Your key to secure and seamless access control: Identity and access management

Let's get to know what is identity and access management:

When the term Identity and access management (IAM) refers to the term who the users are and what they are allowed to use. The core component of IAM is to stop hackers from unauthorized access, while allowing authorized users to easily do everything but not more than they are allowed to do.

IAM system has a database or directory of users which contains the details of who each user is and what they can do. As users move through the systems IAM uses the information in the database and identifies the users, monitors their activities and verifies that the user does only what they are allowed to do.

Keycloak the framework:

Keycloak is a framework which is an open source identity and access management solution designed to simplify authentication and authorization for application and services. Keycloak offers various features such as,

- Single-Sign-on
- Identity brokering
- User federation
- Admin console

- Account management console
- Standard protocol

Single Sign-on (SSO)

Basically SSO is an authentication scheme that enables users to securely access multiple applications using a single ID. When SSO is integrated with certain apps like Gmail, facebook it provides a login page for the same set of credentials. Using SSO users can access many apps without login for each single time.

Identity Brokering:

Keycloak enables users to log in using their existing social media accounts, such as Google or facebook. This eliminates the need for users to create new accounts for each application, streamlining the login process and reducing friction for users.

User federation:

Keycloak enables user federation allowing organizations to integrate with existing identity sources like **Lightweight Directory Access Protocol (LDAP)**, or Active directory. This means administrators can manage user accounts from a single location, simplifying user provisioning and authentication across multiple systems.

RBAC: The right access for the right people

Role based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. So basically RBAC refers to the levels of access that employees have to the network.

Some of the designation RBAC tool can include:

- Management role scope
- Management role group
- Management role
- Management role assignments

Key components of identity and access management decoded:

Authentication and authorization are how IAM systems apply tailored access control policies in practice.

Authentication:

Authentication is a process of determining that a user, human or non-human is who they claim to be. When a user logs in to a system or requests access to a resource, they submit credentials to verify their identity.

Authorization:

Authorization is the process of allowing users to do what they are allowed to perform within a system or application after they've been authenticated. Authorization controls what resources a user can access and what actions they can take, such as viewing, editing, or deleting data.

Authentication confirms your identity while authorization decides what you’re allowed to do once you’re in. So while these two combine together they form a foundation of secure access control in the IAM system.

Final thoughts:

Identity and access management is vital in enhancing security by controlling access to sensitive data and resources, ensuring that only authorized users can interact with them. On the other hand IAM enhances the user experience by simplifying authentication and authorization processes which leads to increased user satisfaction. IAM is useful for businesses which contributes to business continuity by ensuring secure and reliable access to resources.