Cấu hình xác thực (authentication) trong Azure là quá trình thiết lập và quản lý việc xác định danh tính của người dùng và ứng dụng khi truy cập vào các tài nguyên trong môi trường Azure. Điều này bao gồm việc xác định và xác thực người dùng, quản lý phân quyền truy cập, và thiết lập các cơ chế bảo mật cho dữ liệu.

Dưới đây là một số khái niệm và phương pháp chính liên quan đến cấu hình xác thực trong Azure:

1. **Azure Active Directory (Azure AD) Authentication**: Azure AD là dịch vụ quản lý danh tính trong môi trường Azure, cho phép bạn quản lý người dùng, nhóm và ứng dụng. Bằng cách sử dụng xác thực Azure AD, bạn có thể đồng bộ hóa người dùng từ Active Directory nội bộ của tổ chức hoặc tạo và quản lý người dùng trực tiếp trong Azure AD.
2. **Xác thực cơ bản (Basic Authentication)**: Azure cung cấp hỗ trợ cho các phương thức xác thực cơ bản như tên người dùng/mật khẩu (username/password). Tuy nhiên, sử dụng xác thực cơ bản không được khuyến khích vì lý do bảo mật, và các phương pháp xác thực hiện đại hơn như xác thực dựa trên mã thông báo (token-based authentication) thường được ưu tiên.
3. **Azure Role-Based Access Control (Azure RBAC)**: Azure RBAC là một dịch vụ quản lý quyền truy cập dựa trên vai trò trong Azure. Bằng cách sử dụng Azure RBAC, bạn có thể quản lý quyền truy cập vào các tài nguyên Azure bằng cách gán vai trò (role) cho người dùng hoặc nhóm người dùng. Ví dụ, bạn có thể gán vai trò "Owner" cho một người dùng để cho phép họ có quyền quản lý toàn bộ tài nguyên trong một subscription.
4. **Azure Private Endpoint**: Azure Private Endpoint cho phép kết nối riêng tư và an toàn tới các dịch vụ Azure thông qua Azure Private Link. Khi sử dụng Azure Private Endpoint, bạn có thể thiết lập các quy tắc truy cập và bảo mật cho các dịch vụ mà không cần thông qua Internet công cộng.
5. **Multi-Factor Authentication (MFA)**: Azure hỗ trợ Multi-Factor Authentication, một cơ chế xác thực mạnh mẽ bằng cách yêu cầu người dùng cung cấp hai hoặc nhiều phương thức xác thực khác nhau, như một mã OTP (One-Time Password) được gửi qua điện thoại di động hoặc một ứng dụng xác thực.

Cấu hình xác thực trong Azure thường được thực hiện thông qua các cài đặt và tùy chọn cụ thể trên Azure Portal hoặc thông qua các lệnh và tệp cấu hình trong Azure CLI hoặc Azure PowerShell. Điều này cho phép bạn quản lý và tuỳ chỉnh việc xác thực cho phù hợp với nhu cầu và yêu cầu bảo mật của tổ chức của bạn.

Top of Form