-secrets-manager/) , [Trung cấp (200)](https://aws.amazon.com/blogs/apn/tag/intermediate-200/) , [Giải pháp đối tác](https://aws.amazon.com/blogs/apn/tag/partner-solutions/) , [Pulumi](https://aws.amazon.com/blogs/apn/tag/pulumi/) , [Bảo mật](https://aws.amazon.com/blogs/apn/tag/security/) , [Lãnh đạo tư tưởng](https://aws.amazon.com/blogs/apn/tag/thought-leadership/)