# **Trao quyền cho các Đối tác AWS mở rộng nền tảng của họ trên toàn cầu**



Tăng trưởng quốc tế đại diện cho tiềm năng to lớn đối với [Amazon Web Services (AWS)](https://aws.amazon.com/) Partners. [Theo Gartner](https://www.gartner.com/en/documents/6302015#:~:text=In%202025%2C%20organizations%20will%20keep,AI%20workloads%20and%20enterprise%20modernization.) ®, thị trường [phần mềm dưới dạng dịch vụ (SaaS)](https://aws.amazon.com/what-is/saas/) toàn cầu dự kiến ​​sẽ đạt 286 tỷ đô la vào năm 2025 và "dự kiến ​​sẽ tăng trưởng ở mức CAGR 15,5% từ năm 2024 đến năm 2029".

Bài đăng này đề cập đến các cân nhắc kỹ thuật dành cho các đối tác mở rộng dịch vụ của họ sang các khu vực địa lý mới và giải thích cách AWS có thể hỗ trợ. Mặc dù chúng tôi tập trung vào các nền tảng SaaS, một phần nội dung cũng áp dụng cho tất cả các dịch vụ được lưu trữ trên toàn cầu.

Có một số lý do thuyết phục khiến các đối tác mở rộng nền tảng của mình trên toàn cầu, bao gồm:

1. Tuân thủ quy định : Nhiều ngành công nghiệp—đặc biệt là chính phủ, chăm sóc sức khỏe và tài chính—có luật bản địa hóa dữ liệu nghiêm ngặt yêu cầu dữ liệu phải được lưu trữ và xử lý trong phạm vi biên giới quốc gia. Việc mở rộng sang [các Vùng AWS](https://aws.amazon.com/about-aws/global-infrastructure/regions_az/) mới cho phép các đối tác đáp ứng các yêu cầu quy định này và khai thác các thị trường trước đây không thể tiếp cận.
2. Cải thiện hiệu suất và trải nghiệm của người dùng : Bằng cách triển khai các dịch vụ gần hơn với người dùng cuối, các đối tác có thể giảm độ trễ và cải thiện khả năng phản hồi của ứng dụng cũng như sự hài lòng của người dùng.
3. Đảm bảo chủ quyền dữ liệu : Khi chính phủ và doanh nghiệp ngày càng quan tâm đến chủ quyền dữ liệu, việc có sự hiện diện tại địa phương chứng tỏ cam kết bảo vệ dữ liệu và có thể là yếu tố khác biệt quan trọng trong việc giành được hợp đồng.

Mỗi quốc gia hoặc khu vực pháp lý có các yêu cầu tuân thủ riêng biệt xung quanh nơi lưu trú dữ liệu, kiểm soát hoạt động và bảo mật ( [chủ quyền kỹ thuật số](https://aws.amazon.com/compliance/digital-sovereignty/) ). Những yêu cầu này thường thúc đẩy các nhà cung cấp SaaS phải xem xét lại kiến ​​trúc của họ: cách họ quản lý lưu trữ, cách họ lưu trữ và xử lý dữ liệu và cách họ triển khai kiểm soát truy cập và bảo mật. Điều này có thể yêu cầu các nhà cung cấp triển khai các mặt phẳng kiểm soát có chủ quyền thay vì mặt phẳng kiểm soát toàn cầu hoặc áp dụng các phương pháp mã hóa cụ thể.

Trong bài đăng này, chúng tôi thảo luận về sáu chiến lược chính có thể trao quyền cho các đối tác để phát triển phương pháp tiếp cận có cấu trúc nhằm mở rộng trong khi vẫn đáp ứng các yêu cầu tuân thủ:

1. Sử dụng AWS Global Infrastructure
2. Phối hợp với AWS về khả năng cung cấp và năng lực dịch vụ
3. Thiết kế kiến ​​trúc nền tảng linh hoạt
4. Quản lý truyền thông liên vùng hiệu quả
5. Thực hiện bảo mật và mã hóa một cách nhất quán
6. Điều hướng các yêu cầu tuân thủ và tự động hóa việc thu thập bằng chứng

## **1) Sử dụng AWS Global Infrastructure**

[AWS Global Infrastructure](https://aws.amazon.com/about-aws/global-infrastructure/) bao gồm Regions, sovereign Regions, [AWS Local Zones](https://aws.amazon.com/about-aws/global-infrastructure/localzones/) , [AWS Dedicated Local Zones](https://aws.amazon.com/dedicatedlocalzones/) và [AWS Outposts](https://aws.amazon.com/outposts/) . Mỗi tùy chọn này cung cấp cho bạn các khả năng độc đáo để đáp ứng các nhu cầu đa dạng của khách hàng. AWS Regions và sovereign Regions cung cấp một bộ dịch vụ rộng, trong khi Local Zones, Dedicated Local Zones và Outposts cung cấp một tập hợp con các dịch vụ. Local Zones và Outposts cũng khả dụng ở các quốc gia không có AWS Regions.

Với tư cách là đối tác, khả năng triển khai phiên bản nền tảng của bạn trên Local Zone hoặc Outposts có thể giúp bạn tiếp cận nhiều khách hàng hơn bằng cách đáp ứng các yêu cầu về chủ quyền dữ liệu trong khi sử dụng giao diện AWS quen thuộc. Điều này cũng có thể cho phép bạn triển khai thử nghiệm cho đến khi AWS Region được ra mắt.

AWS [European Sovereign Cloud](https://aws.amazon.com/compliance/europe-digital-sovereignty/) , dự kiến ​​ra mắt vào cuối năm 2025, sẽ cung cấp cho các đối tác khả năng đáp ứng các yêu cầu nghiêm ngặt về quyền tự chủ hoạt động và lưu trữ dữ liệu trong các ngành được quản lý chặt chẽ. Cơ sở hạ tầng cho đám mây này hoàn toàn nằm trong Liên minh Châu Âu (EU) và được vận hành độc lập với các Khu vực hiện có.

## **2) Phối hợp với AWS về khả năng cung cấp và năng lực dịch vụ**

Khi lập kế hoạch triển khai nền tảng của bạn tại một Khu vực mới, bạn nên cân nhắc một số điểm.

Trước tiên, bạn nên xem xét các yêu cầu dịch vụ AWS của mình so với [danh sách Dịch vụ AWS theo Khu vực](https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/) và các yêu cầu mô hình AI tạo ra của bạn so với [hỗ trợ mô hình theo Khu vực AWS trong Amazon Bedrock](https://docs.aws.amazon.com/bedrock/latest/userguide/models-regions.html) . Các Khu vực mới ra mắt với một [bộ dịch vụ cốt lõi](https://aws.amazon.com/about-aws/global-infrastructure/regions_az/) (được liệt kê trong Dịch vụ trong Lợi ích ) cần thiết cho hầu hết các khối lượng công việc, cung cấp nền tảng vững chắc cho việc triển khai. Sau khi ra mắt, chúng tôi tiếp tục cung cấp các dịch vụ bổ sung dựa trên nhu cầu, cải thiện tính đồng đều giữa các Khu vực.

Thứ hai, bạn nên xác định mức độ phụ thuộc vào nền tảng và API của bên thứ ba do các đối tác khác cung cấp, có thể cần phải có sẵn trong Khu vực trước khi bạn có thể triển khai nền tảng của mình.

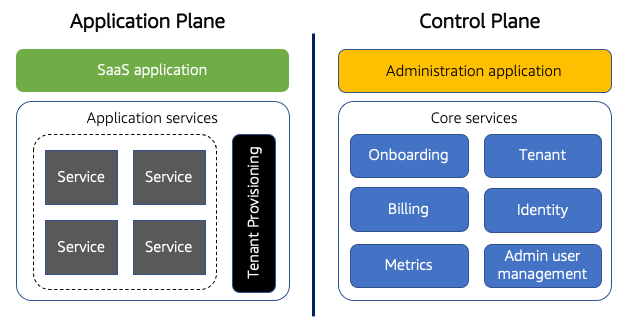
Nếu bạn có nhiều nền tảng, bạn nên xác định thứ tự cung cấp các nền tảng đó dựa trên nhu cầu của khách hàng.

Dựa trên những điều này, chúng tôi có thể làm việc với bạn về mốc thời gian để cung cấp nền tảng của bạn trong Khu vực. Trong trường hợp có sự phụ thuộc vào dịch vụ AWS hoặc nền tảng Đối tác AWS không khả dụng hoặc có yêu cầu về năng lực lớn, bạn nên sớm liên hệ với nhóm tài khoản AWS của mình để chúng tôi có thể nắm bắt nhu cầu và cung cấp hướng dẫn.

Đối với các dịch vụ chưa có sẵn trong một Khu vực, bạn có thể cân nhắc các giải pháp tạm thời về mặt kiến ​​trúc hoặc các dịch vụ thay thế cung cấp chức năng tương tự. Điều này có thể bao gồm sử dụng quyền truy cập liên Khu vực khi phù hợp và tuân thủ, đồng thời lập kế hoạch cải tiến dần dần khi các dịch vụ có sẵn trong Khu vực.

## **3) Thiết kế kiến ​​trúc nền tảng linh hoạt**

Các đối tác thường thiết kế nền tảng của họ thành SaaS đa thuê bao để có [tính linh hoạt và hiệu quả hoạt động](https://docs.aws.amazon.com/whitepapers/latest/saas-architecture-fundamentals/saas-is-a-business-model.html) . Trong mô hình SaaS, một nền tảng có [một mặt phẳng điều khiển và một mặt phẳng ứng dụng](https://docs.aws.amazon.com/whitepapers/latest/saas-architecture-fundamentals/control-plane-vs.-application-plane.html) . Mặt phẳng điều khiển dành cho các tác vụ như quản lý thuê bao và đưa khách hàng mới lên tàu, và thường chỉ chứa siêu dữ liệu chứ không phải dữ liệu khách hàng thực tế. Mặt phẳng ứng dụng là nơi dữ liệu khách hàng được lưu trữ và xử lý. Sơ đồ sau đây cho thấy mô hình SaaS đa thuê bao này.



*Hình 1. Sơ đồ hiển thị mô hình SaaS đa thuê bao*

Bạn có thể đã thiết kế mặt phẳng điều khiển của mình để tập trung, trong khi mặt phẳng ứng dụng có thể được triển khai trong một Khu vực dựa trên các yêu cầu về nơi lưu trú dữ liệu của khách hàng. Mặt phẳng điều khiển có thể là toàn cầu, ví dụ, trong một Khu vực Hoa Kỳ hoặc có thể là Khu vực, ví dụ, trong một Khu vực EU. Miễn là mặt phẳng điều khiển không lưu trữ dữ liệu khách hàng thực tế và bị giới hạn ở siêu dữ liệu liên quan đến việc triển khai, thì điều này có thể đáp ứng các yêu cầu của hầu hết khách hàng. Tuy nhiên, trong các ngành được quản lý chặt chẽ, có thể có yêu cầu phải có mặt phẳng điều khiển có chủ quyền, được triển khai trong Khu vực nơi có dữ liệu khách hàng. Việc lựa chọn kiến ​​trúc phụ thuộc vào các yêu cầu theo quy định, nhu cầu của khách hàng và các tiêu chuẩn của ngành.

Một cân nhắc thiết kế quan trọng khác trong mô hình SaaS là [​​cô lập người thuê](https://docs.aws.amazon.com/whitepapers/latest/saas-tenant-isolation-strategies/saas-tenant-isolation-strategies.html) . Có nhiều cách để đạt được điều này: mô hình silo, mô hình nhóm và mô hình cầu nối. Mô hình silo là nơi mỗi người thuê chạy một ngăn xếp tài nguyên được cô lập hoàn toàn. Trong mô hình nhóm, người thuê sử dụng cơ sở hạ tầng được chia sẻ bởi tất cả người thuê. Mô hình cầu nối là sự kết hợp của mô hình silo và mô hình nhóm.

Mô hình silo có thể được yêu cầu bởi những khách hàng được quản lý chặt chẽ, trong khi mô hình nhóm cung cấp hiệu quả và tối ưu hóa. Trong mô hình silo cũng có nhiều cách khác nhau để thực hiện cô lập, từ việc có các tài khoản AWS riêng biệt đến [Amazon Virtual Private Cloud (VPC)](https://aws.amazon.com/vpc/) riêng biệt đến các mạng con riêng biệt. Kết hợp tất cả những điều này, cô lập theo tầng cung cấp các loại cô lập khác nhau cho các đối tượng thuê khác nhau với các cấu hình khác nhau, cho phép linh hoạt trong việc đáp ứng các yêu cầu riêng biệt.

[Tenant Onboarding Best Practices in SaaS](https://aws.amazon.com/blogs/apn/tenant-onboarding-best-practices-in-saas-with-the-aws-well-architected-saas-lens/) bao gồm cách quản lý việc onboarding của người thuê trong mô hình theo tầng. Ngoài ra, [mô hình triển khai theo ô](https://www.youtube.com/watch?v=wYm_PJc2U8c) có thể giúp giải quyết những phức tạp phát sinh từ điều này.

Để hỗ trợ các đối tác trong việc điều hướng các quyết định về kiến ​​trúc này và triển khai các giải pháp linh hoạt, tuân thủ, AWS cung cấp [Chương trình SaaS Factory](https://aws.amazon.com/partners/programs/saas-factory/?saas-factory-cards.sort-by=item.additionalFields.sortOrder&saas-factory-cards.sort-order=asc&awsf.saas-factory-featured=*all&awsf.saas-factory-role=*all&awsf.saas-factory-category=*all&awsf.saas-factory-content=*all&awsf.saas-factory-learning-level=*all) . Chương trình này giúp các đối tác ở bất kỳ giai đoạn nào trong hành trình của họ, cho dù bạn muốn xây dựng các dịch vụ mới, di chuyển các ứng dụng hiện có hay tối ưu hóa nền tảng SaaS trên AWS.

Bên cạnh mô hình phân phối SaaS, bạn có thể cân nhắc các phương pháp phân phối khác như [Amazon Machine Image](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html) hoặc hình ảnh container thông qua [Amazon Marketplace](https://aws.amazon.com/marketplace) có thể giúp bạn thâm nhập thị trường nhanh hơn cho đến khi bạn cung cấp phiên bản SaaS. Những phương pháp này cũng có thể giúp triển khai dễ dàng hơn trên Local Zone hoặc Outposts.

## **4) Quản lý truyền thông liên vùng hiệu quả**

Khi các nhà cung cấp SaaS mở rộng trên toàn cầu, giao tiếp giữa các khu vực cần được chú ý đặc biệt. Điều này xuất phát từ hai thách thức quan trọng: cân bằng nhu cầu tuân thủ các yêu cầu về lưu trú dữ liệu trong khi vẫn mang lại trải nghiệm nhất quán, hiệu suất cao cho tất cả người dùng của họ.

Khi thiết kế các chiến lược truyền thông liên khu vực, nhà cung cấp cần cân nhắc nhiều khía cạnh của kiến ​​trúc của họ:

* Cách các thành phần khác nhau của nền tảng SaaS giao tiếp giữa các Vùng, đặc biệt là giữa các mặt phẳng điều khiển và mặt phẳng ứng dụng.
* Cách triển khai các chiến lược sao lưu và sao chép dữ liệu tôn trọng ranh giới khu vực.
* Làm thế nào để tương tác hiệu quả với các hệ thống bên ngoài trên nhiều khu vực địa lý khác nhau.

Hiểu phạm vi dịch vụ AWS là rất quan trọng đối với kiến ​​trúc liên vùng hiệu quả. Các dịch vụ AWS hoạt động ở ba cấp độ khác nhau: [dịch vụ vùng](https://docs.aws.amazon.com/whitepapers/latest/aws-fault-isolation-boundaries/zonal-services.html) trong các Vùng khả dụng cụ thể, [dịch vụ Vùng](https://docs.aws.amazon.com/whitepapers/latest/aws-fault-isolation-boundaries/regional-services.html) trong một Vùng AWS và [dịch vụ toàn cầu](https://docs.aws.amazon.com/whitepapers/latest/aws-fault-isolation-boundaries/global-services.html) hoạt động trên nhiều Vùng. Ví dụ: [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/ec2/) là vùng, [Amazon Simple Storage Service (Amazon S3)](https://aws.amazon.com/s3/) là Vùng và [Amazon CloudFront](https://aws.amazon.com/cloudfront/) là toàn cầu. Sự hiểu biết này giúp các kiến ​​trúc sư đưa ra quyết định sáng suốt về việc bố trí dịch vụ và các mẫu giao tiếp liên vùng.

### **Truyền thông trong nền tảng SaaS**

Những thông tin liên lạc này thường thuộc hai loại: quản lý nền tảng và hoạt động liên quan đến người thuê, đồng thời yêu cầu cân nhắc cẩn thận về việc xử lý dữ liệu người thuê.

Khi sử dụng kiến ​​trúc mặt phẳng điều khiển tập trung, giao tiếp liên vùng trở nên thiết yếu đối với các hoạt động quản lý đối tượng thuê. Mặt phẳng điều khiển cần tương tác với các mặt phẳng ứng dụng trên khắp các vùng để thực hiện các tác vụ như cung cấp đối tượng thuê, quản lý cấu hình và theo dõi tình trạng. Những tương tác này thường liên quan đến siêu dữ liệu hơn là dữ liệu đối tượng thuê, cho phép tối ưu hóa thông qua các dịch vụ như [AWS Global Accelerator](https://aws.amazon.com/global-accelerator/) và Amazon CloudFront.

Đối với các nền tảng SaaS xử lý dữ liệu của người thuê, giao tiếp liên vùng phải tôn trọng các yêu cầu về nơi lưu trú dữ liệu. Điều này có nghĩa là giữ cho việc xử lý dữ liệu của người thuê trong Vùng được chỉ định và chỉ giới hạn việc truyền dữ liệu liên vùng cho các hoạt động thiết yếu. Nhà cung cấp phải thực hiện các biện pháp kiểm soát chặt chẽ về thời điểm và cách dữ liệu của người thuê có thể vượt qua ranh giới Vùng. Ví dụ, dữ liệu của người thuê EU thường phải được xử lý và lưu trữ trong các Vùng EU, với giao tiếp liên vùng giới hạn ở các trao đổi siêu dữ liệu cần thiết với mặt phẳng điều khiển.

### **Sao chép và sao lưu liên vùng**

Trong khi duy trì chủ quyền dữ liệu, các nhà cung cấp SaaS cũng phải cung cấp độ bền dữ liệu, tính liên tục của dịch vụ và khả năng phục hồi sau thảm họa. Điều này thường liên quan đến sao chép và sao lưu liên vùng, phải được thiết kế để tuân thủ các yêu cầu về lưu trú dữ liệu. AWS cung cấp một số dịch vụ vốn cung cấp sao chép liên vùng như [Amazon Aurora Global Database](https://aws.amazon.com/rds/aurora/global-database/) , [Amazon DynamoDB](https://aws.amazon.com/dynamodb/) và [Amazon S3 Cross-Region Replication (CRR)](https://aws.amazon.com/s3/features/replication/) . Danh sách các dịch vụ cung cấp khả năng đa vùng khác có thể được tìm thấy tại [AWS Multi-Region Capabilities](https://repost.aws/articles/AR02pJIdoARYKX6Rhkdra-Zg/aws-multi-region-capabilities) .

### **Tương tác với các hệ thống bên ngoài**

Các nền tảng SaaS thường cần tương tác với API của bên thứ ba hoặc các dịch vụ bên ngoài, có thể nằm ở các khu vực địa lý khác nhau. Để duy trì hiệu suất và sự tuân thủ:

* Triển khai Cổng API khu vực để quản lý các lệnh gọi API bên ngoài. Ví dụ: dữ liệu của người thuê EU phải tương tác với điểm cuối EU của bộ xử lý thanh toán thông qua Cổng API được triển khai trong Khu vực EU thay vì định tuyến qua Khu vực Hoa Kỳ.
* Sử dụng [AWS PrivateLink](https://aws.amazon.com/privatelink/) để kết nối an toàn, riêng tư với các dịch vụ của bên thứ ba. Đối với kết nối mạng của khách hàng, hãy cân nhắc các tùy chọn như [AWS Direct Connect](https://aws.amazon.com/directconnect/) cho các kết nối riêng chuyên dụng, [AWS Site-to-Site VPN](https://aws.amazon.com/vpn/site-to-site-vpn/) cho các kết nối internet được mã hóa, [AWS Transit Gateway](https://aws.amazon.com/transit-gateway/) để quản lý mạng tập trung hoặc VPC Peering để giao tiếp trực tiếp từ VPC đến VPC.
* Đảm bảo việc chuyển đổi dữ liệu hoặc ẩn danh diễn ra trước khi chuyển dữ liệu giữa các khu vực khi cần thiết.

### **Cân nhắc về hiệu suất**

Hiệu suất trong triển khai SaaS xuyên vùng phải tính đến nhu cầu cụ thể của từng đối tượng thuê. Chúng tôi khuyên bạn nên tập trung vào các biện pháp thực hành tốt nhất sau:

* Áp dụng các chiến lược định tuyến lưu lượng mạng phù hợp với từng đối tượng thuê bao, hướng dẫn người dùng đến khu vực triển khai phù hợp dựa trên yêu cầu của họ.
* Bất cứ khi nào có thể, hãy xử lý dữ liệu của người thuê trong Vùng được chỉ định của họ để duy trì sự tuân thủ và tối ưu hóa hiệu suất. Lưu ý rằng siêu dữ liệu cũng có thể chứa dữ liệu có yêu cầu về nơi lưu trú dữ liệu.
* Triển khai bộ nhớ đệm siêu dữ liệu hiệu quả để giảm thiểu các cuộc gọi liên vùng không cần thiết đến mặt phẳng điều khiển.
* Thiết lập giám sát toàn diện các số liệu cụ thể của từng đối tượng thuê để đảm bảo bạn đáp ứng các yêu cầu về hiệu suất và SLA trên khắp các Khu vực.

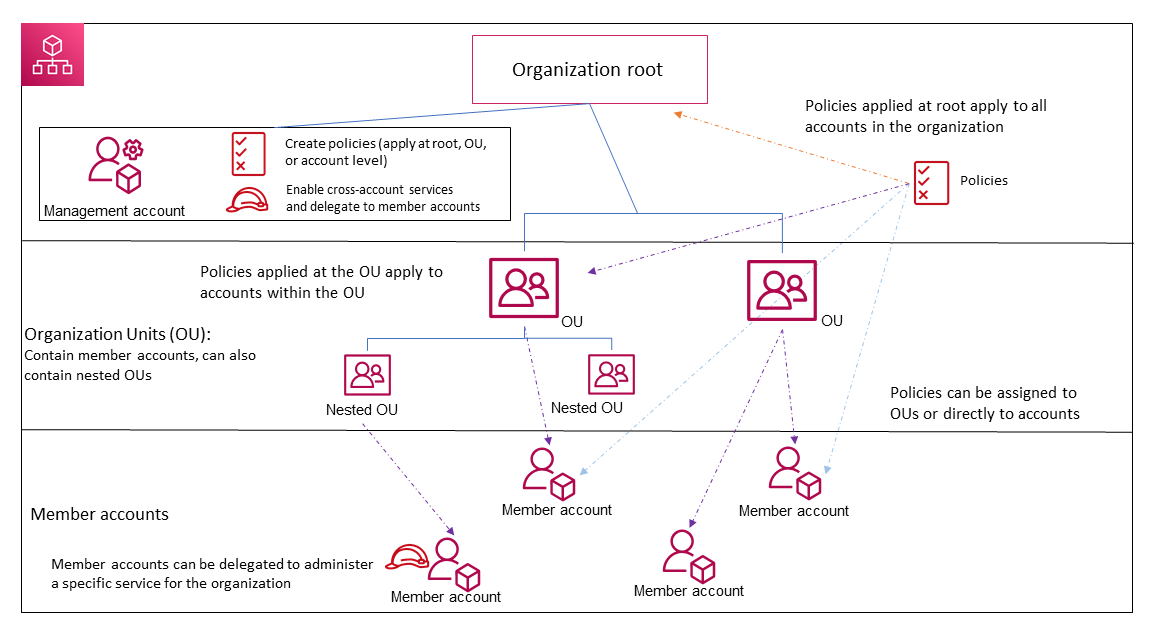
Để biết thêm hướng dẫn về việc xây dựng kiến ​​trúc SaaS đa vùng, hãy tham khảo [Kiến trúc giải pháp SaaS đa vùng trên AWS](https://aws.amazon.com/blogs/apn/architecting-multi-region-saas-solutions-on-aws/) .

## **5) Thực hiện bảo mật và mã hóa một cách nhất quán**

Khi mở rộng nền tảng SaaS trên nhiều Vùng, kiến ​​trúc bảo mật có thể trở nên ngày càng phức tạp. Hãy cùng khám phá cách duy trì trạng thái bảo mật mạnh mẽ trong khi quản lý hiệu quả các triển khai đa Vùng.

Chiến lược quản lý danh tính và truy cập (IAM) có cấu trúc tốt là rất quan trọng đối với các hoạt động SaaS đa vùng. [AWS Control Tower](https://aws.amazon.com/controltower/) và [landing zone](https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-aws-environment/understanding-landing-zones.html) cung cấp nền tảng cho quản trị đa tài khoản, đặc biệt có giá trị khi mở rộng trên toàn cầu. Ví dụ: bạn có thể thiết lập các tài khoản riêng cho môi trường phát triển, dàn dựng và sản xuất trong mỗi vùng, với sự cô lập bổ sung cho bảo mật, kiểm tra, ghi nhật ký và khối lượng công việc nhạy cảm với tuân thủ. Sử dụng [AWS Organizations](https://aws.amazon.com/organizations/) với [chính sách kiểm soát dịch vụ (SCP)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html) , bạn có thể thực thi ranh giới bảo mật không chỉ trên các vùng mà còn trên các tài khoản chức năng này. Chiến lược đa tài khoản này, kết hợp với việc cung cấp tài khoản tự động và các rào cản của landing zone, giúp duy trì các biện pháp kiểm soát bảo mật nhất quán khi bạn mở rộng quy mô. Đối với quản lý truy cập tập trung, [AWS IAM Identity Center](https://aws.amazon.com/iam/identity-center/) tích hợp với cấu trúc này để cung cấp quyền truy cập hợp lý cho người dùng trong khi vẫn duy trì bảo mật. Ví dụ: bạn có thể thực thi xác thực đa yếu tố (MFA) cho tất cả quyền truy cập quản trị và triển khai thu hồi quyền tự động cho người dùng không hoạt động trên tất cả các tài khoản và vùng.

Sơ đồ sau đây minh họa cấu trúc tổ chức có nhiều tài khoản.



*Hình 2. Sơ đồ thể hiện cấu trúc tổ chức nhiều tài khoản*

Khi thiết kế kiến ​​trúc mạng, bạn cần cân nhắc cẩn thận khả năng kết nối liên vùng. Thay vì quản lý nhiều VPC bị ngắt kết nối, bạn có thể sử dụng [AWS Transit Gateway](https://aws.amazon.com/transit-gateway/) với tính năng liên vùng để tạo kiến ​​trúc mạng toàn cầu. Điều này có nghĩa là bạn có thể duy trì các biện pháp kiểm soát bảo mật nhất quán trong khi vẫn đáp ứng các yêu cầu về vị trí dữ liệu. Bạn có thể định cấu hình bảng định tuyến để dữ liệu của đối tượng thuê chỉ được xử lý trong các dịch vụ cục bộ của vùng, đồng thời cho phép truy cập quản trị toàn cầu thông qua mặt phẳng điều khiển.

AWS cung cấp nhiều tùy chọn mã hóa để đáp ứng các yêu cầu tuân thủ khác nhau. Mặc dù [AWS Key Management Services (AWS KMS)](https://aws.amazon.com/kms/) với khóa khu vực hoạt động cho hầu hết các tình huống, các ngành được quản lý chặt chẽ có thể yêu cầu các biện pháp kiểm soát bổ sung. Đối với những trường hợp này, hãy cân nhắc sử dụng tính năng [lưu trữ khóa bên ngoài](https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html) , cho phép lưu trữ khóa mã hóa bên ngoài AWS trong khi vẫn tích hợp với các dịch vụ AWS. Bạn cũng có thể triển khai khóa mã hóa đa khu vực cho các tình huống yêu cầu sao chép dữ liệu giữa các khu vực trong khi vẫn duy trì kiểm soát chặt chẽ đối với quản lý khóa.

Mỗi khu vực địa lý có thể có các yêu cầu bảo mật riêng. Chúng tôi khuyên bạn nên triển khai các quy tắc [WAF AWS](https://aws.amazon.com/waf/) khu vực phù hợp với các yêu cầu của địa phương, cho phép [Amazon GuardDuty](https://aws.amazon.com/guardduty/) ở mỗi Khu vực có chức năng giám sát tập trung và sử dụng [AWS Security Hub](https://aws.amazon.com/security-hub/) để quản lý tình trạng bảo mật tổng hợp và [AWS Config](https://aws.amazon.com/config/) để theo dõi sự tuân thủ tài nguyên trên khắp các Khu vực.

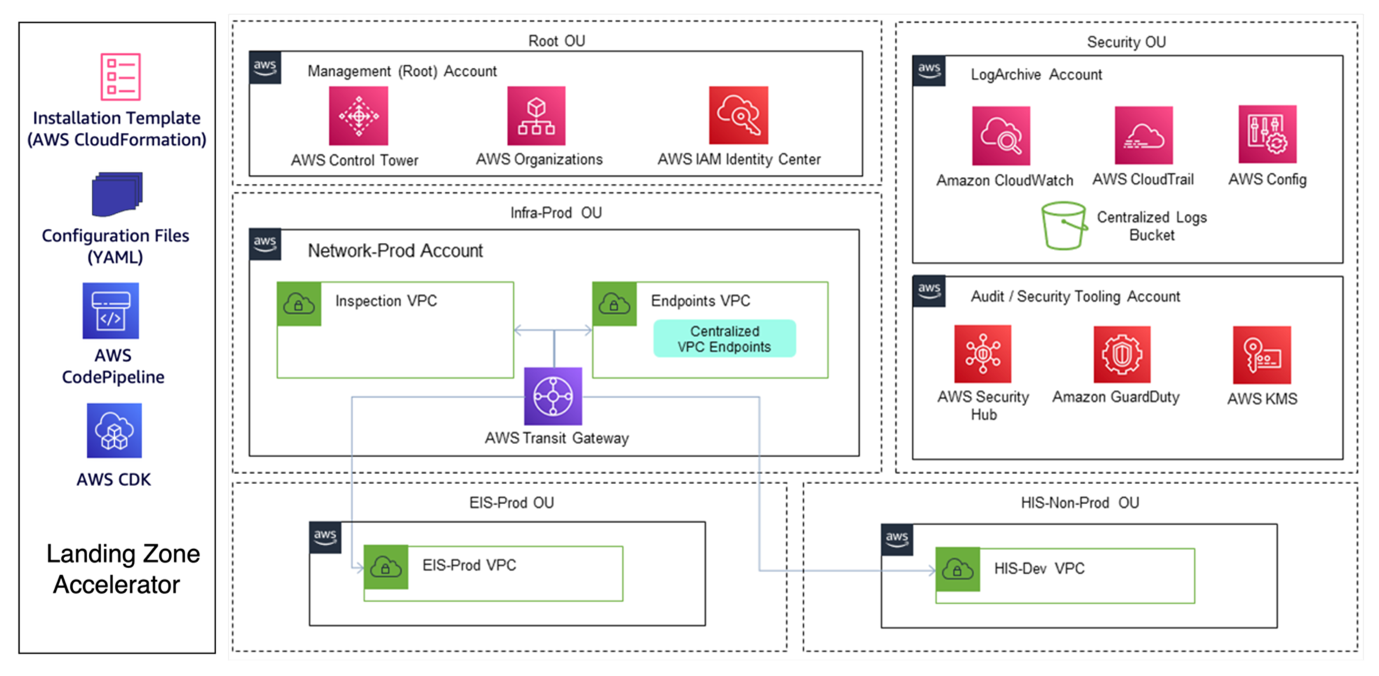
Trong môi trường SaaS đa vùng, việc triển khai đặc quyền tối thiểu trở nên tinh tế hơn. Tạo cấu trúc quyền phân cấp xem xét quyền truy cập quản trị toàn cầu cho các hoạt động nền tảng, quyền truy cập quản trị khu vực cho các hoạt động cục bộ, quyền truy cập dành riêng cho đối tượng thuê trong phạm vi các vùng cụ thể và giao tiếp dịch vụ với dịch vụ trong và giữa các vùng.

Việc quản lý chứng chỉ trên nhiều Vùng đòi hỏi phải lập kế hoạch cẩn thận. [AWS Certificate Manager (ACM)](https://aws.amazon.com/certificate-manager/) cung cấp chứng chỉ Vùng, nhưng bạn sẽ cần tự động hóa quy trình gia hạn chứng chỉ trên nhiều Vùng, triển khai giám sát ngày hết hạn chứng chỉ, duy trì tính nhất quán trong xác thực tên miền và cân nhắc sử dụng [AWS Private Certificate Authority](https://aws.amazon.com/private-ca/) cho các giao tiếp dịch vụ nội bộ.

Ví dụ, nhà cung cấp SaaS chăm sóc sức khỏe có thể sử dụng:

* Khóa AWS KMS khu vực để mã hóa dữ liệu thuê bao tiêu chuẩn
* Kho lưu trữ khóa ngoài dành cho những khách hàng cụ thể yêu cầu quyền sở hữu khóa đầy đủ
* AWS Certificate Manager để quản lý chứng chỉ SSL hoặc TLS khu vực
* AWS Private Certificate Authority cho giao tiếp dịch vụ nội bộ

Sơ đồ sau đây cho thấy kiến ​​trúc của giải pháp [Landing Zone Accelerator trên AWS](https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/) dành cho chăm sóc sức khỏe.



*Hình 3. Sơ đồ hiển thị kiến ​​trúc cho giải pháp Landing Zone Accelerator trên AWS dành cho chăm sóc sức khỏe*

Trong một ví dụ khác, một nền tảng SaaS tài chính có thể triển khai các ranh giới Khu vực, trong đó quyền truy cập dữ liệu của người thuê bị hạn chế đối với các Khu vực cụ thể thông qua sự kết hợp giữa các chính sách [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) , thẻ tài nguyên và các biện pháp kiểm soát mạng. Quyền truy cập quản trị có thể được cấp thông qua AWS IAM Identity Center với yêu cầu xác thực tăng dần cho các hoạt động liên Khu vực.

## **6) Điều hướng các yêu cầu tuân thủ và tự động thu thập bằng chứng**

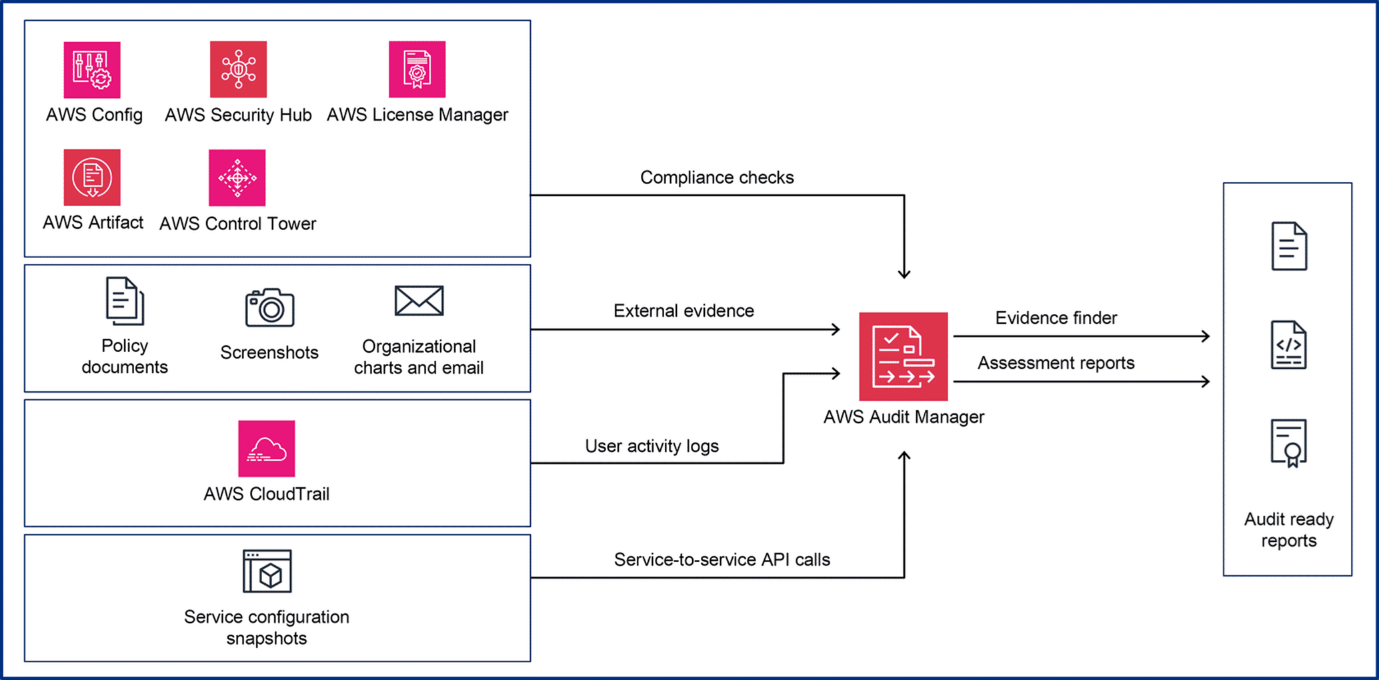
Khi mở rộng sang một quốc gia mới, các đối tác cần phải nhận thức được các yêu cầu tuân thủ và đảm bảo nền tảng và hoạt động của họ đáp ứng các yêu cầu đó. Đáp ứng các yêu cầu này là [trách nhiệm chung](https://aws.amazon.com/compliance/shared-responsibility-model/) giữa AWS, các đối tác và khách hàng. Để biết thông tin về các dịch vụ và chứng nhận của chúng tôi, hãy truy cập [AWS Compliance](https://aws.amazon.com/compliance/) . Để biết báo cáo về bảo mật và tuân thủ, hãy truy cập [AWS Artifact](https://aws.amazon.com/artifact/) .

Chương [trình Tăng tốc Bảo mật & Tuân thủ Toàn cầu trên AWS (GSCA)](https://aws.amazon.com/partners/programs/gsca/) có thể tư vấn cho bạn về các yêu cầu áp dụng cho một quốc gia và ngành cụ thể. Chương trình cũng có thể giới thiệu các đối tác có thể giúp bạn điều hướng và triển khai các thay đổi cần thiết.

AWS có các nhóm quản lý tài khoản địa phương, bao gồm các kiến ​​trúc sư giải pháp và chuyên gia bảo mật, có chuyên môn sâu và kinh nghiệm làm việc với khách hàng trong các ngành được quản lý và có thể chia sẻ kiến ​​thức thực tế để giúp đỡ các đối tác.

Chúng tôi khuyên bạn nên tích hợp các biện pháp kiểm soát chủ quyền và kiểm tra tuân thủ trực tiếp vào quy trình phát triển của mình thay vì coi chúng là các cân nhắc sau khi triển khai. Sử dụng các tính năng như [quy tắc AWS Config](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html) , [AWS CloudFormation Guard](https://docs.aws.amazon.com/cfn-guard/latest/ug/what-is-guard.html) và [các biện pháp kiểm soát tùy chỉnh trong AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/cfct-customizations-dev-guide.html) , bạn có thể tự động hóa xác thực tuân thủ trong suốt vòng đời phát triển. Điều này cho phép bạn đáp ứng các yêu cầu ngay từ những giai đoạn phát triển đầu tiên, giảm nguy cơ không tuân thủ và loại bỏ các nỗ lực khắc phục tốn kém.

Chúng tôi cũng đề xuất tự động hóa việc thu thập bằng chứng bằng các dịch vụ như AWS Config, AWS Security Hub, [AWS License Manager](https://aws.amazon.com/license-manager/) , AWS Artifact, AWS Control Tower và [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) , và sử dụng [AWS Audit Manager](https://aws.amazon.com/audit-manager/) để liên tục kiểm tra việc sử dụng AWS nhằm quản lý rủi ro và tuân thủ các quy định hiệu quả hơn. Kiến trúc này được minh họa trong sơ đồ sau.



*Hình 4. Sơ đồ hiển thị thu thập bằng chứng tự động*

## **Phần kết luận**

Việc mở rộng nền tảng SaaS của bạn sang các khu vực địa lý mới mang đến cả cơ hội và thách thức. Mặc dù bài đăng này đã nêu ra những cân nhắc kỹ thuật quan trọng, nhưng bạn không phải tự mình thực hiện hành trình này. AWS cung cấp hỗ trợ toàn diện thông qua chuyên môn từ các kiến ​​trúc sư giải pháp AWS, chương trình tài trợ, chương trình AWS SaaS Factory và các chuyên gia phát triển đối tác hiểu rõ nhu cầu của thị trường địa phương.

Hãy thực hiện bước đầu tiên hướng tới mở rộng toàn cầu ngay hôm nay. Liên hệ với nhóm tài khoản AWS của bạn để phát triển chiến lược mở rộng tùy chỉnh hoặc [truy cập trang chương trình AWS SaaS Factory](https://aws.amazon.com/partners/programs/saas-factory/?saas-factory-cards.sort-by=item.additionalFields.sortOrder&saas-factory-cards.sort-order=asc&awsf.saas-factory-featured=*all&awsf.saas-factory-role=*all&awsf.saas-factory-category=*all&awsf.saas-factory-content=*all&awsf.saas-factory-learning-level=*all) .



### **Mehmet Bakkaloglu**

Mehmet là kiến ​​trúc sư giải pháp chính cho các đối tác nhà cung cấp phần mềm độc lập (ISV) tại Amazon Web Services (AWS), dẫn đầu các sáng kiến ​​chiến lược giúp các đối tác phát triển trên toàn cầu. Hiện tại, ông tập trung vào việc ra mắt Sovereign Cloud tại Châu Âu, mở rộng sang Trung Đông và đưa AI ra thị trường.



### **Mohan CV**

Mohan là kiến ​​trúc sư chính tại AWS có trụ sở tại Bắc Virginia. Với nền tảng vững chắc về di chuyển và hiện đại hóa doanh nghiệp quy mô lớn, ông chuyên về dữ liệu, phân tích và AI. Mohan đam mê tận dụng các công nghệ mới để hỗ trợ khách hàng trong khu vực công và hơn thế nữa, điều chỉnh các sáng kiến ​​để đáp ứng nhu cầu kinh doanh độc đáo.

### **Damian Randell**Damian Randell

Damian là kiến ​​trúc sư giải pháp cấp cao trong nhóm Khu vực công tại AWS. Ông giúp các đối tác và khách hàng hiểu cách tốt nhất để sử dụng công nghệ AWS để chuyển đổi nhu cầu kinh doanh thành giải pháp và có hơn 25 năm kinh nghiệm trong việc cung cấp và thiết kế các giải pháp trong nhiều ngành, bao gồm khu vực công, quốc phòng, viễn thông, ISV và ngân hàng. Ông chuyên về bảo mật, Chủ quyền số, AI/ML, di chuyển và hiện đại hóa.