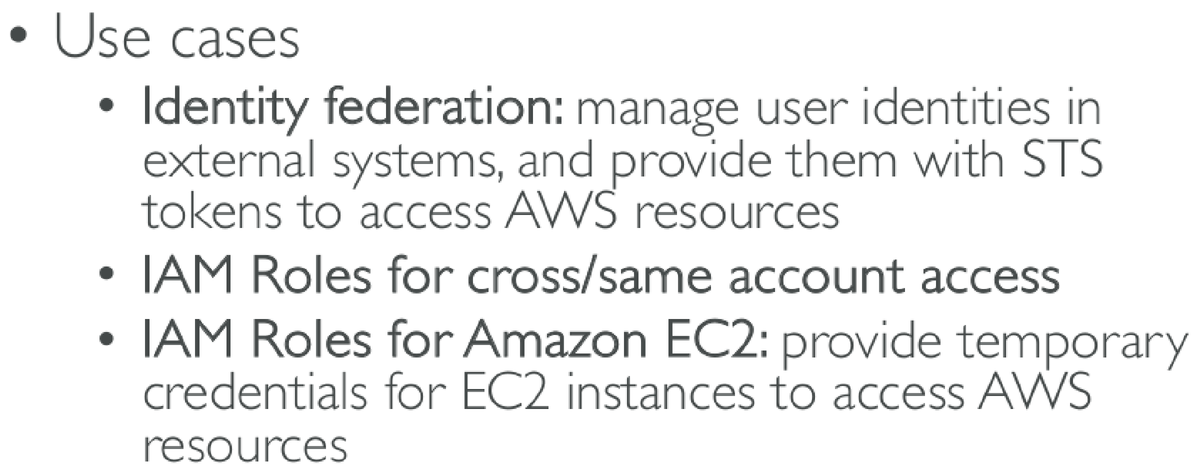
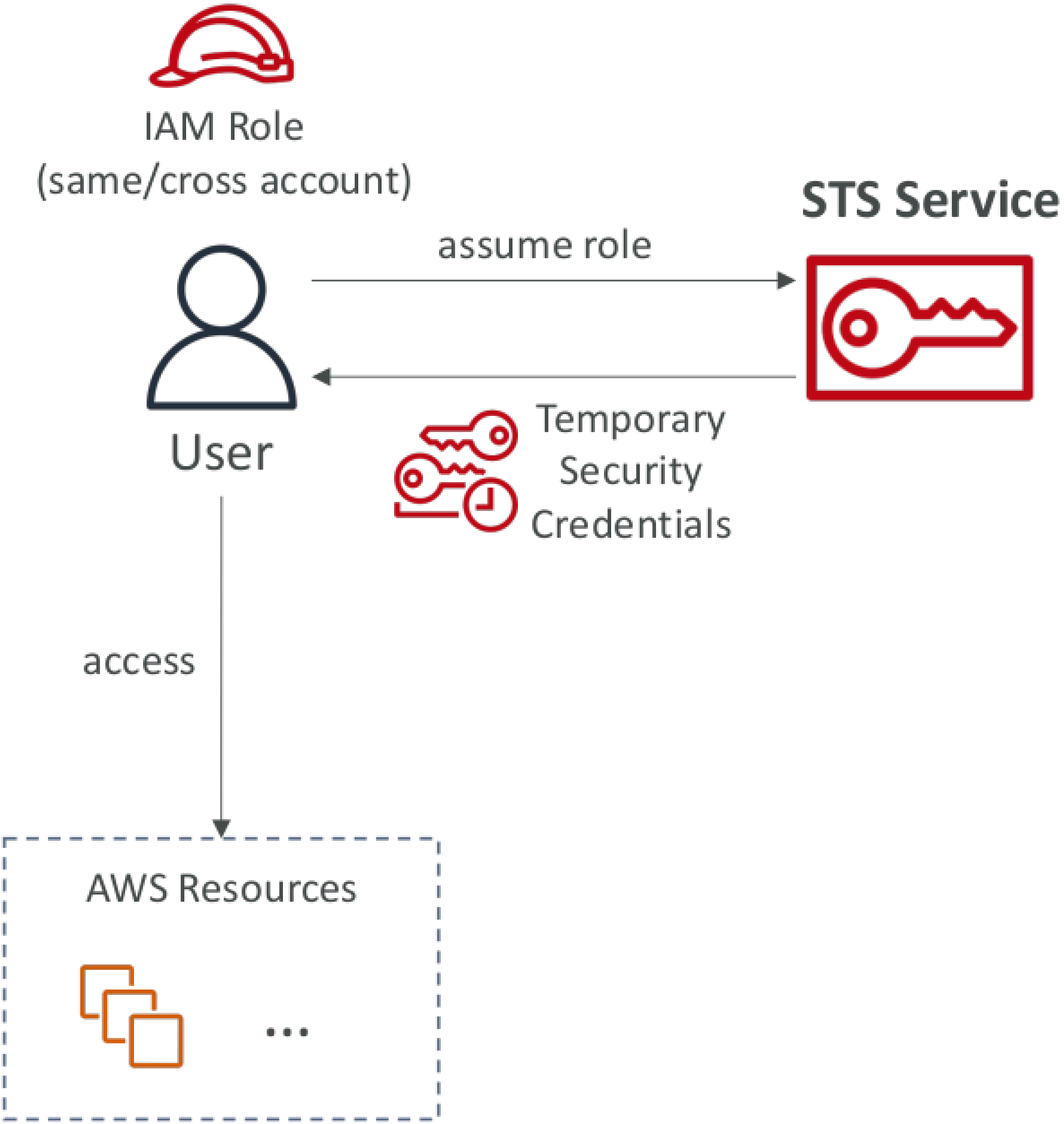
Advanced Identity

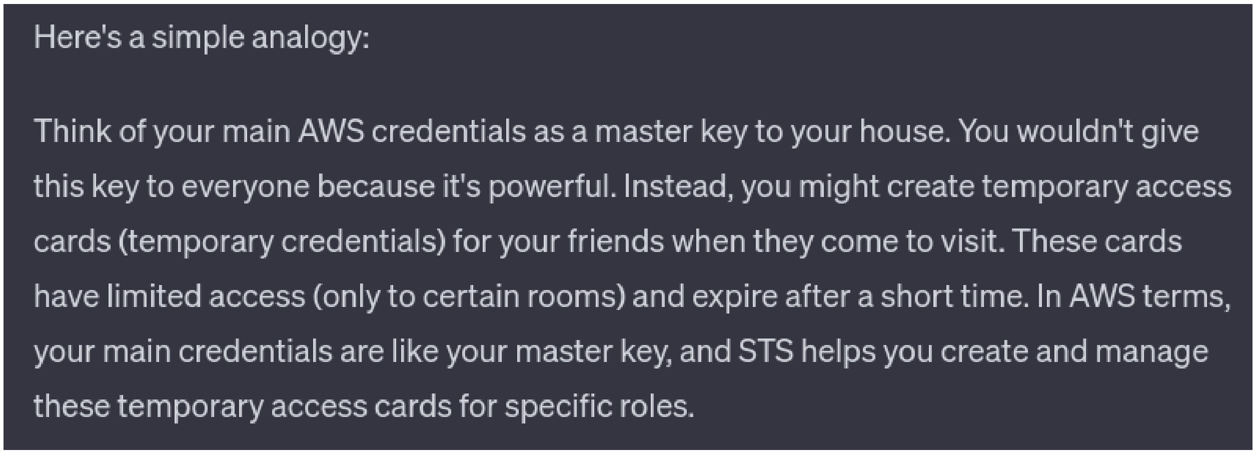
AWS Security Token Service (STS)

- Enables you to create **temporary, limited-privileges credentials** to access your AWS resources.
- Short-term credentials: you configure expiration period.



- Use cases
  - Identity federation: manage user identities in external systems, and provide them with STS tokens to access AWS resources
  - IAM Roles for cross/same account access
  - IAM Roles for Amazon EC2: provide temporary credentials for EC2 instances to access AWS resources


IAM Role
(same/cross account)
STS Service
assume role
User
Temporary
Security
Credentials
access
AWS Resources
...

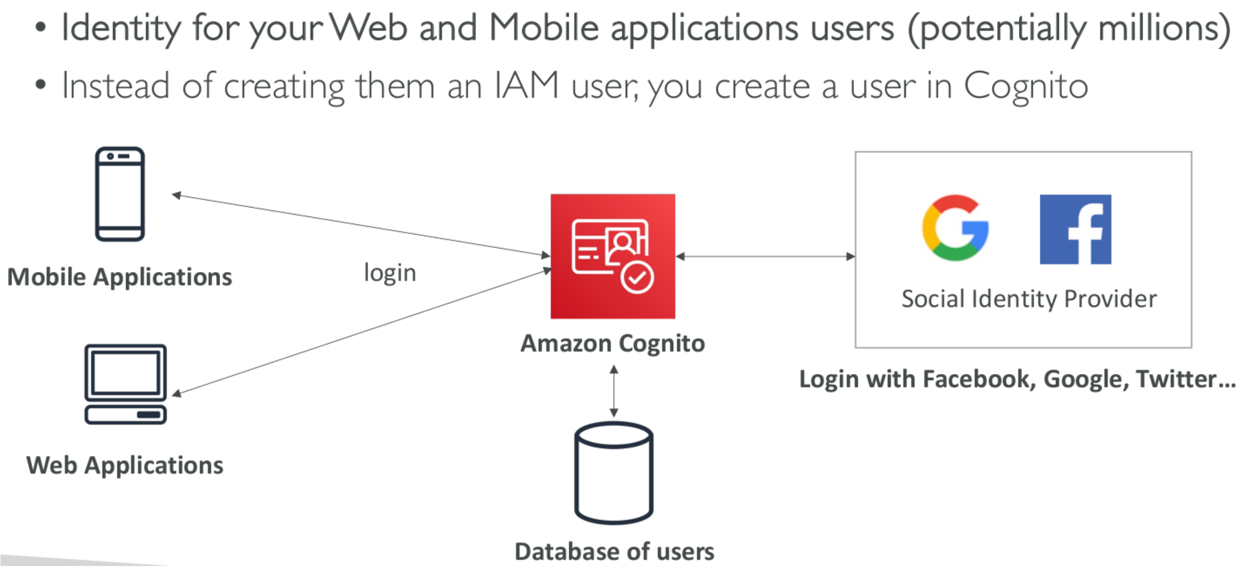


Here's a simple analogy:

Think of your main AWS credentials as a master key to your house. You wouldn't give this key to everyone because it's powerful. Instead, you might create temporary access cards (temporary credentials) for your friends when they come to visit. These cards have limited access (only to certain rooms) and expire after a short time. In AWS terms, your main credentials are like your master key, and STS helps you create and manage these temporary access cards for specific roles.

Amazon Cognito

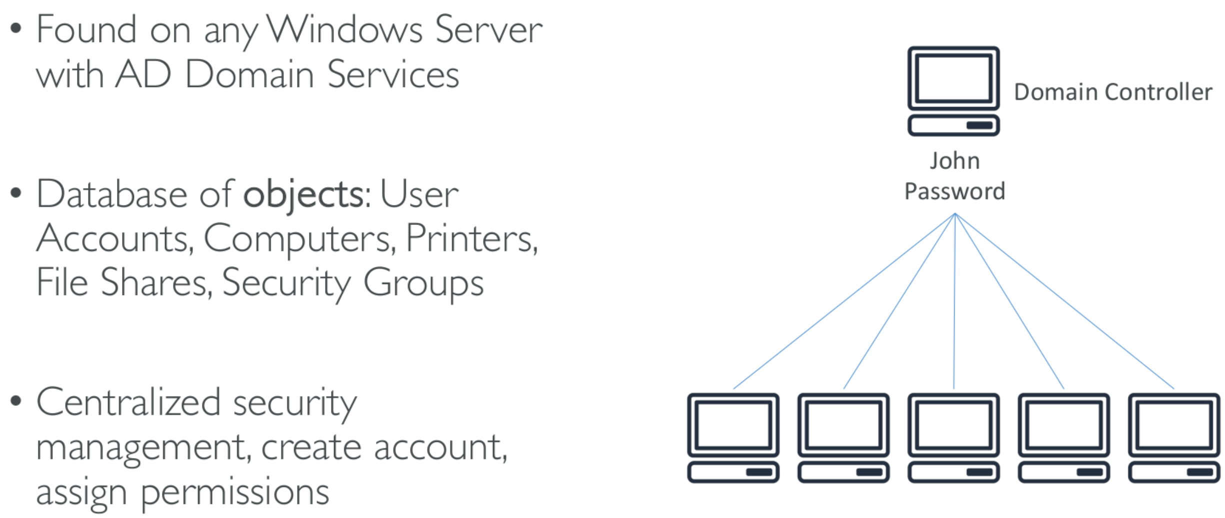
- A service that makes it easier to add authentication, user management, and secure access control to your applications.



- Identity for your Web and Mobile applications users (potentially millions)
- Instead of creating them an IAM user, you create a user in Cognito

Microsoft Active Directory (AD)

- Microsoft Active Directory (AD) is a directory service developed by Microsoft that provides a centralized repository for managing and organizing information about network resources.
- In simpler terms, it's a system that helps organizations manage and secure their computer systems, users, and other resources on a network.
- It is a database of objects such as users, computers, printers, file shares, security groups, etc.
- Found on any Windows Server with AD Domain Services
- A **domain** in Active Directory represents a logical grouping of network objects, including computers, users, and devices. Each domain has its own security policies and trust relationships with other domains.
- **Windows, central security management, active directory, domains = Microsoft AD**



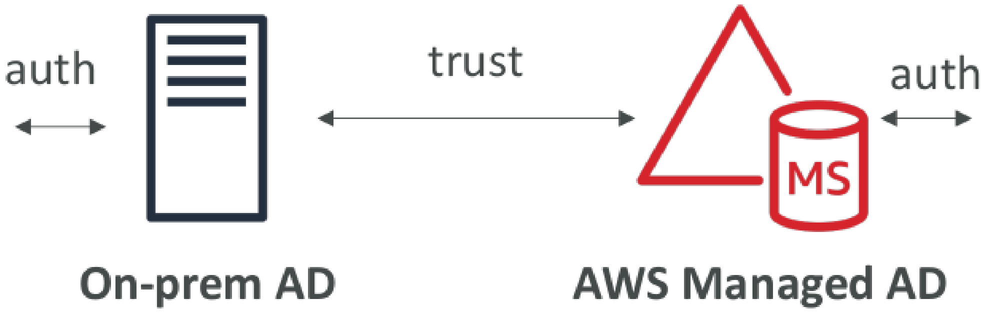
- Found on any Windows Server with AD Domain Services
- Database of **objects**: User Accounts, Computers, Printers, File Shares, Security Groups
- Centralized security management, create account, assign permissions

AWS Directory Services

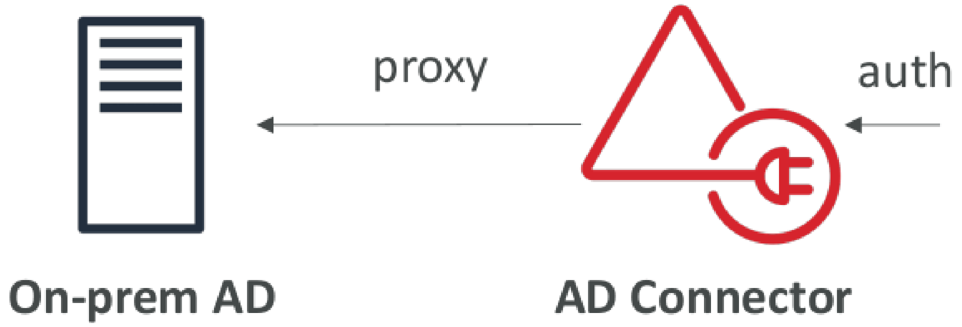
- AWS doesn’t have active directory on it but you can extent AD on it using directory services

- There are three flavours to it:

1. **AWS Managed Microsoft AD** - you can create your own AD in AWS, manage users locally, support MFA. And, if you have an on-premises AD already, then, you can establish **“trust”** between the two to join them.



2. **AD Connector** - This is basically a proxy which will redirect your requests made on AWS to the on-premises AD. Users are managed on the on-premises AD only and it supports MFA.



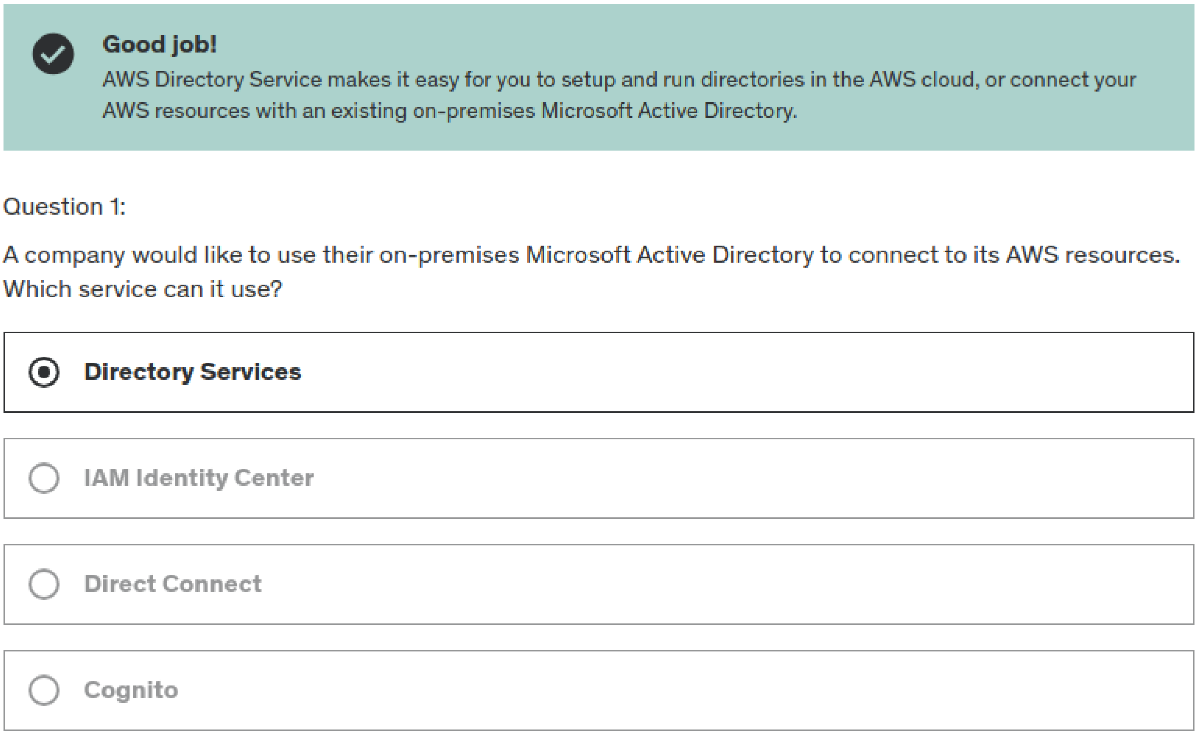
3. **Simple AD** - AD-compatibility managed directory on AWS. It is not microsoft AD, it is a standalone simple AD within AWS and cannot be joined with on-premises AD.

AWS IAM Identity Center
(Successor to AWS Single Sign-On)

- You see either name on the exam, know that it’s functionality is to provide one login / single sign-on for:
  - all your AWS accounts in AWS organizations
  - business cloud applications (like salesforce, box, microsoft 365, etc.)
  - SAML 2.0 enabled applications
  - EC2 windows instances
- Basically, a user logs in and has access to everything you defined for them to access.
- These identity providers could be built-into AWS like IAM Identity Center or 3rd party like microsoft AD or OneLogin, etc.
- **Exam: one access to multiple accounts = IAM Identity Center**

SUMMARY

- IAM
  - Identity and Access Management inside your AWS account
  - For users that you trust and belong to your company
- Organizations: Manage multiple accounts
- Security Token Service (STS): temporary, limited-privileges credentials to access AWS resources
- Cognito: create a database of users for your mobile & web applications
- Directory Services: integrate Microsoft Active Directory in AWS
- IAM Identity Center: one login for multiple AWS accounts & applications



Good job!

AWS Directory Service makes it easy for you to setup and run directories in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory.

Question 1:

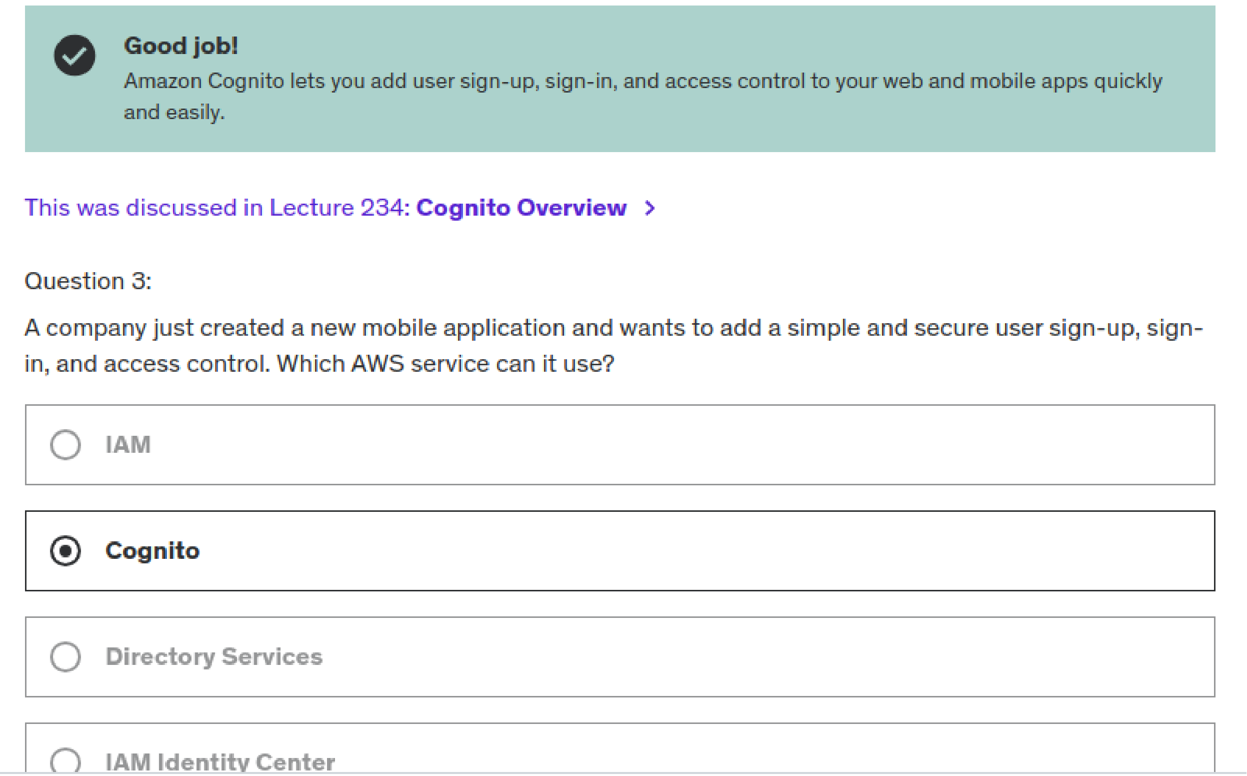
A company would like to use their on-premises Microsoft Active Directory to connect to its AWS resources. Which service can it use?

● **Directory Services**

○ **IAM Identity Center**

○ **Direct Connect**

○ **Cognito**



✓ **Good job!**
Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

This was discussed in Lecture 234: **Cognito Overview** ›

Question 3:

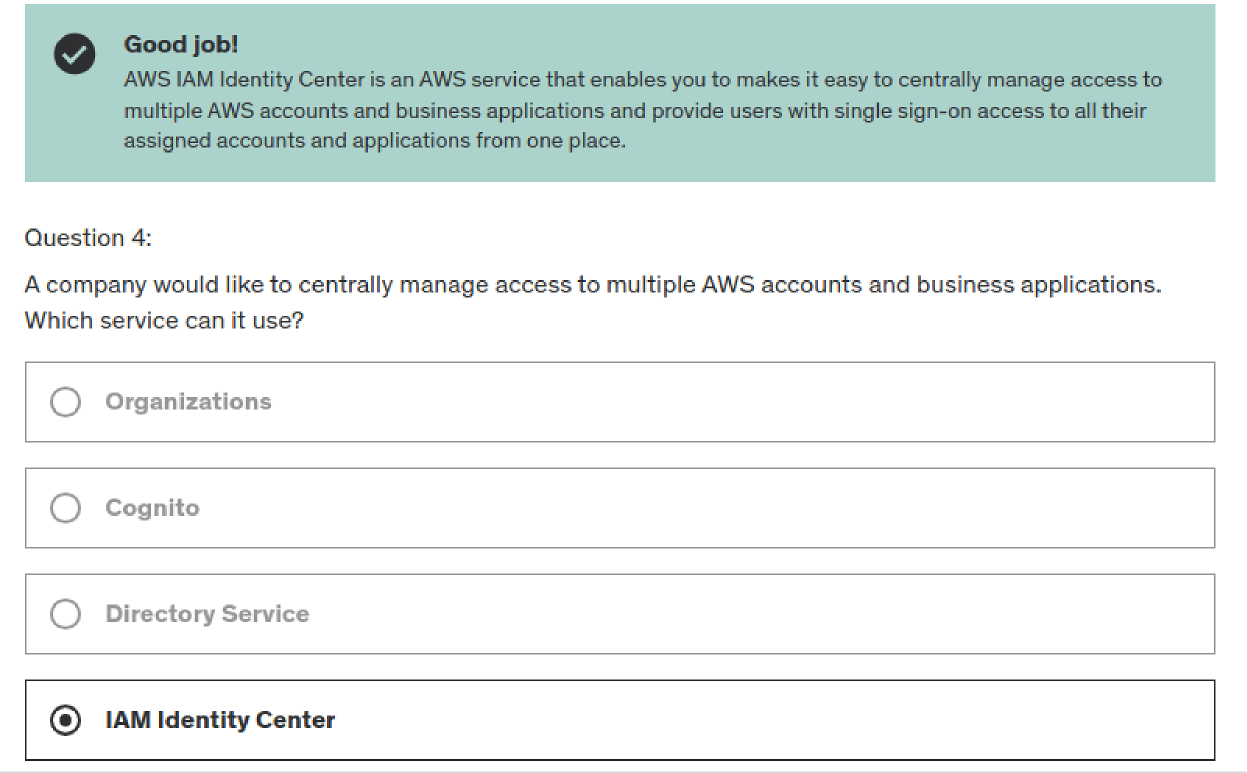
A company just created a new mobile application and wants to add a simple and secure user sign-up, sign-in, and access control. Which AWS service can it use?

○ IAM

● **Cognito**

○ Directory Services

○ IAM Identity Center



✓ **Good job!**
AWS IAM Identity Center is an AWS service that enables you to makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

Question 4:

A company would like to centrally manage access to multiple AWS accounts and business applications. Which service can it use?

○ Organizations

○ Cognito

○ Directory Service

● **IAM Identity Center**