**Azure directory services**

* Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop.
* Microsoft Entra ID can also help you maintain your on-premises Active Directory deployment.
* Microsoft Entra ID is Microsoft's cloud-based identity and access management service.
* Microsoft Entra ID can detect sign-in attempts from unexpected locations or unknown devices.

**Who uses Microsoft Entra ID?**

* **IT administrators**. Administrators can use Microsoft Entra ID to control access to applications and resources based on their business requirements.
* **App developers**. Developers can use Microsoft Entra ID to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
* **Users**. Users can manage their identities and take maintenance actions like self-service password reset.
* **Online service subscribers**. Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Microsoft Entra ID to authenticate into their account.

**What does Microsoft Entra ID do?**

* **Authentication**: This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
* **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
* **Application management**: You can manage your cloud and on-premises apps by using Microsoft Entra ID. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.
* **Device management**: Along with accounts for individual people, Microsoft Entra ID supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.