# **GIỚI THIỆU QUYỀN TRUY CẬP NÚT JUST-IN-TIME BẰNG AWS SYSTEMS MANAGER**

bởi Chetan Makvana , Anthony Verleysen và Mark Brealey vào29 THÁNG 4 NĂM 2025 trong [Thông báo](https://aws.amazon.com/blogs/mt/category/post-types/announcements/) , [AWS Systems Manager](https://aws.amazon.com/blogs/mt/category/management-tools/aws-systems-manager/) , [Công cụ quản lý](https://aws.amazon.com/blogs/mt/category/management-tools/) , [Bảo](https://aws.amazon.com/blogs/mt/category/security-identity-compliance/security/) [mật Liên kết cố định](https://aws.amazon.com/blogs/mt/introducing-just-in-time-node-access-using-aws-systems-manager/) [Chia sẻ](https://aws.amazon.com/blogs/mt/introducing-just-in-time-node-access-using-aws-systems-manager/)

Hôm nay, chúng tôi rất vui mừng thông báo về tính khả dụng chung của [quyền truy cập nút just-in-time](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-just-in-time-node-access.html) , một khả năng mới trong [AWS Systems Manager](https://aws.amazon.com/systems-manager/) . Quyền truy cập nút just-in-time cho phép truy cập động, có giới hạn thời gian vào [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/ec2/) , tại chỗ và các nút đa đám mây do AWS Systems Manager quản lý. Nó sử dụng quy trình phê duyệt dựa trên chính sách, cho phép bạn xóa quyền truy cập lâu dài trong khi vẫn duy trì hiệu quả hoạt động và tăng cường bảo mật.

Các tổ chức mở rộng hoạt động của mình lên hàng nghìn nút cần có quyền chi tiết dựa trên danh tính để hỗ trợ mục tiêu kiểm toán và tuân thủ của họ. Họ muốn loại bỏ hoàn toàn thông tin xác thực dài hạn. Thực tế sử dụng thông tin xác thực dài hạn để truy cập nút tạo ra lỗ hổng bảo mật, làm tăng nguy cơ truy cập trái phép và vi phạm tiềm ẩn.

Trước đây, khách hàng phải đối mặt với sự đánh đổi đầy thách thức giữa bảo mật và hiệu quả hoạt động. Thay vì xác định cẩn thận những ai cần truy cập vào các tài nguyên cụ thể, các nhóm CNTT sẽ cấp quá nhiều quyền cho các nhóm người dùng lớn. Thực hành này tạo ra nguy cơ gia tăng các lỗi vô tình của người vận hành và cơ hội cho những kẻ xấu, do nhu cầu về sự tiện lợi trong hoạt động. Họ hoặc duy trì thông tin xác thực dài hạn, làm tăng nguy cơ bảo mật bị xâm phạm hoặc triển khai các biện pháp kiểm soát truy cập hạn chế làm chậm phản hồi sự cố. Các giải pháp được xây dựng riêng tỏ ra phức tạp để duy trì và mở rộng quy mô; trong khi các công cụ không phải của AWS sử dụng tác nhân yêu cầu danh tính và quyền để truy cập các nút.

## **Tổng quan**

Quyền truy cập nút Just-in-time giúp bạn triển khai quyền truy cập ít đặc quyền nhất trong khi vẫn đảm bảo các nhóm vận hành có thể phản hồi nhanh chóng các sự cố. Nó hoạt động liền mạch trên toàn [Tổ chức AWS](https://aws.amazon.com/organizations/) của bạn , cho phép bạn thiết lập các biện pháp kiểm soát truy cập nhất quán cho dù bạn đang quản lý một tài khoản hay nhiều tài khoản. Khả năng mới này cho phép quản trị viên xác định các biện pháp kiểm soát truy cập chính xác thông qua các chính sách phê duyệt chỉ định ai có thể truy cập vào nút nào và trong điều kiện nào. Các tổ chức có thể lựa chọn giữa các quy trình phê duyệt thủ công với nhiều người phê duyệt hoặc các chính sách phê duyệt tự động dựa trên điều kiện, mang lại sự linh hoạt để phù hợp với các yêu cầu bảo mật của họ.

Ví dụ, quản trị viên có thể thiết lập chính sách phê duyệt tự động để nhanh chóng cung cấp quyền truy cập cho các kỹ sư trực trong các sự cố, chỉ cấp quyền truy cập cho các nhà điều hành trong nhóm [AWS IAM Identity Center](https://aws.amazon.com/iam/identity-center/) trực . Thông qua quyền truy cập nút đúng lúc, các nhà điều hành có thể yêu cầu quyền truy cập vào các nút khi họ cần. Dựa trên các chính sách phê duyệt được cấu hình trước, họ nhận được quyền truy cập tạm thời tự động hết hạn sau một khoảng thời gian xác định. Sau khi được phê duyệt, họ có thể truy cập trực tiếp vào các nút này thông qua shell dựa trên trình duyệt một cú nhấp chuột, [Giao diện dòng lệnh AWS (AWS CLI)](https://aws.amazon.com/cli/) hoặc Giao thức máy tính từ xa (RDP) được Systems Manager hỗ trợ, mà không cần phải mở cổng đến hoặc quản lý khóa SSH.

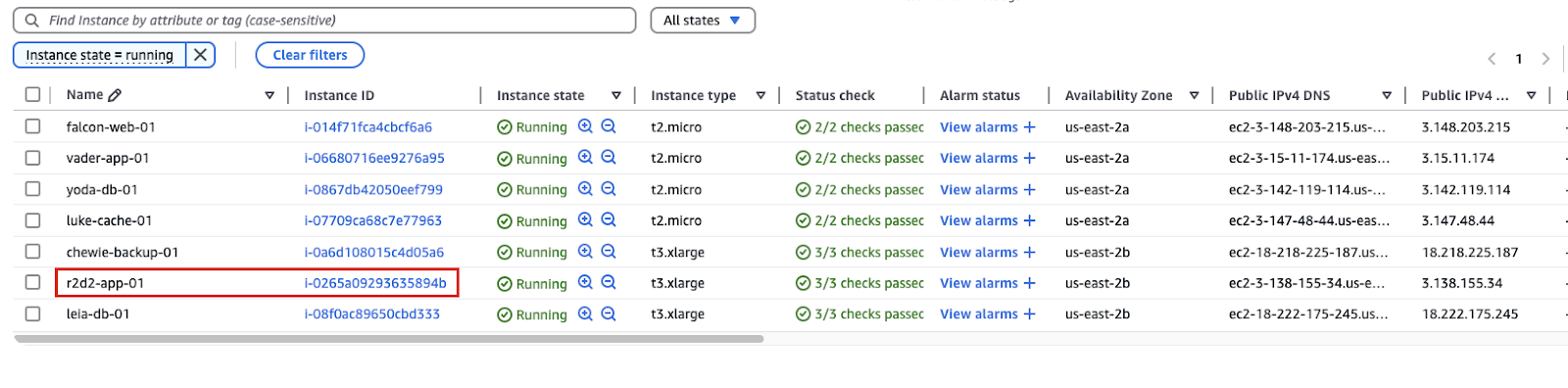
Để đơn giản hóa quy trình phê duyệt, quyền truy cập nút đúng lúc tích hợp với các công cụ như Slack và Microsoft Teams thông qua [Amazon Q Developer](https://aws.amazon.com/q/developer/) và email để thông báo cho người phê duyệt về các yêu cầu đang chờ xử lý. Systems Manager cũng phát các sự kiện đến [Amazon EventBridge](https://aws.amazon.com/eventbridge/) để cập nhật trạng thái cho yêu cầu truy cập phiên nút đúng lúc. Các sự kiện này có thể được định tuyến đến [Amazon Simple Notification Service (Amazon SNS)](https://aws.amazon.com/sns/) để thông báo hoặc tích hợp với các hệ thống nội bộ của bạn, cho phép nhóm của bạn theo dõi và phản hồi các yêu cầu truy cập thông qua quy trình công việc hiện có của bạn. Điều này cho phép bạn giám sát các yêu cầu truy cập và duy trì các dấu vết kiểm toán trên toàn tổ chức của mình. Hơn nữa, quyền truy cập nút đúng lúc có thể cung cấp khả năng hiển thị bổ sung vào các hoạt động của người vận hành bằng cách ghi nhật ký các lệnh chạy trong các phiên và ghi lại hành động của chúng trong các phiên RDP.

Systems Manager cung cấp bản dùng thử miễn phí quyền truy cập nút just-in-time cho mỗi tài khoản trên mỗi Khu vực, cho phép bạn khám phá và đánh giá đầy đủ tính năng này cho tổ chức của mình. Thời gian dùng thử này bao gồm phần còn lại của kỳ thanh toán mà bạn bật tính năng này, cộng với toàn bộ kỳ thanh toán tiếp theo. Trong thời gian dùng thử này, bạn sẽ có quyền truy cập vào tất cả các chức năng, cho phép bạn kiểm tra cấu hình và chính sách truy cập mà không phải trả thêm bất kỳ khoản phí nào. Sau khi thời gian dùng thử kết thúc, quyền truy cập nút just-in-time sẽ trở thành dịch vụ trả phí, với mức phí dựa trên các mẫu sử dụng của bạn. Để biết thông tin giá chi tiết và phân tích chi phí, vui lòng tham khảo [AWS Systems Manager Pricing](https://aws.amazon.com/systems-manager/pricing/) .

## **Sử dụng Truy cập nút Just-in-Time**

Khi bạn triển khai truy cập nút just-in-time, bạn sẽ làm việc với ba vai trò riêng biệt: Quản trị viên, Người vận hành và Người phê duyệt. Người quản trị thiết lập và duy trì các chính sách phê duyệt. Người vận hành khởi tạo các yêu cầu truy cập cho các nút cụ thể. Và người phê duyệt xem xét và ủy quyền các yêu cầu truy cập.

Chúng ta hãy cùng tìm hiểu cách thiết lập và sử dụng tính năng này, trong trường hợp kỹ sư trực của bạn cần truy cập vào hệ thống sản xuất, cụ thể là một phiên bản có tên ' r2d2-app-01 ' từ nhóm phiên bản bên dưới như trong hình 1.



*Hình 1: Bảng điều khiển Amazon EC2 hiển thị danh sách các phiên bản EC2*

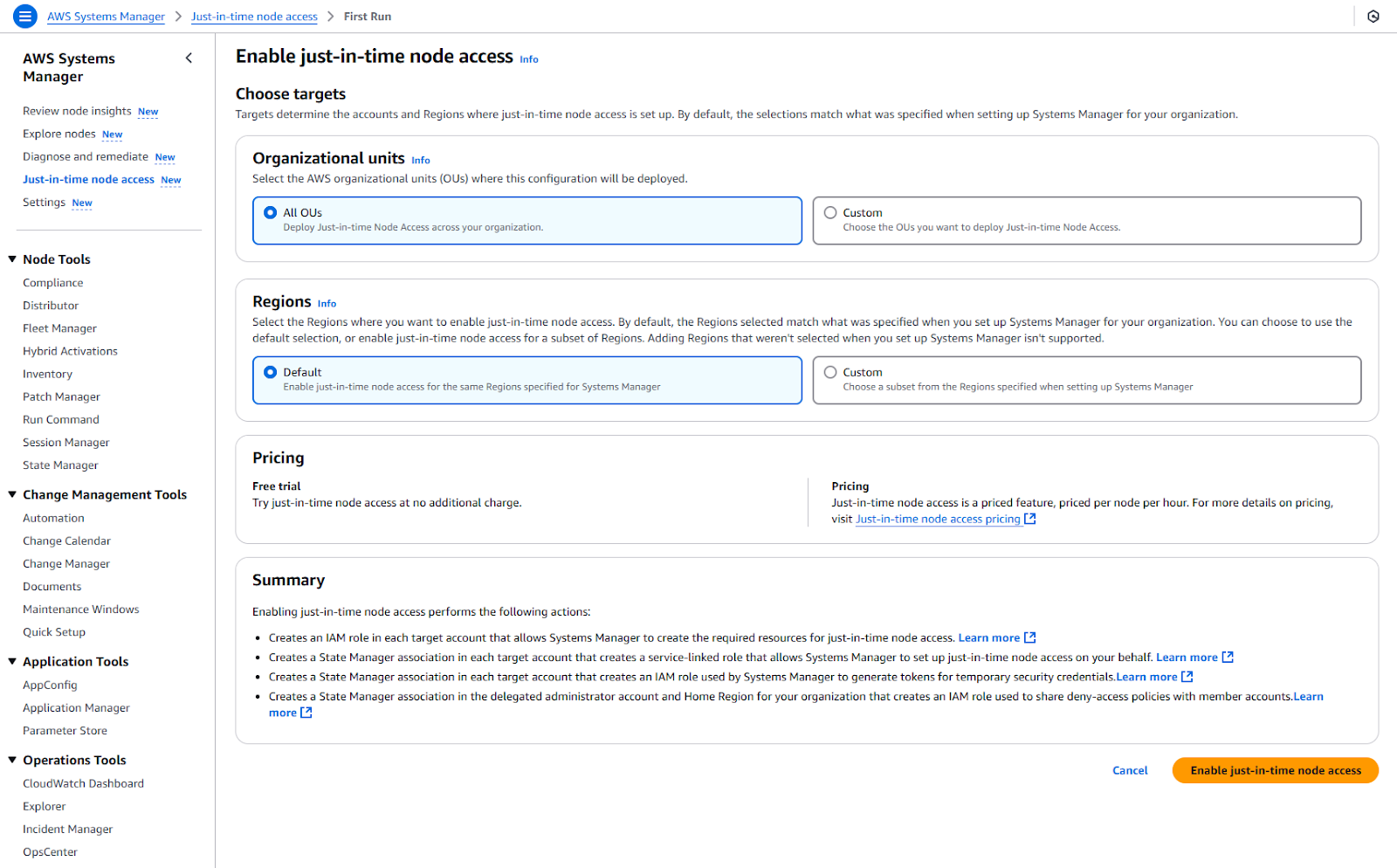
Chúng ta sẽ tìm hiểu cách một kỹ sư trực ban (Người vận hành) có thể yêu cầu quyền truy cập vào hệ thống sản xuất, với người đứng đầu DevOps (Người phê duyệt) quản lý việc phê duyệt, tất cả đều nằm trong chính sách phê duyệt do Quản trị viên xác định.

## **Thiết lập quyền truy cập nút Just-in-time với tư cách là Quản trị viên**

#### Bước 1 – Kích hoạt Truy cập Nút Just-in-Time

Trong hướng dẫn này, chúng tôi sẽ bật quyền truy cập nút just-in-time cho Tổ chức AWS. Để bắt đầu, trước tiên bạn phải thiết lập [bảng điều khiển hợp nhất Systems Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-setting-up-organizations.html) . Sau khi bảng điều khiển hợp nhất được thiết lập, bạn có thể bật quyền truy cập nút just-in-time trong Systems Manager.

Sau đó, bạn có thể chọn Đơn vị tổ chức (OU) và Vùng AWS nào để nhắm mục tiêu triển khai. Điều này cho phép bạn kiểm soát chính xác nơi giải pháp được triển khai, cho dù trên toàn bộ tổ chức của bạn hay trong các khu vực cụ thể như thể hiện trong hình 2.



*Hình 2: Cho phép truy cập nút đúng lúc*

#### Bước 2 – Tạo chính sách phê duyệt

Sau khi bật tính năng này, bước quan trọng tiếp theo là tạo chính sách phê duyệt. Chính sách phê duyệt xác định cách người dùng có quyền truy cập vào các nút. Các chính sách này có ba loại: phê duyệt tự động , phê duyệt thủ công và chính sách từ chối truy cập . Chính sách phê duyệt tự động xác định người dùng có thể kết nối tự động đến các nút nào. Chính sách phê duyệt thủ công xác định số lượng và mức độ phê duyệt thủ công phải được cung cấp để truy cập vào các nút bạn chỉ định. Chính sách từ chối truy cập ngăn chặn rõ ràng việc tự động phê duyệt các yêu cầu truy cập vào các nút bạn chỉ định.

Trong ví dụ của chúng tôi, chúng tôi sẽ tập trung vào việc tạo chính sách phê duyệt thủ công cho các nút được gắn thẻ Workload:Application01, bao gồm nút ' r2d2-app-01 ' của chúng tôi.

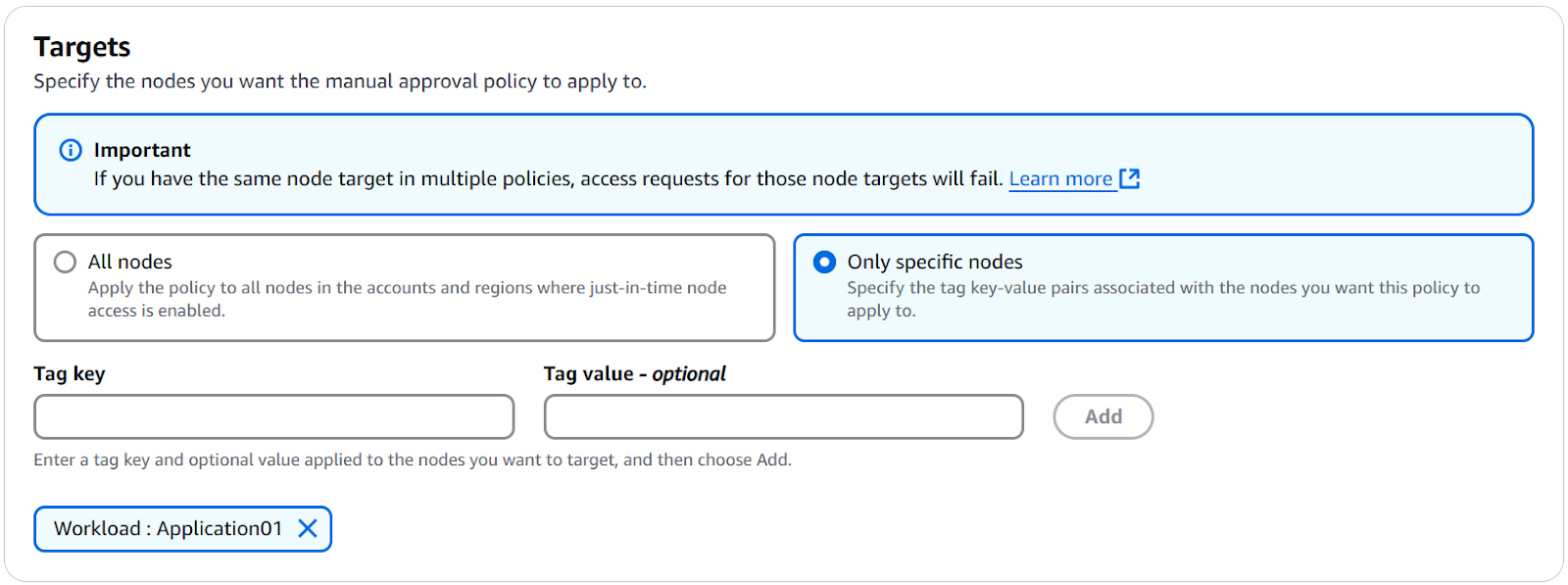
Để tạo chính sách, hãy điều hướng đến [bảng điều khiển AWS Systems Manager](https://console.aws.amazon.com/systems-manager/home) , chọn just-in-time node access trong ngăn điều hướng, chọn tab Approval policies và chọn Create manual policy . Cấu hình chính sách yêu cầu một số thành phần chính.

Đầu tiên, trong phần Chi tiết chính sách phê duyệt , hãy cung cấp tên và mô tả cho chính sách phê duyệt, cùng với việc thiết lập thời hạn truy cập tối đa như thể hiện trong hình 3. Thời hạn này xác định thời gian quyền truy cập được phê duyệt vẫn có hiệu lực trước khi tự động hết hạn.



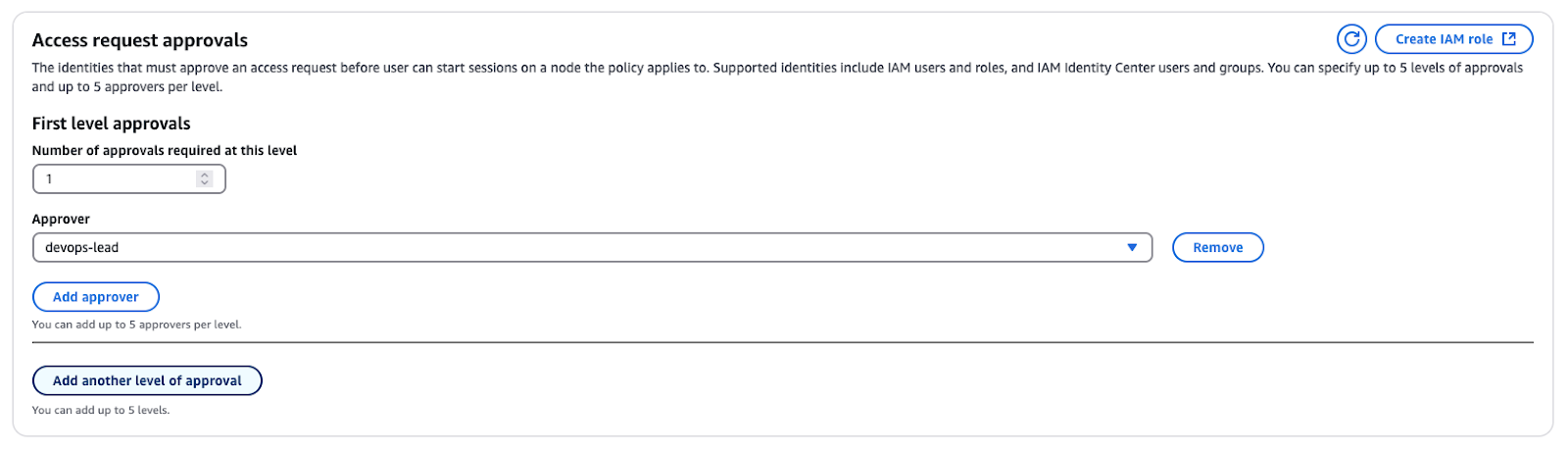
*Hình 3: Trang chính sách phê duyệt thủ công*

Trong phần Mục tiêu , hãy sử dụng cặp khóa-giá trị thẻ để xác định các nút mà chính sách áp dụng. Đối với ví dụ này, chúng tôi sẽ nhắm mục tiêu đến các nút được gắn thẻ Workload:Application01, bao gồm nút ' r2d2-app-01 ' của chúng tôi. Cách tiếp cận này đảm bảo chính sách áp dụng cho tất cả các nút được liên kết với Application01như thể hiện trong hình 4.



*Hình 4: Mục tiêu chính sách phê duyệt thủ công*

Trong phần Người phê duyệt yêu cầu truy cập , bạn sẽ chỉ định những cá nhân hoặc nhóm được ủy quyền phê duyệt yêu cầu truy cập. Trong kịch bản của chúng tôi, chúng tôi sẽ chỉ định vai trò trưởng nhóm DevOps làm người phê duyệt. Người phê duyệt yêu cầu truy cập có thể là người dùng và nhóm IAM Identity Center hoặc người dùng, nhóm và vai trò IAM như thể hiện trong hình 5.



*Hình 5: Phê duyệt yêu cầu truy cập*

Bạn cũng có thể định nghĩa các quy tắc truy cập tự động bằng [ngôn ngữ chính sách Cedar](https://www.cedarpolicy.com/en) , loại bỏ nhu cầu phê duyệt thủ công trong các tình huống đáng tin cậy. Hãy coi các chính sách phê duyệt tự động như sổ tay quy tắc truy cập được phê duyệt trước của tổ chức bạn. Các chính sách này chỉ định những nút nào mà người dùng có thể truy cập tự động, dựa trên các điều kiện được xác định trước và mức độ tin cậy. Để biết thêm thông tin, hãy xem [Tạo chính sách phê duyệt tự động cho quyền truy cập nút đúng lúc](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-just-in-time-node-access-create-auto-approval-policies.html) và [Cấu trúc câu lệnh và toán tử tích hợp cho các chính sách phê duyệt tự động và từ chối truy cập](https://docs.aws.amazon.com/systems-manager/latest/userguide/auto-approval-deny-access-policy-statement-structure.html) .

Ví dụ: bạn có thể tạo chính sách phê duyệt tự động cho phép các thành viên của nhóm “DevOpsTeam” truy cập vào các nút được gắn thẻ bằng Environment: Developmentcách sử dụng chính sách Cedar sau:

// Policy to permit access to Development nodes for members of the DevOpsTeam IDC group

permit (

    principal in AWS::IdentityStore::Group::"911b8590-7041-70fa-d20b-12345EXAMPLE",

    action == AWS::SSM::Action::"getTokenForInstanceAccess",

    resource)

  when {

    resource.hasTag("Environment") &&

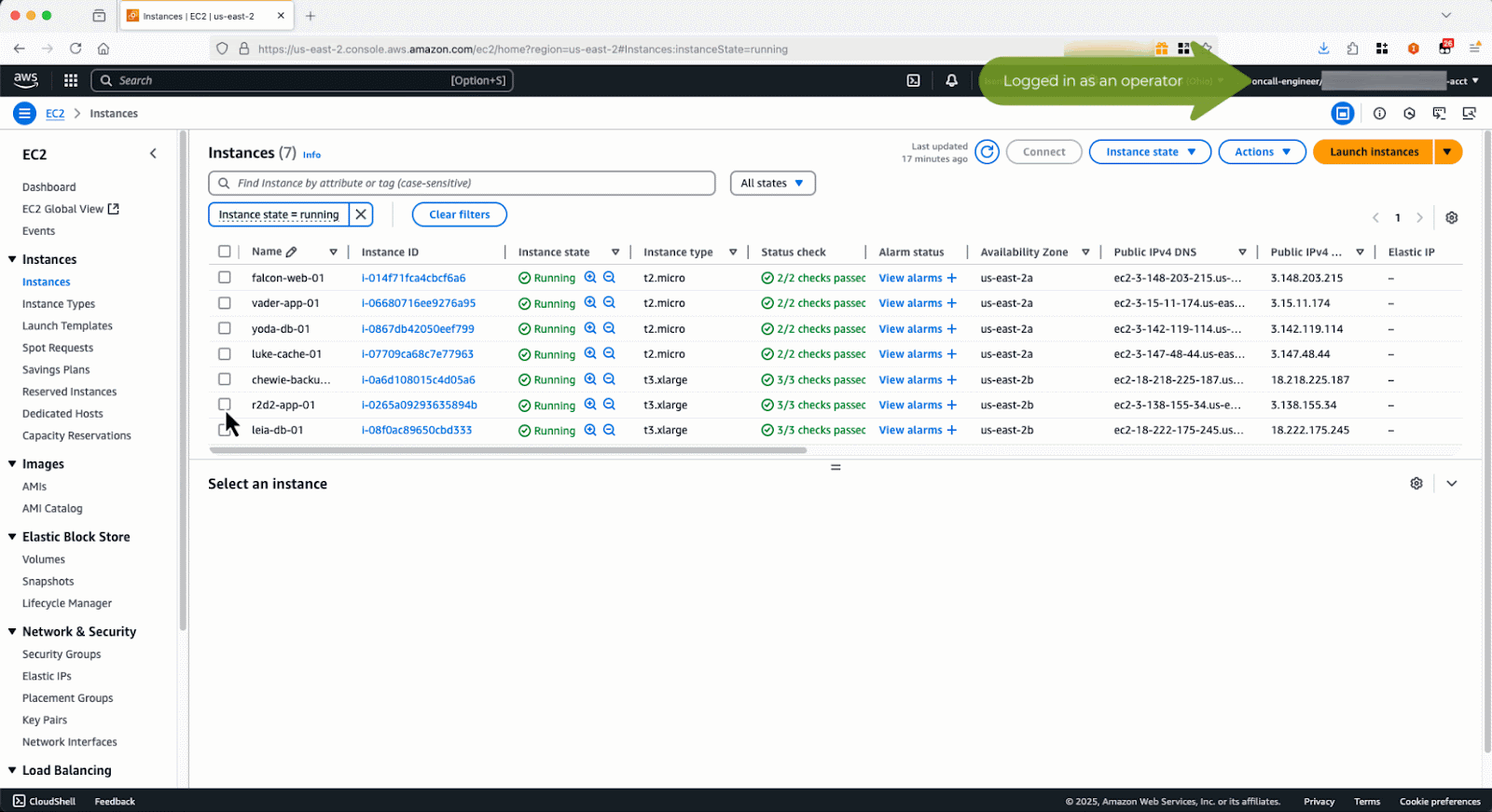
    resource.getTag("Environment") == "Development"

  };

tuyết tùng

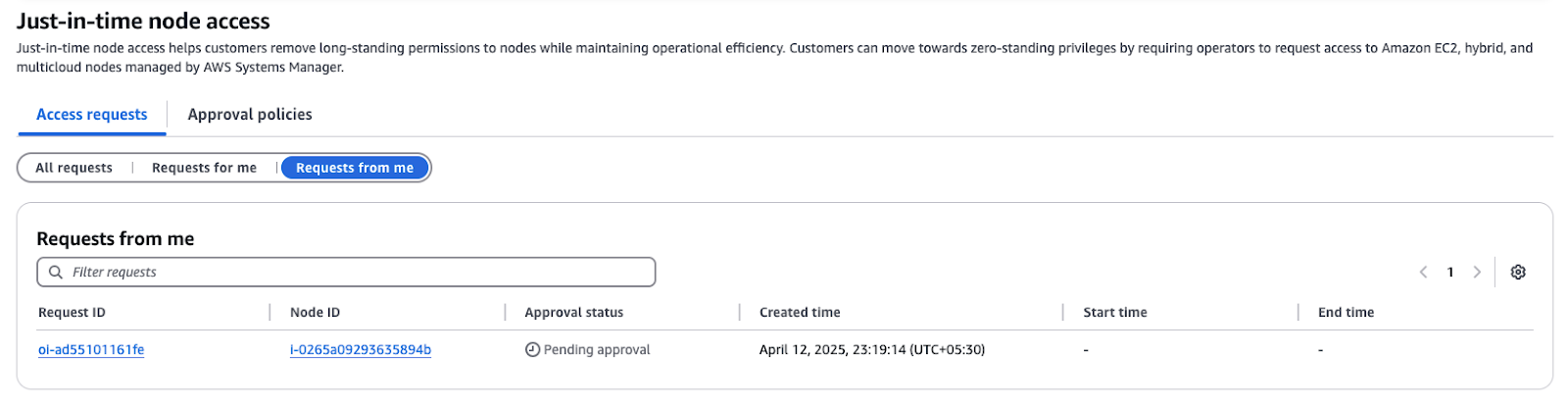
## **Yêu cầu quyền truy cập với tư cách là Người vận hành**

Khi bạn cần truy cập vào một nút được bảo vệ với tư cách là người vận hành, bạn sẽ thấy một quy trình yêu cầu được sắp xếp hợp lý. Thay vì truy cập ngay lập tức, bạn sẽ được nhắc gửi yêu cầu truy cập khi cố gắng kết nối thông qua Trình quản lý phiên. Bạn sẽ cần cung cấp lý do chính đáng cho việc truy cập như thể hiện trong hình 6.



*Hình 6: Người vận hành đưa ra yêu cầu truy cập vào nút*

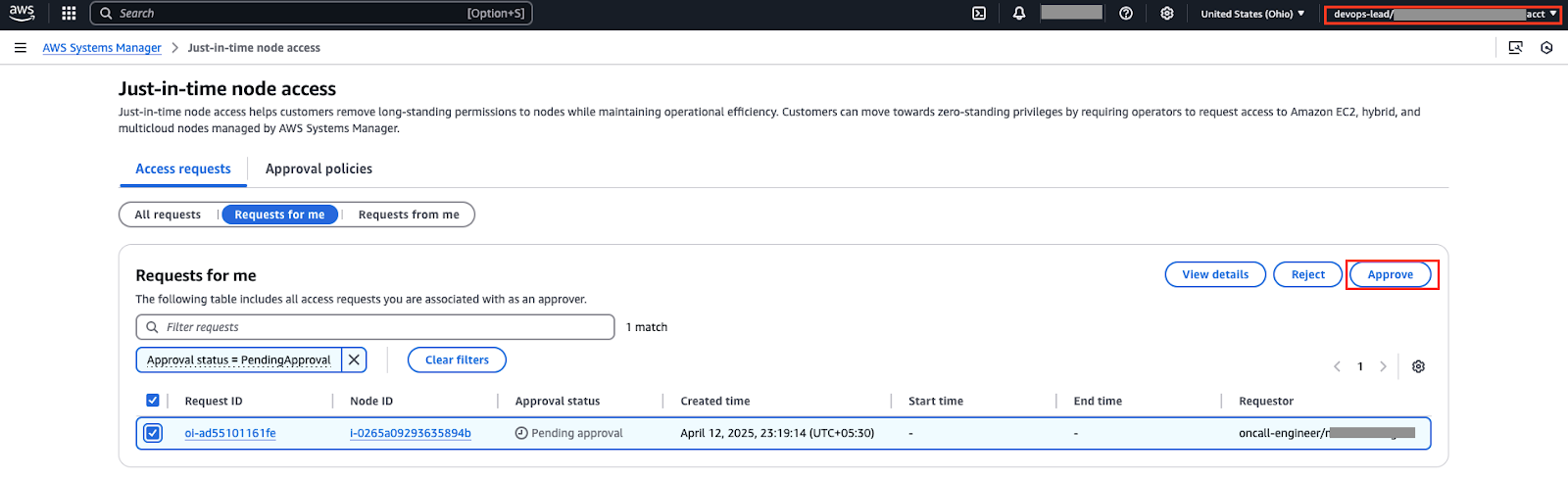
Sau khi gửi yêu cầu, bạn có thể theo dõi trạng thái của yêu cầu thông qua tab Yêu cầu truy cập như thể hiện trong hình 7. Bạn sẽ có thể theo dõi yêu cầu của mình thông qua quy trình phê duyệt và biết chính xác thời điểm bạn có thể truy cập. Bạn sẽ nhận được thông báo qua kênh liên lạc ưa thích của mình, có thể là email, Slack, Microsoft Teams hoặc một nền tảng tích hợp khác. Để biết thêm thông tin, hãy xem [Cấu hình thông báo cho các yêu cầu truy cập đúng lúc](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-just-in-time-node-access-notifications.html) .



*Hình 7: Danh sách trang yêu cầu truy cập*

## **Quản lý phê duyệt**

Với tư cách là người phê duyệt, bạn sẽ nhận được thông báo về các yêu cầu truy cập đang chờ xử lý thông qua kênh thông báo đã cấu hình của mình. Bạn có thể lập trình phê duyệt các yêu cầu bằng [Giao diện dòng lệnh AWS](https://aws.amazon.com/cli/) (AWS CLI) hoặc [SDK](https://aws.amazon.com/developer/tools/) ưa thích của bạn . Hoặc bạn có thể xem xét các yêu cầu này trong bảng điều khiển Systems Manager trong tab Yêu cầu cho tôi như thể hiện trong hình 8.

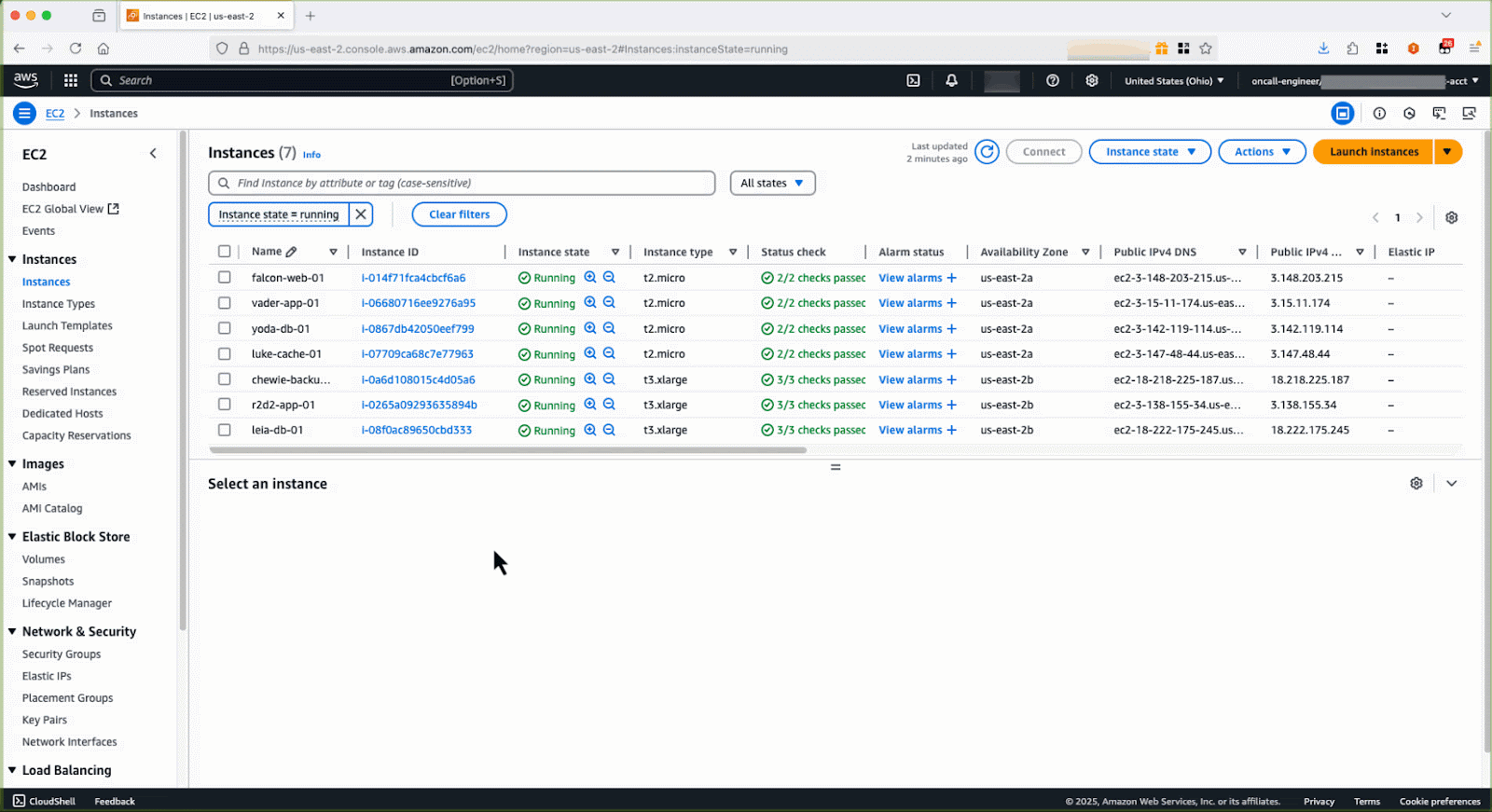


*Hình 8: Danh sách các yêu cầu truy cập đang chờ phê duyệt*

Sau khi xem xét yêu cầu, bạn có thể chấp thuận hoặc từ chối yêu cầu và tùy ý thêm bình luận liên quan đến quyết định.

## **Hoàn tất chu kỳ truy cập**

Khi yêu cầu được chấp thuận, với tư cách là người vận hành, bạn sẽ nhận được thông báo rằng quyền truy cập của bạn đã được cấp. Sau đó, bạn có thể kết nối với nút bằng bảng điều khiển AWS Management hoặc AWS CLI trong thời gian trong chính sách chấp thuận như thể hiện trong hình 9.



*Hình 9: Người vận hành truy cập vào nút được quản lý*

## **Phần kết luận**

Trong blog này, chúng tôi đã giới thiệu về [just-in-time node access](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-just-in-time-node-access.html) , một khả năng mới trong AWS Systems Manager. Just-in-time node access giải quyết thách thức cân bằng hiệu quả hoạt động với các yêu cầu bảo mật bằng cách loại bỏ các đặc quyền thường trực trong khi vẫn đảm bảo truy cập nhanh chóng vào các nút Amazon EC2, on-premises và multicloud. Thông qua phương pháp tiếp cận dựa trên chính sách linh hoạt và hỗ trợ cho cả phê duyệt thủ công và tự động, giờ đây bạn có thể triển khai các đặc quyền thường trực bằng không mà không ảnh hưởng đến khả năng hoạt động.

Systems Manager cung cấp bản dùng thử miễn phí quyền truy cập nút đúng lúc, cho phép bạn khám phá và đánh giá đầy đủ tính năng này cho tổ chức của mình.

Để tìm hiểu thêm, hãy xem [Truy cập nút kịp thời bằng Systems Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-just-in-time-node-access.html) để biết thêm chi tiết.

Hãy xem [bản demo tương tác](https://aws-cloudops.storylane.io/share/qazsu1mgqiho) này để có cái nhìn trực quan đầy đủ về trải nghiệm truy cập nút đúng lúc.



### Chetan Makvana

Chetan Makvana là Kiến trúc sư Giải pháp Doanh nghiệp tại Amazon Web Services. Anh giúp khách hàng doanh nghiệp thiết kế giải pháp cấp doanh nghiệp có khả năng mở rộng, linh hoạt, bảo mật và tiết kiệm chi phí bằng cách sử dụng dịch vụ AWS. Anh là người đam mê công nghệ và là nhà xây dựng với lĩnh vực cốt lõi là trí tuệ nhân tạo, không cần máy chủ, hiện đại hóa ứng dụng và DevOps. Ngoài công việc, anh thích xem phim, du lịch và âm nhạc.



### Đánh dấu Brealey

Mark Brealey là Kiến trúc sư Giải pháp Di chuyển Cao cấp, ông trao quyền cho các đối tác xây dựng kiến trúc đám mây mạnh mẽ, an toàn và hiệu quả. Ông chuyên thiết kế các giải pháp có thể mở rộng giúp các tổ chức tối đa hóa cơ sở hạ tầng AWS của họ đồng thời đảm bảo sự xuất sắc trong hoạt động.



### Anthony Verleysen

Anthony Verleysen là Trưởng phòng sản phẩm – Kỹ thuật (Dịch vụ bên ngoài) trong nhóm AWS Systems Manager. Anh tập trung vào khả năng quản lý nút. Ngoài công việc, Anthony là một cầu thủ bóng đá và quần vợt nhiệt thành.

THẺ: [AWS System Manager](https://aws.amazon.com/blogs/mt/tag/aws-system-manager/) , [Bảo mật](https://aws.amazon.com/blogs/mt/tag/security/)