IAM Roles when using AD

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. AD enables organizations to enforce security policies, manage access to resources, and maintain a hierarchical structure of the network in a centralized way. They perform the tasks of making sure each person is who they claim to be (Authentication), usually by checking the user ID and password they enter, and allow them to access only the data they're allowed to use (Authorization). The two methods available to us if we wish to use IAM roles alongside AD are as follows: **IAM Roles** and **AWS AD Connector**.

A keen reader might've noticed that both authentication and authorization are tasks usually performed using IAM in an AWS environment. Integrating Active Directory with IAM therefore makes logical sense, and AWS allows us to perform this using IAM Roles, usually done by first granting the roles with necessary permissions and then using a language called SAML (Security Assertion Markup Language) to create a relationship between our Active Directory service and desired IAM Roles.

Another way of using AD and AWS together is through the **AWS AD Connector,** a rather straightforward service that does exactly what it sounds like, it acts as a proxy between the AD service and AWS, connecting them without the need to replicate the AD infrastructure within our AWS environment.