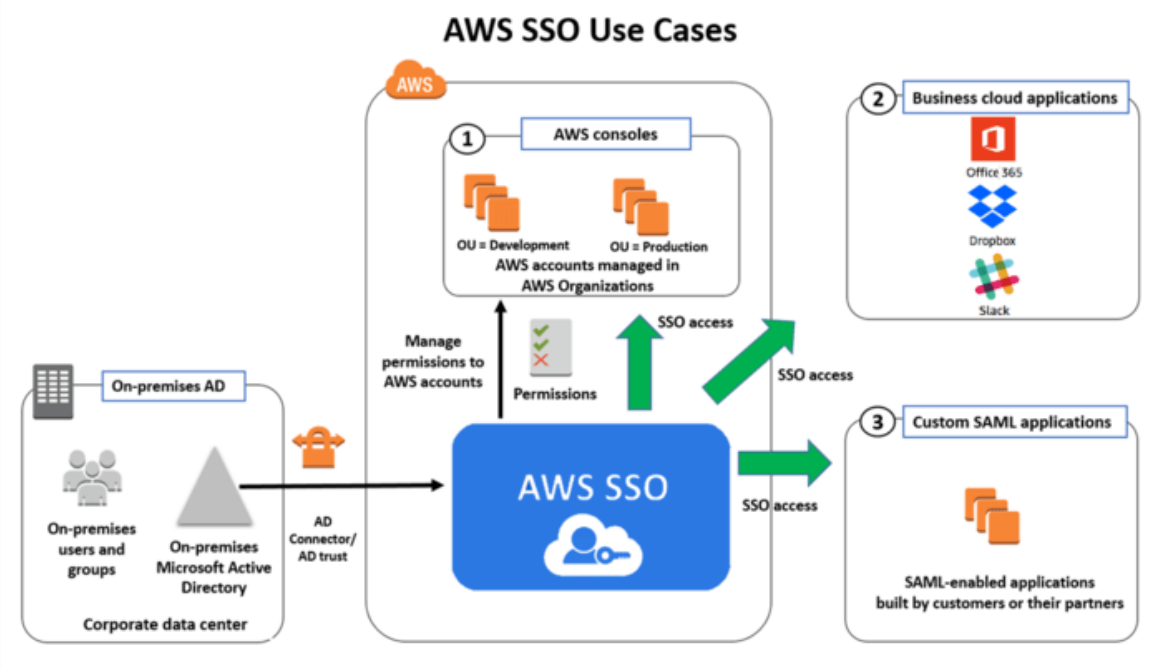
SSO là gì?

SSO là gì?

Đăng nhập đơn (SSO) là giải pháp xác thực cho phép người dùng đăng nhập vào nhiều ứng dụng và trang web nhờ khả năng xác thực người dùng một lần. Trong bối cảnh người dùng ngày nay thường xuyên truy cập trực tiếp vào ứng dụng từ trình duyệt của họ, các tổ chức đang ưu tiên áp dụng những chiến lược quản lý quyền truy cập có thể cải thiện cả khả năng bảo mật và trải nghiệm người dùng. SSO mang đến cả hai khía cạnh kể trên, do đó người dùng có thể truy cập vào tất cả tài nguyên có mật khẩu bảo vệ mà không cần đăng nhập lại sau khi đã xác minh danh tính.

Tại sao SSO lại quan trọng?

Sử dụng SSO để hợp lý hóa việc đăng nhập của người dùng mang lại lợi ích cho người dùng và các tổ chức theo một số cách.



Tăng cường bảo mật mật khẩu

Khi không sử dụng SSO, ta sẽ phải nhớ nhiều mật khẩu cho các trang web khác nhau. Điều này có thể dẫn đến một số thói quen bảo mật không được khuyến nghị, chẳng hạn như sử dụng mật khẩu đơn giản hoặc sử dụng cùng một mật khẩu cho các tài khoản khác nhau. Bên cạnh đó, người dùng có thể quên hoặc nhập sai thông tin chứng thực của họ khi đăng nhập vào một dịch vụ. SSO giúp hạn chế việc quên mật khẩu và khuyến khích người dùng tạo một mật khẩu mạnh có thể được sử dụng cho nhiều trang web.

Cải thiện năng suất

Nhân viên thường sử dụng nhiều ứng dụng doanh nghiệp yêu cầu phải xác thực riêng biệt. Việc nhập tên người dùng và mật khẩu theo cách thủ công trong mọi ứng dụng tốn nhiều thời gian và thiếu hiệu quả. SSO hợp lý hóa quy trình xác thực người dùng cho các ứng dụng doanh nghiệp và giúp truy cập các tài nguyên được bảo vệ dễ dàng hơn.

Giảm chi phí

Khi cố gắng nhớ nhiều mật khẩu, người dùng doanh nghiệp có thể quên thông tin chứng thực của họ để đăng nhập. Điều này dẫn đến việc họ thường xuyên gửi yêu cầu truy xuất hoặc đặt lại mật khẩu, làm tăng khối lượng công việc cho đội ngũ CNTT nội bộ. Việc triển khai SSO làm giảm việc quên mật khẩu, từ đó giảm các tài nguyên hỗ trợ trong việc xử lý các yêu cầu đặt lại mật

khẩu.

Nâng cao khả năng bảo mật

Bằng cách giảm thiểu số lượng mật khẩu cho mỗi người dùng, SSO tạo điều kiện thuận lợi cho việc kiểm tra quyền truy cập của người dùng và cung cấp khả năng kiểm soát quyền truy cập mạnh mẽ cho tất cả các loại dữ liệu. Điều này làm giảm nguy cơ xảy ra các sự kiện bảo mật nhắm vào mật khẩu, đồng thời giúp các tổ chức tuân thủ các quy định về bảo mật dữ liệu.

Cung cấp trải nghiệm khách hàng tốt hơn

Các nhà cung cấp ứng dụng đám mây sử dụng SSO để cung cấp cho người dùng cuối trải nghiệm đăng nhập và quản lý thông tin chứng thực liền mạch. Người dùng quản lý ít mật khẩu hơn mà vẫn có thể truy cập an toàn vào thông tin và ứng dụng họ cần để hoàn thành công việc hàng ngày của họ.

SSO hoạt động như thế nào?

SSO xác lập tín nhiệm giữa ứng dụng hoặc dịch vụ với nhà cung cấp dịch vụ bên ngoài, còn được gọi là nhà cung cấp danh tính (IdP). Việc này được thực hiện thông qua một loạt các bước xác thực, xác nhận và giao tiếp giữa ứng dụng và dịch vụ SSO tập trung. Dưới đây là các thành phần quan trọng trong các giải pháp SSO.

Dịch vụ SSO

Dịch vụ SSO là một dịch vụ trung tâm mà các ứng dụng dựa vào khi người dùng đăng nhập. Nếu người dùng chưa được xác thực yêu cầu quyền truy cập vào một ứng dụng, ứng dụng sẽ chuyển hướng họ đến dịch vụ SSO. Sau đó, dịch vụ này sẽ xác thực và chuyển hướng người dùng trở lại ứng dụng ban đầu. Dịch vụ này thường chạy trên một máy chủ chính sách SSO chuyên dụng.

Mã thông báo SSO

Mã thông báo SSO là một tệp kỹ thuật số chứa thông tin nhận dạng người dùng, chẳng hạn như tên người dùng hoặc địa chỉ email. Khi người dùng yêu cầu quyền truy cập vào một ứng dụng, ứng dụng sẽ trao đổi mã thông báo

SSO với dịch vụ SSO để xác thực người dùng.

Quy trình SSO

Quy trình SSO như sau:

1. Khi người dùng đăng nhập vào một ứng dụng, ứng dụng sẽ tạo mã thông báo SSO và gửi yêu cầu xác thực đến dịch vụ SSO.
2. Dịch vụ sẽ kiểm tra xem người dùng đã được xác thực trước đó trong hệ thống hay chưa. Nếu đã xác thực, dịch vụ sẽ gửi một phản hồi xác nhận xác thực đến ứng dụng để cấp quyền truy cập cho người dùng.
3. Nếu người dùng không có thông tin chứng thực đã xác minh, dịch vụ SSO sẽ chuyển hướng người dùng đến hệ thống đăng nhập trung tâm và nhắc người dùng gửi tên người dùng và mật khẩu của họ.
4. Sau khi gửi, dịch vụ xác mình thông tin chứng thực của người dùng và gửi phản hồi tích cực cho ứng dụng.
5. Nếu không, người dùng sẽ nhận được thông báo lỗi và phải nhập lại thông tin chứng thực. Nhiều lần đăng nhập không thành công có thể dẫn đến việc dịch vụ chặn người dùng thử đăng nhập lại trong một khoảng thời gian cố định.

SSO có những loại nào?

Các giải pháp SSO sử dụng các tiêu chuẩn và giao thức khác nhau để xác minh và xác thực thông tin chứng thực của người dùng.

SAML

SAML, hoặc Ngôn ngữ đánh dấu xác nhận bảo mật, là một giao thức hoặc tập hợp các quy tắc mà các ứng dụng sử dụng để trao đổi thông tin xác thực với dịch vụ SSO. SAML sử dụng XML, một ngôn ngữ đánh dấu thân thiện với trình duyệt, để trao đổi dữ liệu nhận dạng người dùng. Các dịch vụ SSO dựa trên SAML có tính bảo mật và tính linh hoạt tốt hơn, vì các ứng dụng không cần lưu trữ thông tin chứng thực của người dùng trên hệ thống của chúng.

OAuth

OAuth, hay Xác thực mở, là một tiêu chuẩn mở cho phép các ứng dụng truy cập một cách bảo mật vào thông tin người dùng từ các trang web khác mà không cần cung cấp mật khẩu. Thay vì yêu cầu mật khẩu của người dùng, các ứng dụng sử dụng OAuth để được người dùng cho phép truy cập vào dữ liệu được bảo vệ bằng mật khẩu. OAuth xác lập tín nhiệm giữa các ứng dụng thông qua API, cho phép ứng dụng gửi và phản hồi các yêu cầu xác thực trong một khuôn khổ đã thiết lập.

OIDC

OpenID là một phương pháp sử dụng một tập hợp thông tin chứng thực của người dùng để truy cập nhiều trang web. Nó cho phép nhà cung cấp dịch vụ đảm nhận vai trò xác thực thông tin chứng thực của người dùng. Thay vì chuyển mã thông báo xác thực cho bên thứ ba cung cấp danh tính, các ứng dụng web sử dụng OIDC để yêu cầu thông tin bổ sung và xác minh tính xác thực của người dùng.

Kerberos

Kerberos là một hệ thống xác thực dựa trên phiếu cho phép hai hoặc nhiều bên xác minh lẫn nhau danh tính trên mạng của họ. Hệ thống này sử dụng mật mã bảo mật để ngăn chặn truy cập trái phép vào thông tin nhận dạng được truyền giữa máy chủ, máy khách và Trung tâm phân phối khóa.

SSO có an toàn không?

Đúng vậy, SSO là một giải pháp quản lý quyền truy cập danh tính tiên tiến và được nhiều người mong muốn. Khi được triển khai, giải pháp đăng nhập một lần giúp các tổ chức quản lý quyền truy cập của người dùng đối với các ứng dụng và tài nguyên của doanh nghiệp. Giải pháp SSO giúp người dùng ứng dụng đặt và ghi nhớ mật khẩu mạnh dễ dàng hơn. Ngoài ra, đội ngũ CNTT cũng có thể sử dụng công cụ SSO để theo dõi hành vi của người dùng, cải thiện khả năng phục hồi của hệ thống và giảm rủi ro bảo mật.

SSO có sự khác biệt gì với các giải pháp quản lý truy cập khác?

Có một số giải pháp quản lý danh tính và quyền truy cập bạn có thể chọn, tùy thuộc vào yêu cầu của bạn.

Quản lý danh tính liên kết

Quản lý danh tính liên kết (FIM) là một khuôn khổ kỹ thuật số cho phép nhiều ứng dụng từ các nhà cung cấp khác nhau chia sẻ, quản lý và xác thực danh tính người dùng. Ví dụ: FIM cho phép lực lượng lao động của bạn đăng nhập vào một ứng dụng và sau đó truy cập vào một số ứng dụng doanh nghiệp khác mà không cần đăng nhập lại. FIM xác thực thông tin chứng thực được gửi từ nhà cung cấp dịch vụ với một nhà cung cấp danh tính đáng tin cậy.

So sánh giữa SSO và quản lý danh tính liên kết

Quản lý danh tính liên kết là một giải pháp quản lý và xác thực danh tính toàn diện cho các ứng dụng đa miền. Trong khi đó, đăng nhập một lần (SSO) là một chức năng cụ thể trong mô hình FIM. Trong khi FIM cho phép người dùng truy cập các dịch vụ từ các nhà cung cấp khác nhau bằng một lần đăng nhập duy nhất, SSO chỉ giới hạn ở các dịch vụ hoặc ứng dụng do một nhà cung cấp duy nhất lưu trữ.

Đăng nhập tương tự

Đăng nhập tương tự, cũng viết tắt là SSO, là một giải pháp kỹ thuật số lưu trữ và đồng bộ hóa thông tin chứng thực của người dùng trên các thiết bị mà người dùng truy cập. Nó tương tự như kho mật khẩu hoặc trình quản lý mật khẩu cho phép người dùng đăng nhập vào nhiều ứng dụng trên các thiết bị khác nhau mà không cần nhớ thông tin chứng thực.

So sánh giữa đăng nhập một lần và đăng nhập tương tự

Hệ thống đăng nhập một lần yêu cầu xác thực một lần từ người dùng. Sau khi đăng nhập, người dùng có thể truy cập các ứng dụng và dịch vụ web khác mà không cần xác thực lại. Trong khi đó, đăng nhập tương tự yêu cầu người dùng lặp lại quy trình đăng nhập mỗi lần với thông tin chứng thực giống nhau.

Xác thực đa yếu tố

Xác thực đa yếu tố là khuôn khổ xác thực người dùng sử dụng hai hoặc nhiều công nghệ để xác minh danh tính của người dùng. Ví dụ: người dùng nhập địa chỉ email và mật khẩu của họ trên một trang web và nhập mật khẩu một lần (OTP) được gửi đến điện thoại di động của họ để cho phép truy cập bảo mật.

So sánh giữa SSO và xác thực đa yếu tố

SSO cho phép các tổ chức đơn giản hóa và tăng cường bảo mật bằng mật khẩu thông qua việc cho phép truy cập vào tất cả các dịch vụ được kết nối với một lần đăng nhập duy nhất. Xác thực đa yếu tố cung cấp các lớp bảo mật bổ sung để giảm khả năng truy cập trái phép thông qua các thông tin chứng thực bị đánh cắp. Cả SSO và xác thực đa yếu tố đều có thể được tích hợp để cải thiện khả năng bảo mật của các ứng dụng web.

AWS có thể trợ giúp như thế nào với SSO?

Trung tâm danh tính AWS IAM là một giải pháp xác thực đám mây cho phép các tổ chức tạo hoặc kết nối danh tính lực lượng lao động của họ một cách bảo mật, đồng thời quản lý tập trung quyền truy cập của họ trên các tài khoản và ứng dụng AWS. Bạn có thể tạo danh tính người dùng hoặc nhập danh tính từ các nhà cung cấp danh tính bên ngoài như Okta Universal Directory hoặc Azure. Một số lợi ích của Trung tâm danh tính AWS IAM bao gồm:

- Bảng thông tin trung tâm để quản lý danh tính của tài khoản AWS hoặc các ứng dụng kinh doanh của bạn.
- Hỗ trợ xác thực đa yếu tố mang lại trải nghiệm xác thực bảo mật cao cho người dùng.
- Hỗ trợ tích hợp với các ứng dụng AWS khác để xác thực và cấp quyền không cấu hình.

Bắt đầu sử dụng SSO trên AWS bằng cách tạo tài khoản AWS miễn phí ngay hôm nay.

Các bước tiếp theo để sử dụng AWS SSO

Tham khảo các tài nguyên bổ sung liên quan đến sản phẩm

Tìm hiểu thêm về Các dịch vụ bảo mật »

Đăng ký tài khoản miễn phí

Nhận ngay quyền sử dụng bậc miễn phí của AWS.

Đăng ký »

Bắt đầu xây dựng trong bảng điều khiển

Bắt đầu xây dựng trong AWS Management Console.

Đăng nhập »

Đăng nhập vào bảng điều khiển

Tìm hiểu về AWS

AWS là gì?
Điện toán đám mây là gì?
Sự hòa nhập, đa dạng và công bằng của AWS
DevOps là gì?
Bộ chứa là gì?
Kho dữ liệu là gì?
Khả năng bảo mật của Đám mây AWS
Thông tin mới
Blog
Thông cáo báo chí

Tài nguyên dành cho AWS

Bắt đầu
Đào tạo và chứng nhận
Thư viện giải pháp AWS
Trung tâm kiến trúc
Câu hỏi thường gặp về sản phẩm và kỹ thuật
Báo cáo của chuyên gia phân tích
Đối tác của AWS

Nhà phát triển trên AWS

Trung tâm dành cho nhà phát triển
SDK và Công cụ
.NET trên AWS
Python trên AWS
Java trên AWS
PHP trên AWS
JavaScript trên AWS

Trợ giúp

Liên hệ với chúng tôi
Nhận trợ giúp từ chuyên gia
Nộp phiếu hỗ trợ
AWS re:Post
Trung tâm kiến thức
Tổng quan về AWS Support
Pháp lý
Việc làm tại AWS

Tạo tài khoản AWS

Amazon là một công ty làm việc bình đẳng: *không phân biệt Dân tộc thiểu số / Nữ giới / Người khuyết tật / Cựu chiến binh / Bản dạng giới / Khuynh hướng tình dục / Tuổi tác.*

Ngôn ngữ

عربي |
Bahasa Indonesia |
Deutsch |
English |
Español |
Français |
Italiano |
Português |
Tiếng Việt |
Türkçe |
Русский |
ไทย |
日本語 |
한국어 |
中文 (简体) |
中文 (繁體)