**I. Định nghĩa về Auth0, vai trò và chức năng**

1. Auth0 là gì ?

Auth0 là một nền tảng cung cấp các dịch vụ authentication và authorization như các chức năng như đăng nhập, đăng ký, quên mật khẩu, đăng nhập bằng SMS, xác thực đa yếu tố,... cho ứng dụng của bạn. Ngoài ra, Auth0 sẽ lưu trữ và cung cấp các dịch vụ để quản lý các thông tin dùng để đăng nhập của người dùng như email, username, số điện thoại, password,... Do vậy dịch vụ này rất hữu ích khi hệ thống của bạn gồm nhiều dịch vụ và bạn muốn người dùng chỉ sử dụng một tài khoản để đăng nhập cho tất cả các dịch vụ này mà không cần phải lặp đi lặp lại việc implement lại chức năng đăng nhập cho các dịch vụ đó.

2. Vai trò và chức năng của Auth0

Hàng tỷ người dùng đang đăng ký hoặc đăng nhập vào một ứng dụng web để chọn sử dụng các dịch vụ của bạn. Họ có thể đang đặt hàng hoặc thực hiện quá trình mua. Việc xây dựng một quy trình xác thực bảo mật là cần thiết cho bất kỳ luồng hoạt động nào như vậy.Auth0 có thể hỗ trợ chuẩn bị ứng dụng được bảo mật tốt nhất. Nó có nhiều tính năng làm cho nó trở thành một lựa chọn tuyệt vời cho các nhà phát triển sử dụng. Một số tính năng là:

-*Đăng nhập chung*:

Auth0 cung cấp hoạt động đăng nhập truyền thống thúc đẩy trải nghiệm người dùng. Nó cho phép người dùng xác thực nhất quán và cảnh báo họ về nỗ lực lừa đảo. Thiết kế đăng nhập phổ biến khiến người dùng chỉ có một biểu mẫu cho thông tin đăng nhập. Nếu có bất cứ điều gì đáng ngờ, nó sẽ bị từ chối.Bất cứ khi nào người dùng đăng nhập, họ sẽ được chuyển hướng đến máy chủ chung đại diện cho hình thức đăng nhập của doanh nghiệp bạn. Tất cả quá trình đăng nhập cũng như xác thực diễn ra cùng một lúc, đảm bảo tính bảo mật.

-*Dấu hiệu duy nhất* :

Đăng nhập một lần cho phép người dùng có quyền truy cập vào tất cả các ứng dụng mà họ có thông qua thông tin đăng nhập duy nhất. Ví dụ; bạn có thể sử dụng tài khoản Google của mình để đăng nhập vào một ứng dụng dịch vụ. Tuy nhiên, việc xây dựng một đăng nhập duy nhất có thể vừa tốn thời gian vừa tốn kém.

Tuy nhiên, việc triển khai đăng nhập một lần qua Auth0 có thể làm nên điều kỳ diệu trong thời gian ngắn hơn. Nó hỗ trợ hơn 40 nhà cung cấp danh tính. Bạn có thể tăng tỷ lệ chuyển đổi bằng cách liên kết các tài khoản trên nhiều nền tảng. Cung cấp sự tự do để viết mã một lần và tích hợp các kết nối khác nhau.

-*Xác thực đa yếu tố*:

Xác thực đa yếu tố là một loại xác minh yêu cầu nhiều hơn một loại thông tin nhận dạng. Điều này làm tăng tính bảo mật của ứng dụng, giảm nguy cơ bị truy cập trái phép. Loại thông tin bao gồm;

Kiến thức: thứ mà người dùng biết (mật khẩu)

Sở hữu: thứ mà người dùng đã có (thiết bị di động)

Tính kế thừa: thứ giúp phân biệt người dùng (quét vân tay hoặc võng mạc)

Auth0 cho phép bạn tùy chỉnh trải nghiệm xác thực đa yếu tố của mình.

-*Không có mật khẩu*:

Mọi người dùng đều nghi ngờ về khả năng bảo mật thông tin của họ. Hệ thống không cần mật khẩu này cho phép người dùng thực hiện quy trình xác thực mà không cần nhập mật khẩu của họ. Người dùng được phép đăng nhập bằng cách nhập địa chỉ email hoặc số điện thoại. Người dùng có thể nhận được một lá thư có liên kết một lần hoặc mã để đăng nhập.

II. Các thành phần có trong auth0: application, api, role, user, permission.

1.Application

Thuật ngữ Application hoặc ứng dụng trong Auth0 không ngụ ý bất kỳ đặc điểm triển khai cụ thể nào.Ví dụ, đó có thể là ứng dụng gốc thực thi trên thiết bị di động, ứng dụng 1 trang thực thi trên trình duyệt, hoặc ứng dụng web thông thường trên máy chủ.

Auth0 phân loại Application dựa trên các đặc điểm sau :

-Loại ứng dụng : Để thêm xác thực vào ứng dụng của bạn, bạn phải đăng ký nó trong Bảng điều khiển Auth0 và chọn từ một trong các loại ứng dụng sau:

-Ứng dụng web thông thường : Các ứng dụng web truyền thống thực hiện hầu hết logic ứng dụng của chúng trên máy chủ (chẳng hạn như Express.js hoặc ASP.NET). Để tìm hiểu cách thiết lập một ứng dụng web thông thường.

-Ứng dụng web một trang (SPA) : Các ứng dụng JavaScript thực hiện hầu hết logic giao diện người dùng của chúng trong trình duyệt web, giao tiếp với máy chủ web chủ yếu bằng API (chẳng hạn như AngularJS + Node.js hoặc React). Để tìm hiểu cách thiết lập ứng dụng web một trang..

-Ứng dụng gốc : Ứng dụng dành cho thiết bị di động hoặc Máy tính để bàn chạy nguyên bản trên một thiết bị (chẳng hạn như iOS hoặc Android). Để tìm hiểu cách thiết lập ứng dụng gốc.

-Ứng dụng giữa máy và máy (M2M) : Các ứng dụng không tương tác, chẳng hạn như các công cụ dòng lệnh, daemon, thiết bị IoT hoặc các dịch vụ chạy trên chương trình phụ trợ của bạn. Thông thường, bạn sử dụng tùy chọn này nếu bạn có dịch vụ yêu cầu quyền truy cập vào API.

-Bảo mật thông tin xác thực: Theo thông số kĩ thuật OAuth 2.0, các ứng dụng có thể được phân loại là công khai hoặc bí mật; các ứng dụng bí mật có thể giữ thông tin đăng nhập một cách an toàn, trong khi các ứng dụng công khai thì không.

-Quyền sở hữu : Việc ứng dụng được phân loại là bên thứ nhất hay bên thứ ba tùy thuộc vào quyền sở hữu và quyền kiểm soát ứng dụng. Các ứng dụng của bên thứ nhất được kiểm soát bởi cùng một tổ chức hoặc cá nhân sở hữu miền Auth0. Ứng dụng của bên thứ ba cho phép các bên hoặc đối tác bên ngoài truy cập an toàn vào các tài nguyên được bảo vệ đằng sau API của bạn.

2.APIs

- API Auth0 : Auth0 tiết lộ các API sau đây để các nhà phát triển sử dụng trong các ứng dụng của họ.

- API xác thực : API xác thực cho thấy chức năng nhận dạng cho Auth0 và các giao thức nhận dạng được hỗ trợ (bao gồm OpenID Connect, OAuth và SAML).Thông thường, bạn nên sử dụng API này thông qua một trong các SDK Auth0, chẳng hạn như Auth0.js hoặc một thư viện như Khóa . Tuy nhiên, nếu bạn đang xây dựng giao diện người dùng xác thực của mình theo cách thủ công, bạn sẽ cần gọi trực tiếp API xác thực.Một số nhiệm vụ ví dụ bao gồm:

.Nhận mã thông báo trong quá trình xác thực

.Yêu cầu hồ sơ của người dùng bằng Mã truy cập

.Trao đổi mã làm mới để lấy mã truy cập mới

.Yêu cầu thử thách đối với xác thực đa yếu tố (MFA)

- Trình khám phá API :

Tìm hiểu và khám phá các yêu cầu và phản hồi cho điểm cuối API xác thực Auth0 trong trình duyệt của bạn với Trình khám phá API xác thực .

Tìm hiểu về và sử dụng API quản lý Auth0 trong trình duyệt của bạn với Trình khám phá API quản lý

- API quản lý : API quản lý cho phép bạn quản lý tài khoản Auth0 của mình theo lập trình, vì vậy bạn có thể tự động cấu hình môi trường của mình. Hầu hết các tác vụ bạn có thể thực hiện trong Bảng điều khiển quản lý Auth0 cũng có thể được thực hiện theo chương trình bằng cách sử dụng API này.

Một số nhiệm vụ ví dụ bao gồm:

.Đăng ký các ứng dụng và API của bạn với Auth0

.Thiết lập các kết nối mà người dùng của bạn có thể xác thực

.Quản lý người dùng

.Liên kết tài khoản người dùng

- Phân trang

Đối với người thuê Đám mây công cộng, điểm cuối API quản lý trả về tối đa 50 kết quả cho mỗi phản hồi. Khi có nhiều kết quả hơn số kết quả có thể được trả về trong một phản hồi, hãy bao gồm các tham số “page” và “per\_page” trong yêu cầu của bạn để truy xuất nhiều kết quả hơn.

3.Role

Mỗi thành viên tổ chức có thể được chỉ định một hoặc nhiều vai trò, được áp dụng khi người dùng đăng nhập thông qua tổ chức. Để tìm hiểu thêm về vai trò và hành vi của họ, hãy đọc kiểm soát truy cập dựa trên vai trò. Bạn có thể thêm vai trò cho các thành viên trong các tổ chức bằng bảng điều khiển Auth0 hoặc API quản lý.

4.User.

Auth0 lưu trữ hồ sơ người dùng cho ứng dụng của bạn trong cơ sở dữ liệu đám mây được lưu trữ. Thông tin hồ sơ người dùng có thể đến từ người dùng của bạn trực tiếp hoặc từ bất kỳ số lượng nguồn bên ngoài nào khác bao gồm các nhà cung cấp nhận dạng xã hội, kết nối doanh nghiệp như SAML hoặc các nguồn tùy chỉnh như Active Directory.

5.Permission.

Bạn có thể gán quyền cho người dùng bằng Bảng điều khiển Auth0 hoặc API quản lý. Các quyền được chỉ định có thể được sử dụng với bộ tính năng lõi ủy quyền API. Thêm quyền trực tiếp vào một người dùng phá vỡ lợi ích của kiểm soát truy cập dựa trên vai trò (RBAC) và thường không được đề xuất.