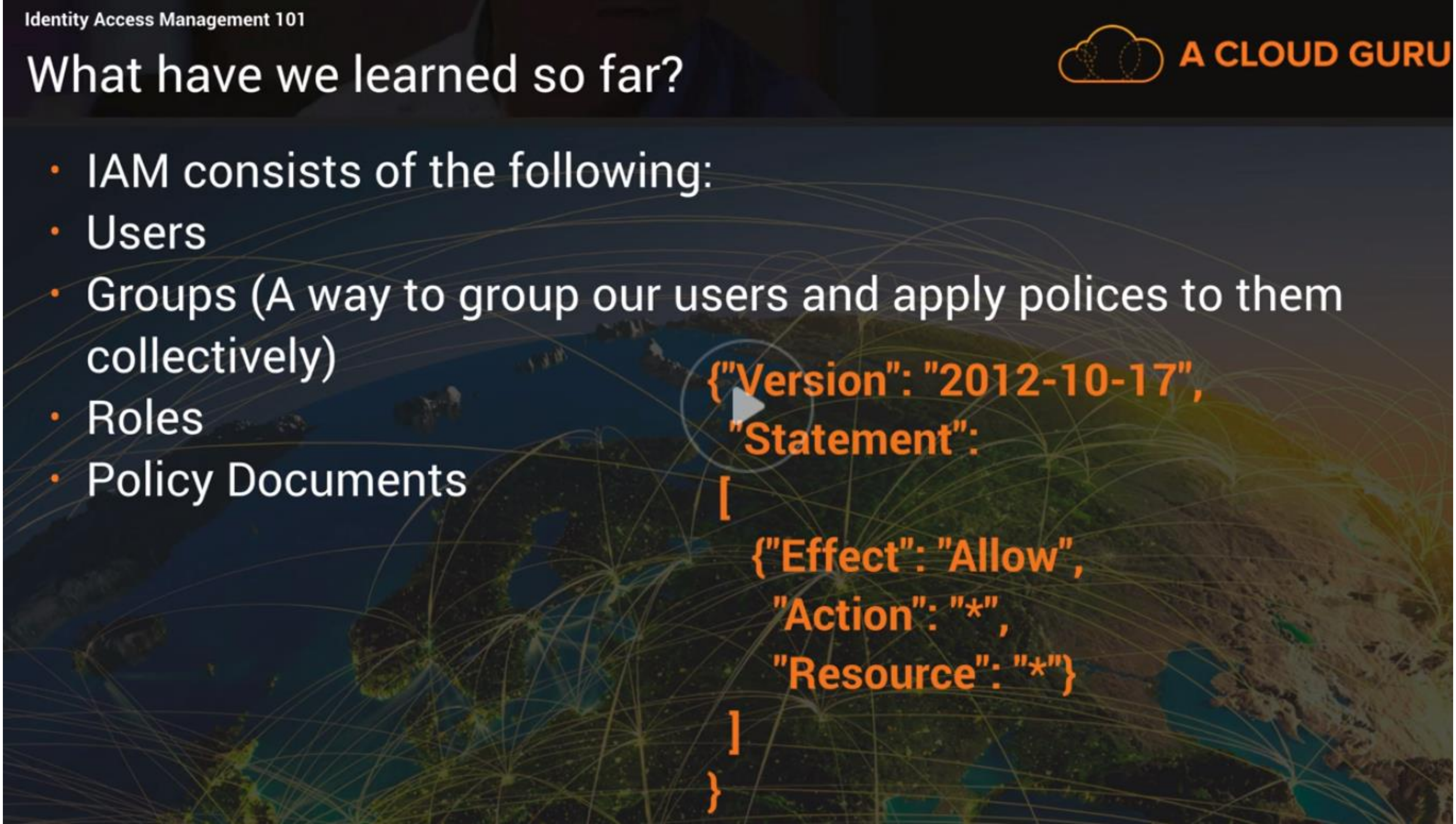
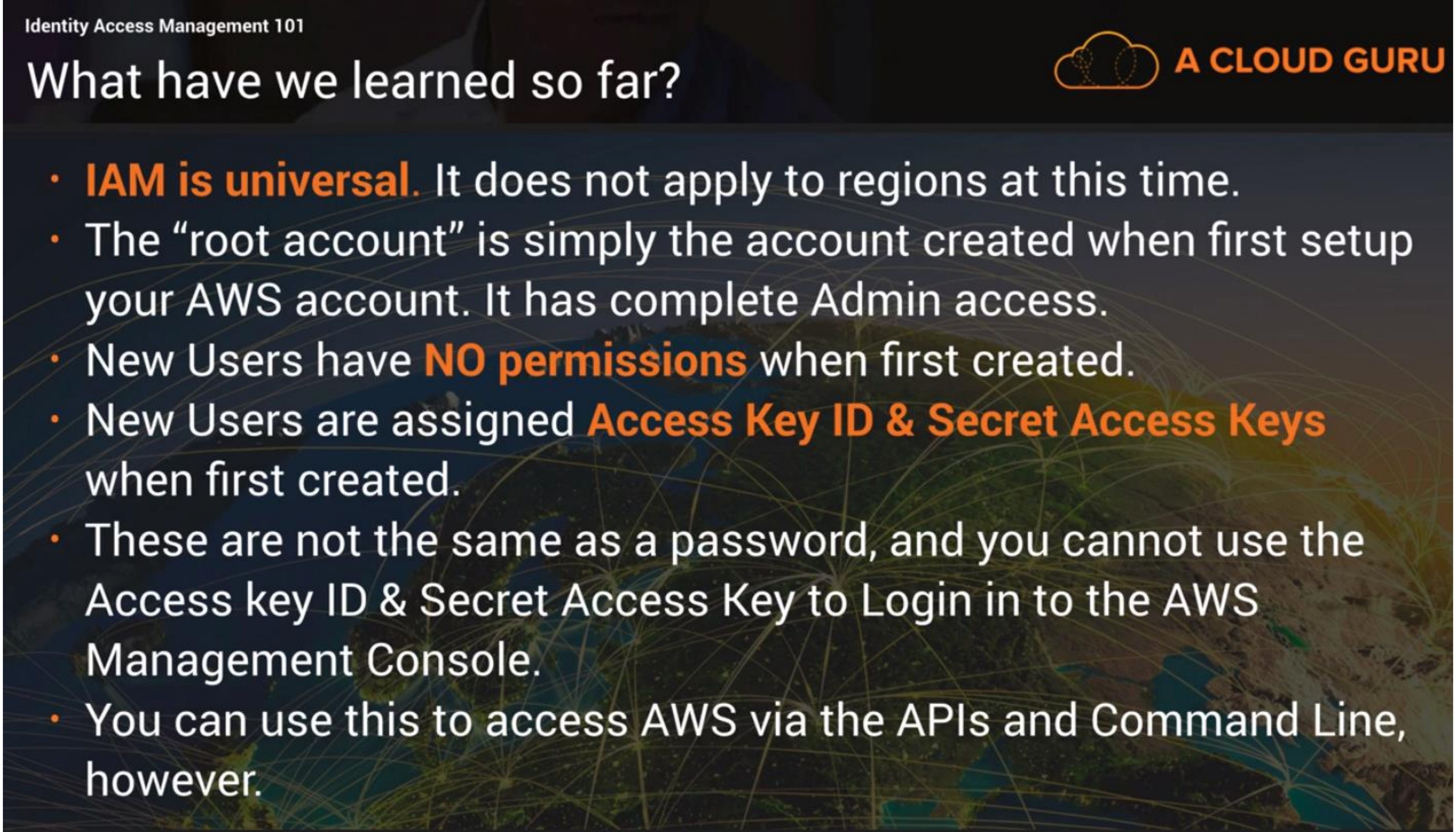


What have we learned so far?

- IAM consists of the following:
- Users
- Groups (A way to group our users and apply polices to them collectively)
- Roles
- Policy Documents

```
{"Version": "2012-10-17",
 "Statement":
 [
   {"Effect": "Allow",
    "Action": "*",
    "Resource": "*"}
  ]
}
```



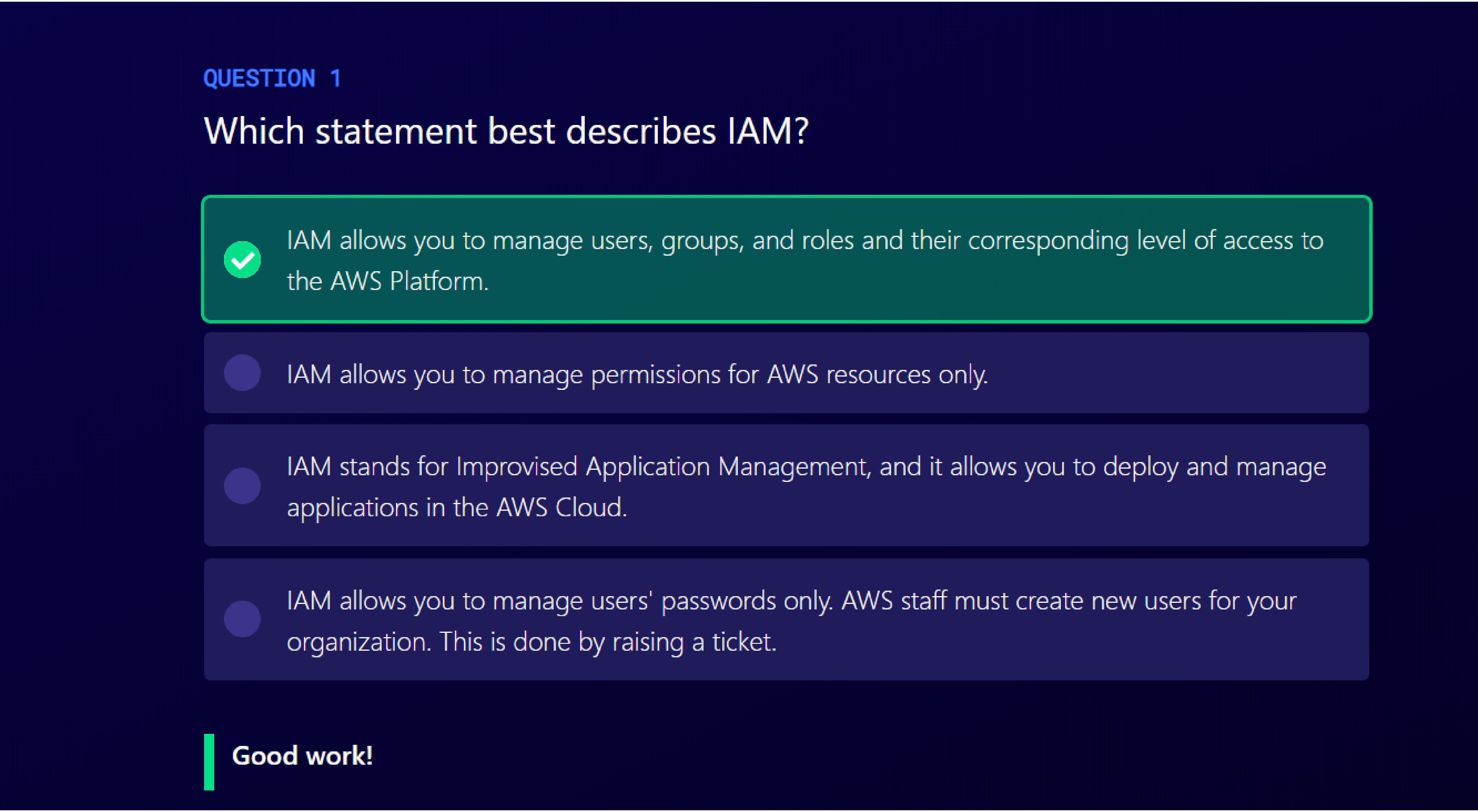
What have we learned so far?

A CLOUD GURU

- **IAM is universal.** It does not apply to regions at this time.
- The “root account” is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have **NO permissions** when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created.
- These are not the same as a password, and you cannot use the Access key ID & Secret Access Key to Login in to the AWS Management Console.
- You can use this to access AWS via the APIs and Command Line, however.

What have we learned so far?

- You only get to view Access key ID & Secret Access Key once. If you lose them, you have to regenerate them. So, save them in a secure location.
- Always setup Multifactor Authentication (MFA) on your root account.
- You can create and customise your own password rotation policies.



QUESTION 1

Which statement best describes IAM?

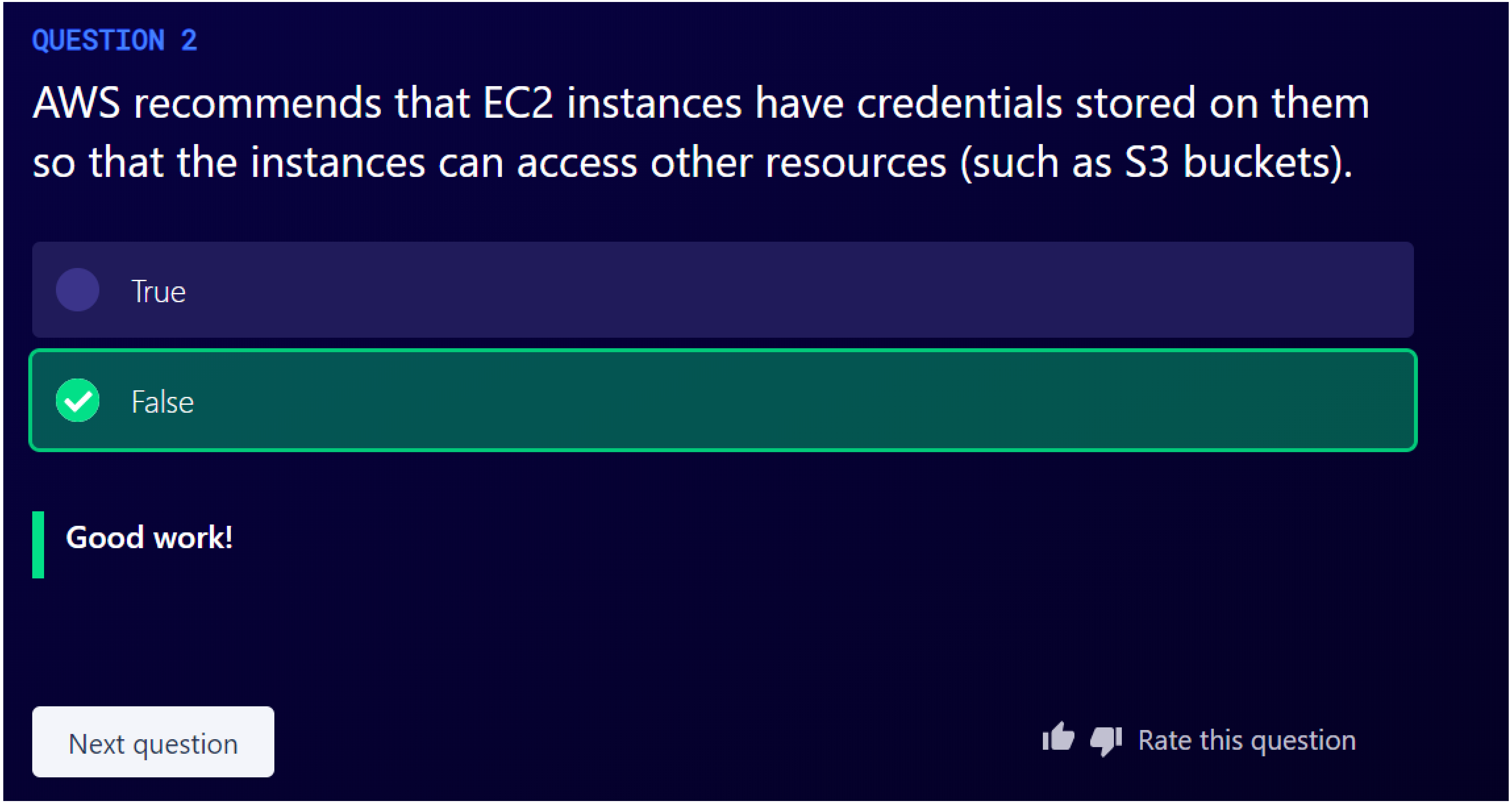
✓ IAM allows you to manage users, groups, and roles and their corresponding level of access to the AWS Platform.

○ IAM allows you to manage permissions for AWS resources only.

○ IAM stands for Improvised Application Management, and it allows you to deploy and manage applications in the AWS Cloud.

○ IAM allows you to manage users' passwords only. AWS staff must create new users for your organization. This is done by raising a ticket.

Good work!



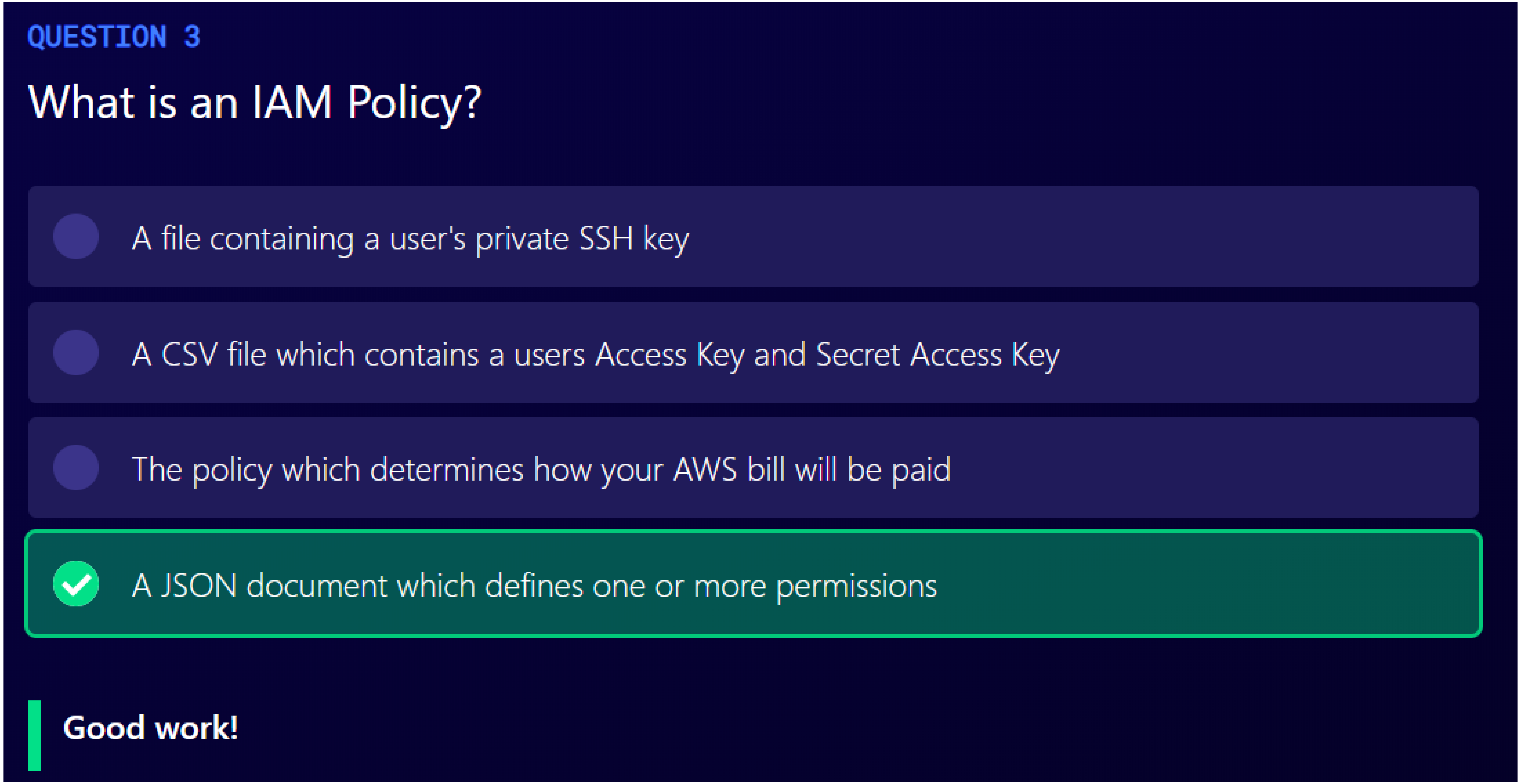
QUESTION 2

AWS recommends that EC2 instances have credentials stored on them so that the instances can access other resources (such as S3 buckets).

○ True

[✓ False]

Good work!

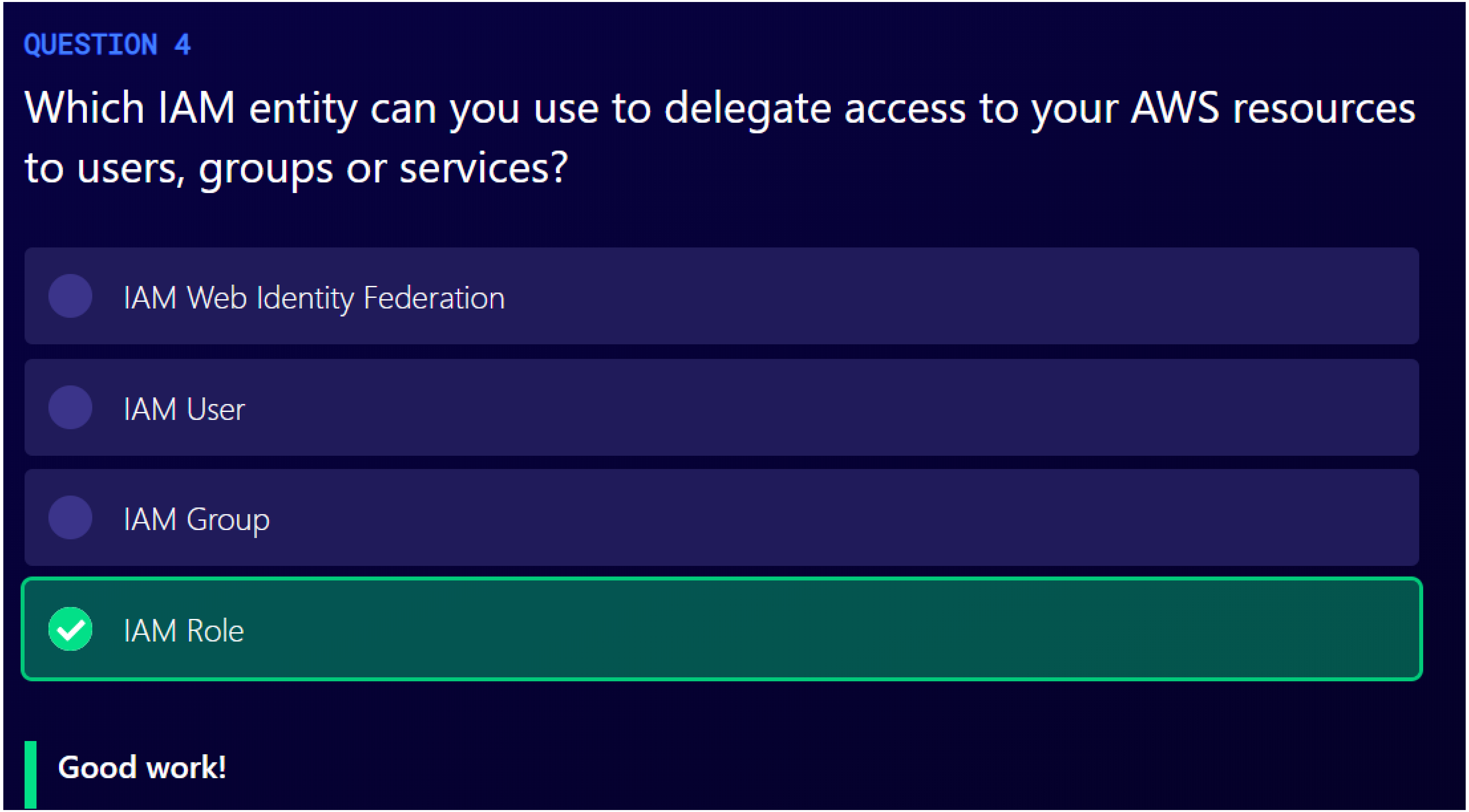


QUESTION 3

What is an IAM Policy?

- ○ A file containing a user's private SSH key
- ○ A CSV file which contains a users Access Key and Secret Access Key
- ○ The policy which determines how your AWS bill will be paid
- ✓ A JSON document which defines one or more permissions

Good work!

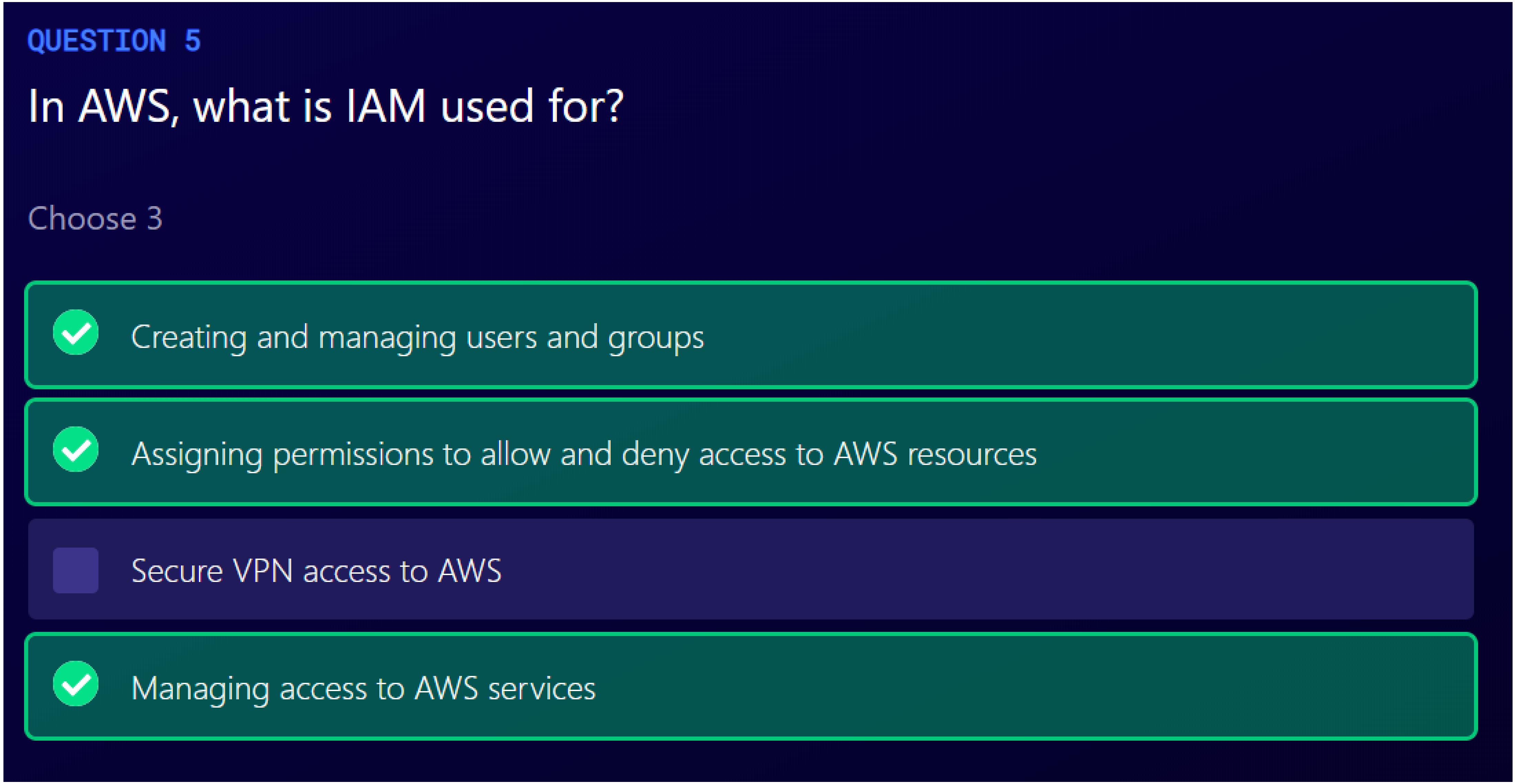


QUESTION 4

Which IAM entity can you use to delegate access to your AWS resources to users, groups or services?

- ○ IAM Web Identity Federation
- ○ IAM User
- ○ IAM Group
- ✓ IAM Role

Good work!



QUESTION 5

In AWS, what is IAM used for?

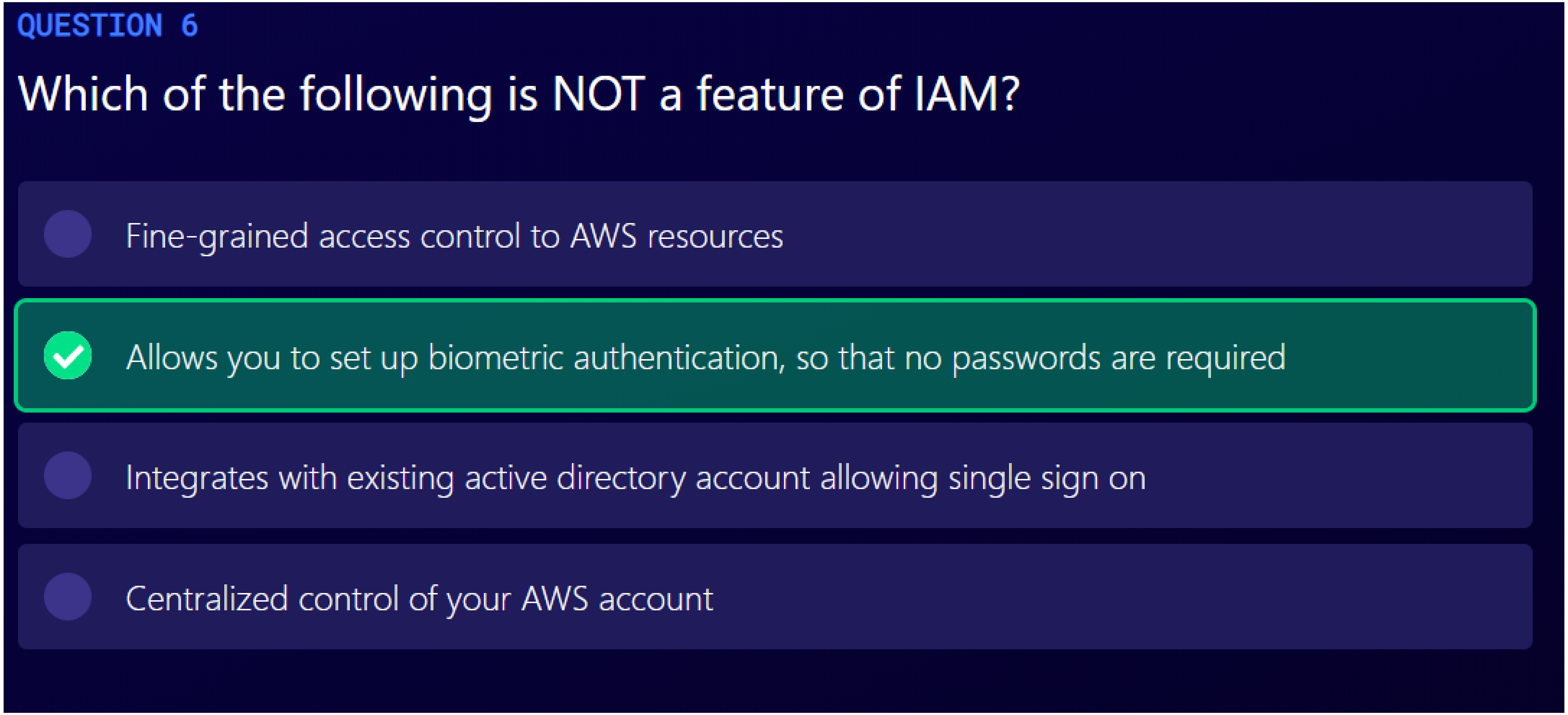
Choose 3

✓ Creating and managing users and groups

✓ Assigning permissions to allow and deny access to AWS resources

□ Secure VPN access to AWS

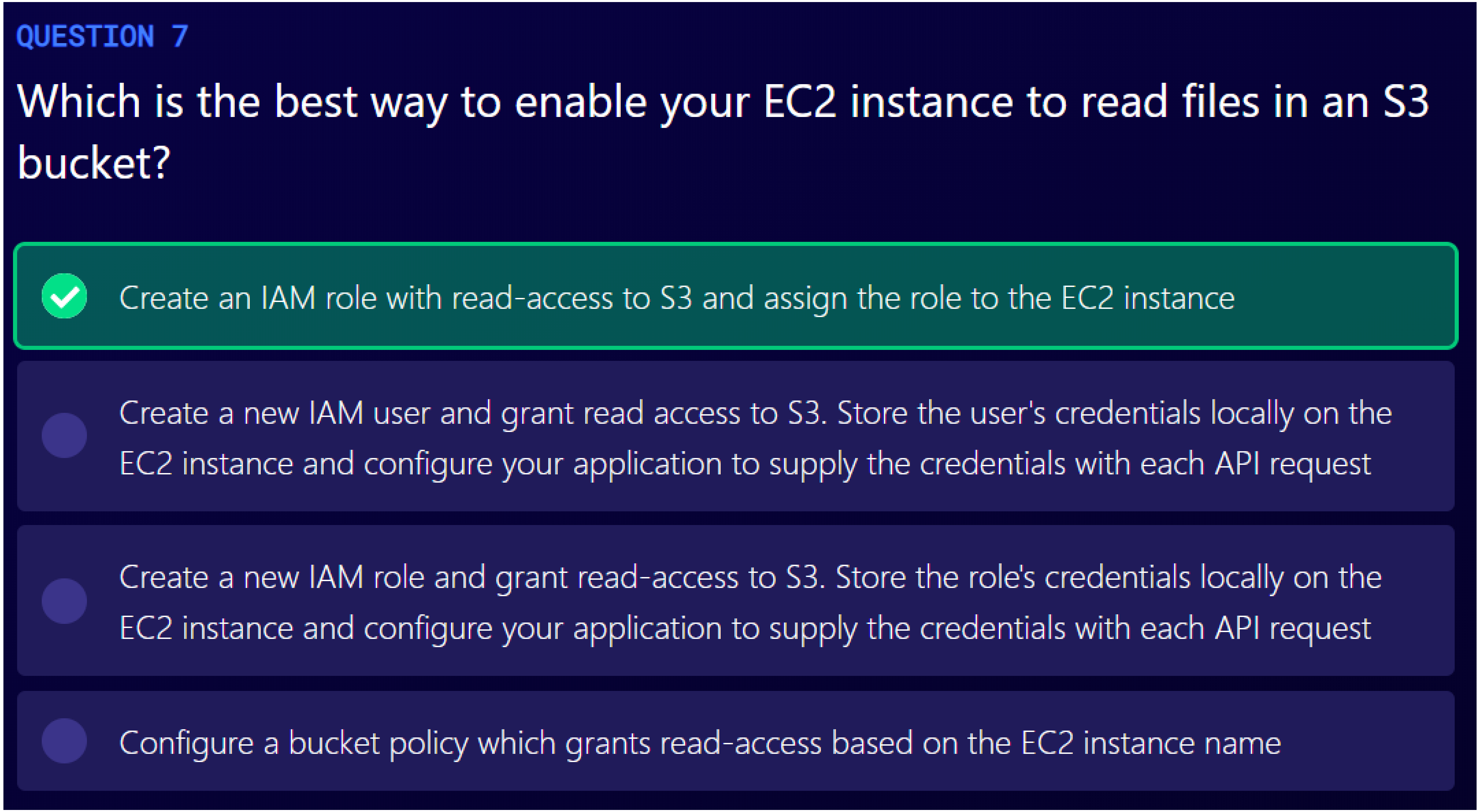
✓ Managing access to AWS services



QUESTION 6

Which of the following is NOT a feature of IAM?

- ○ Fine-grained access control to AWS resources
- ✓ Allows you to set up biometric authentication, so that no passwords are required
- ○ Integrates with existing active directory account allowing single sign on
- ○ Centralized control of your AWS account



QUESTION 7

Which is the best way to enable your EC2 instance to read files in an S3 bucket?

- ✓ Create an IAM role with read-access to S3 and assign the role to the EC2 instance
- ○ Create a new IAM user and grant read access to S3. Store the user's credentials locally on the EC2 instance and configure your application to supply the credentials with each API request
- ○ Create a new IAM role and grant read-access to S3. Store the role's credentials locally on the EC2 instance and configure your application to supply the credentials with each API request
- ○ Configure a bucket policy which grants read-access based on the EC2 instance name