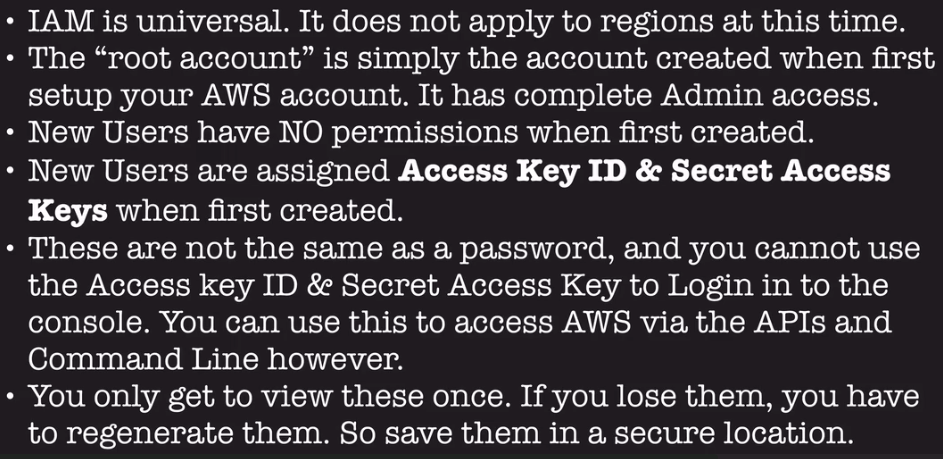
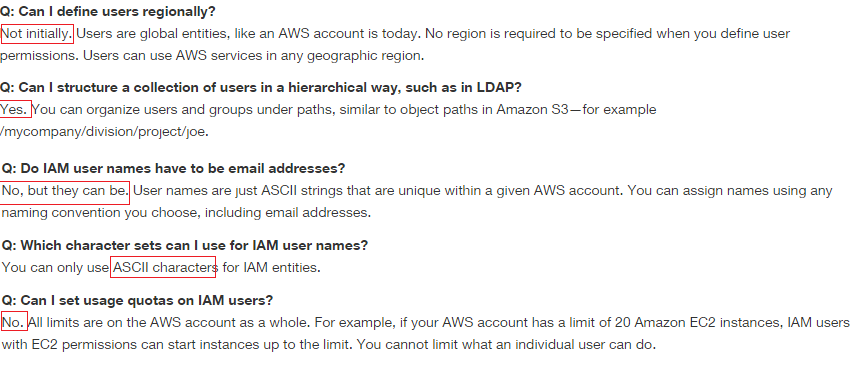
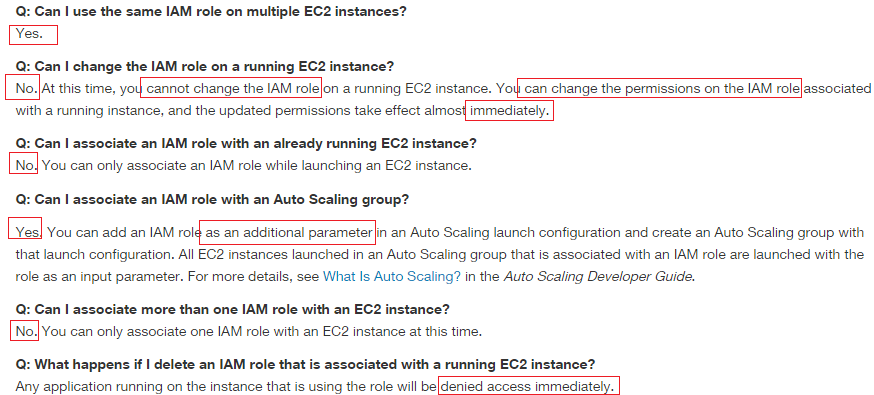
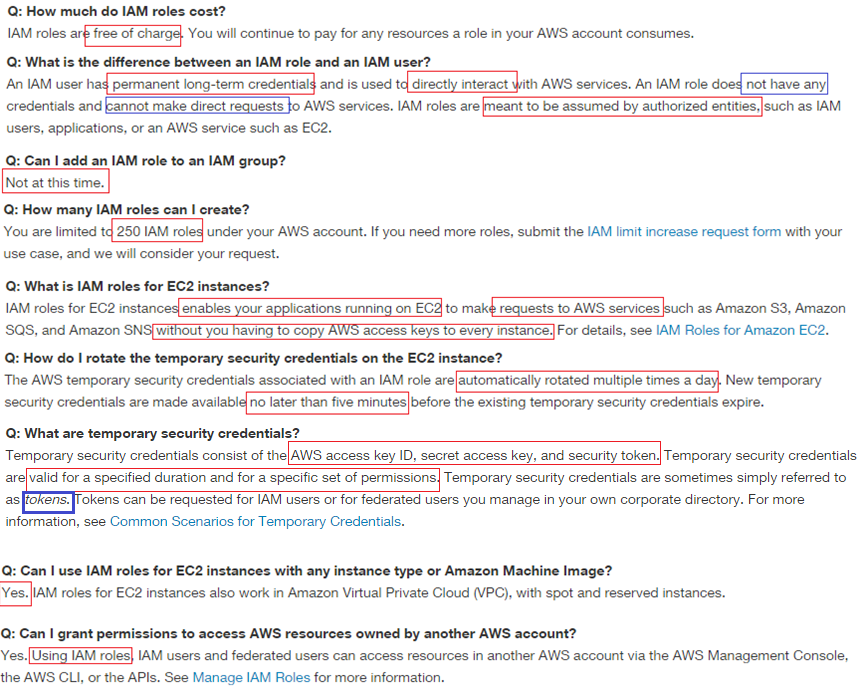
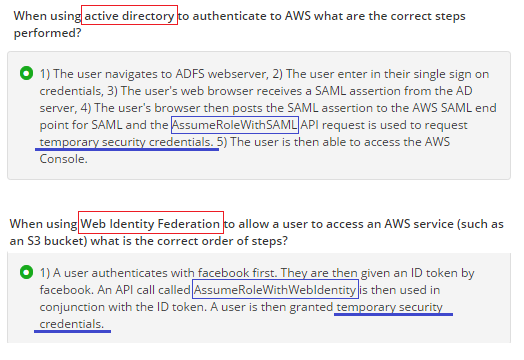
# IAM





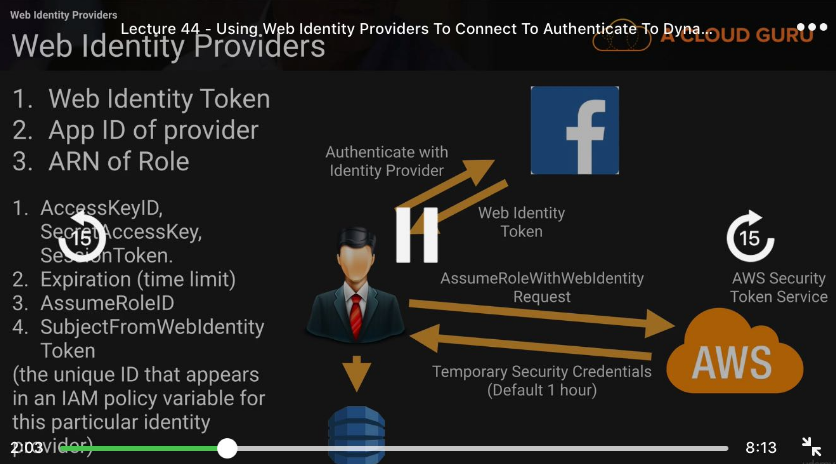




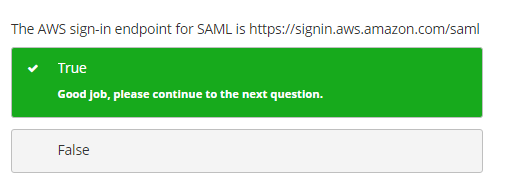


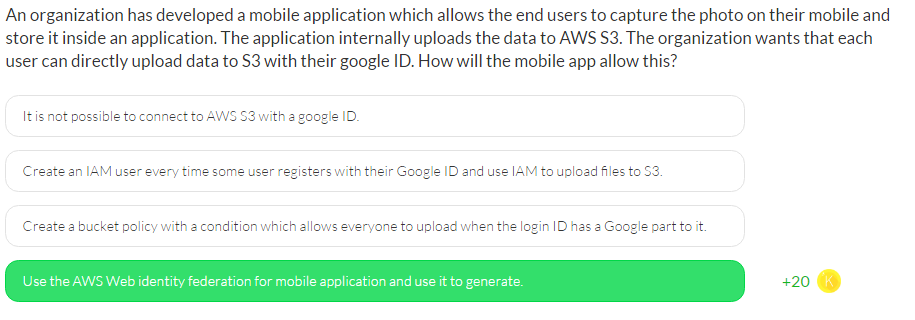
|  |  |
| --- | --- |
|  | 1) The user navigates to ADFS webserver  2) The user enter in their single sign on credentials,  3) The user's web browser receives a SAML assertion from the AD server,  4) The user's browser then posts the SAML assertion to the AWS SAML end point for SAML and the AssumeRoleWithSAML API request is used to request temporary security credentials.  5) The user is then able to access the AWS Console. |

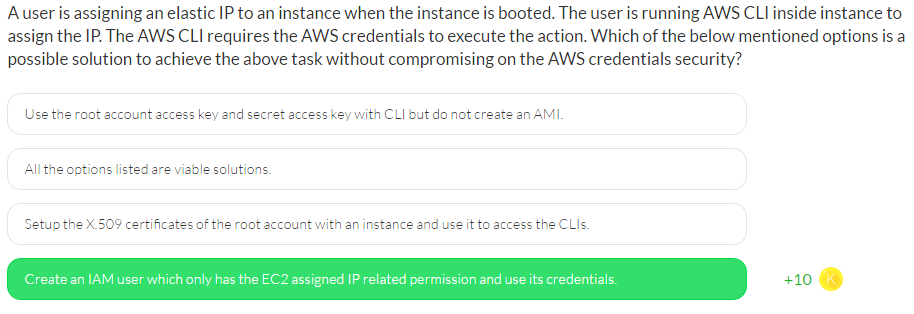
|  |  |
| --- | --- |
|  | 1) A user authenticates with facebook first.  2) They are then given an ID token by facebook.  3) An API call called AssumeRoleWithWebIdentity is then used in conjunction with the ID token.  4) A user is then granted temporary security credentials. |

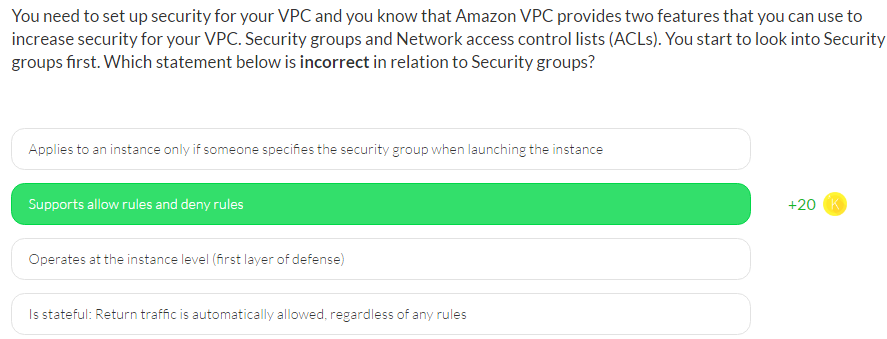


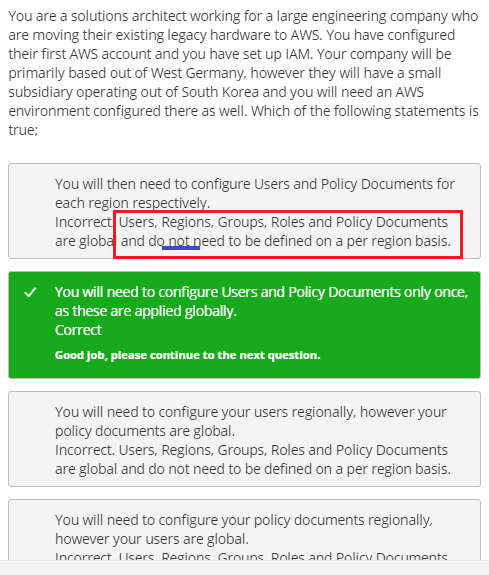
Steps:

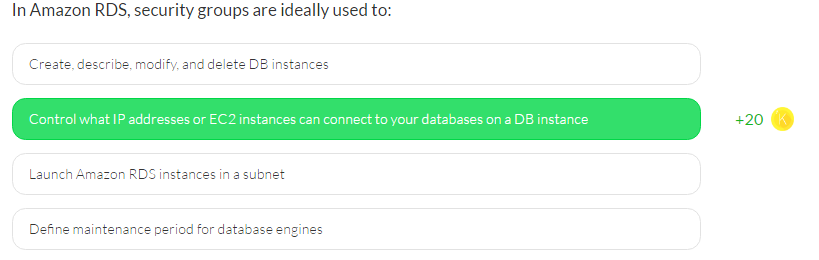


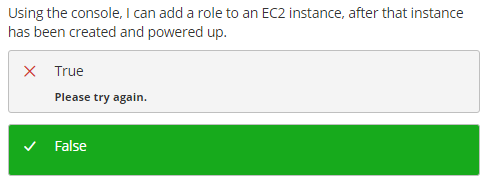


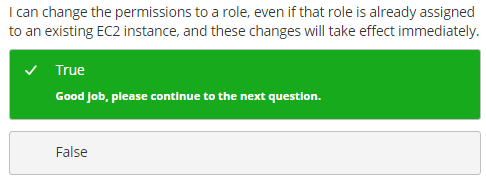


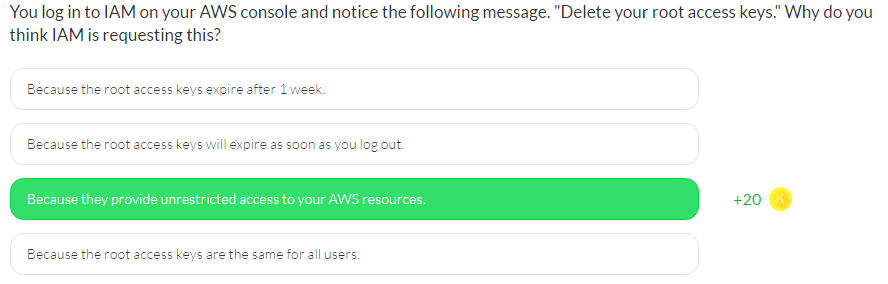


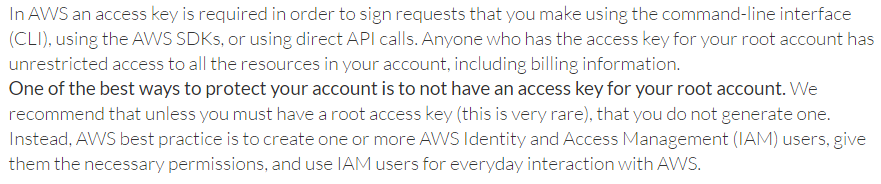


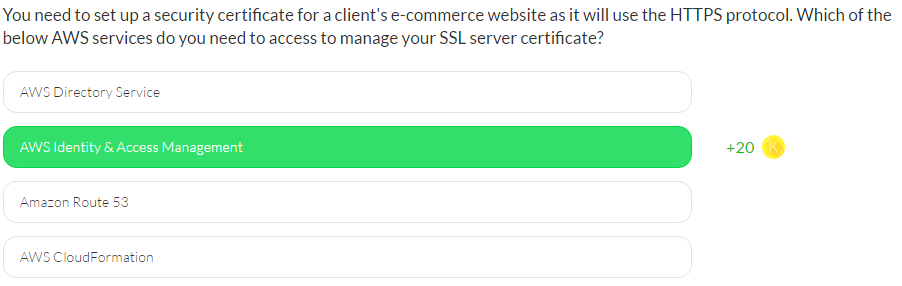






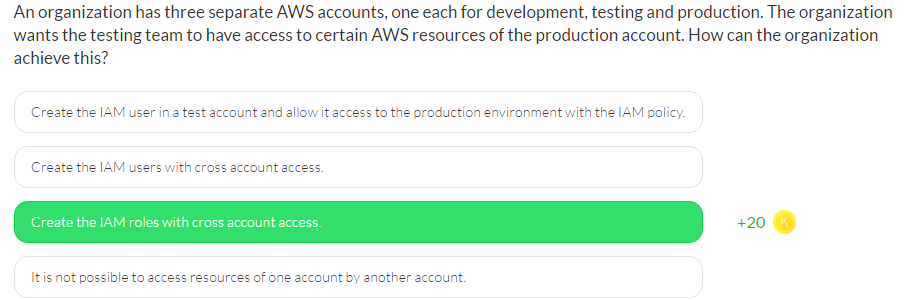


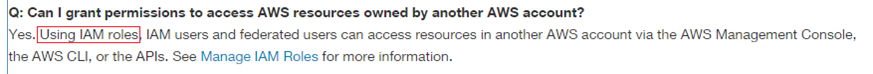


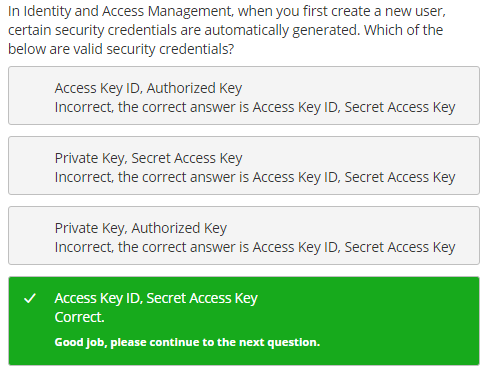


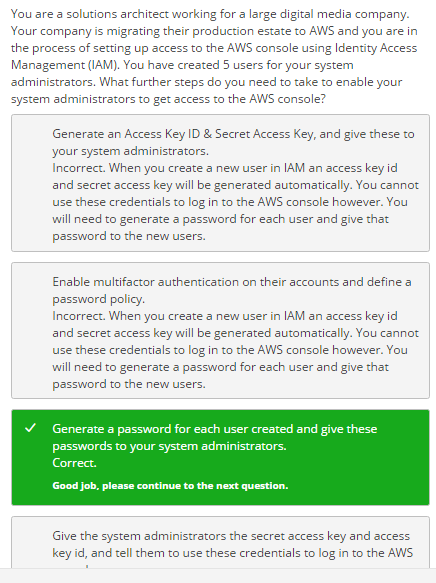
AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.

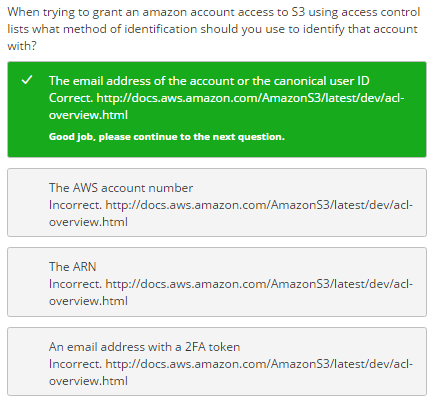
All your SSL server certificates are managed by AWS Identity and Access management (IAM).

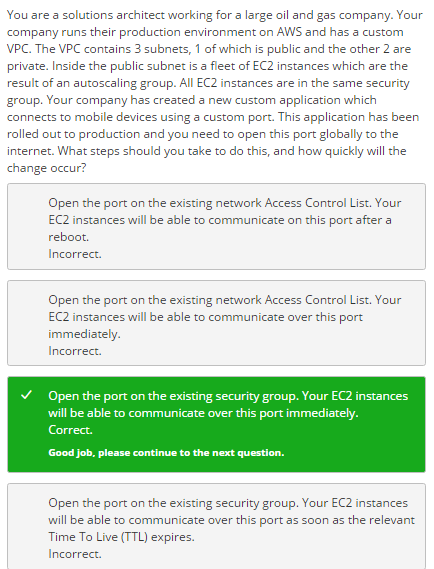


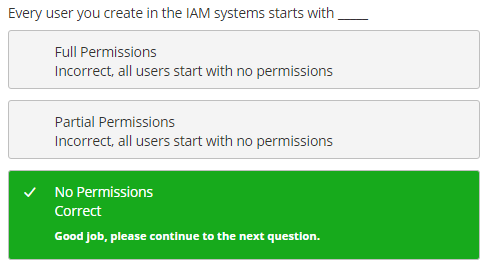


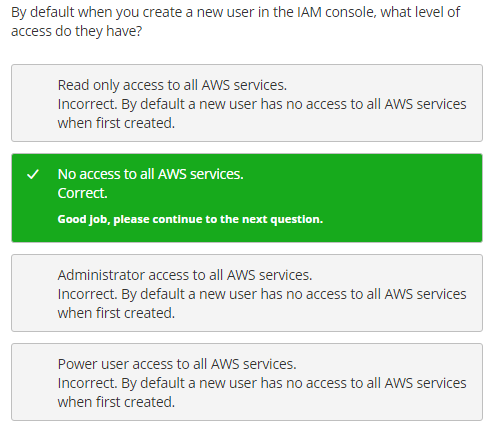


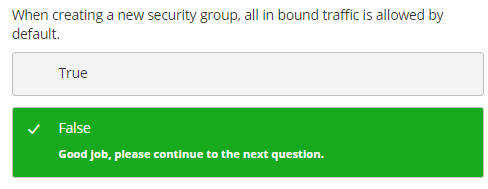


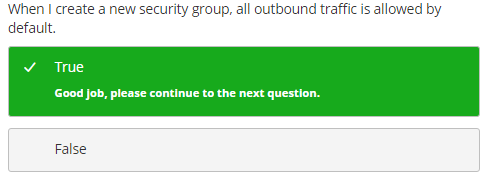


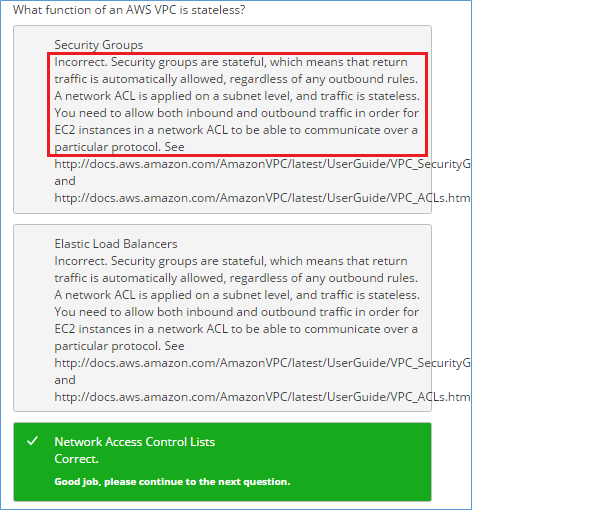


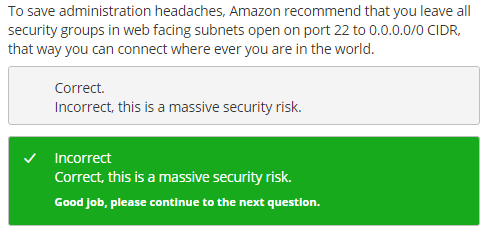


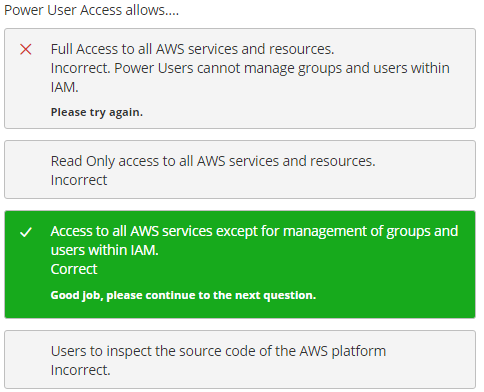


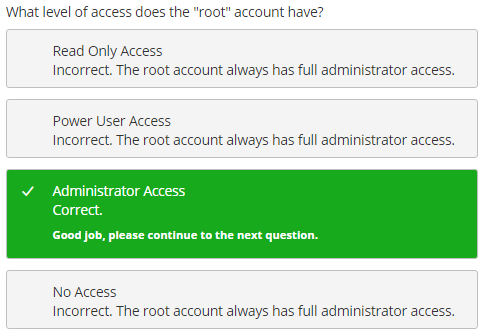


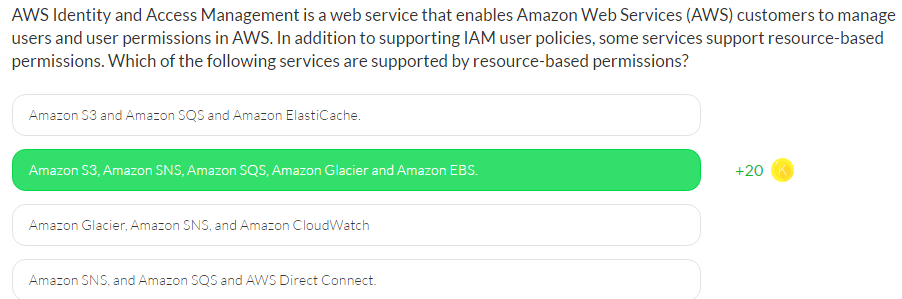


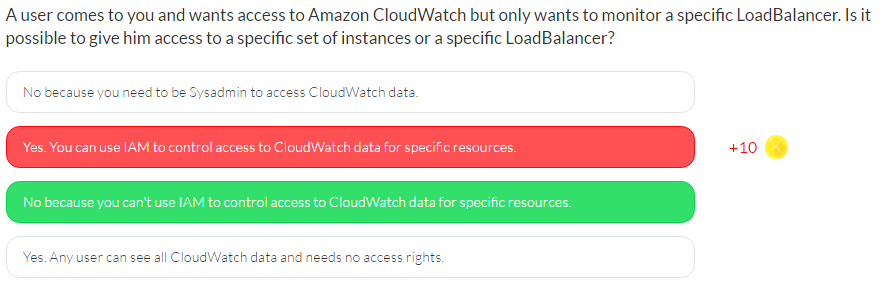


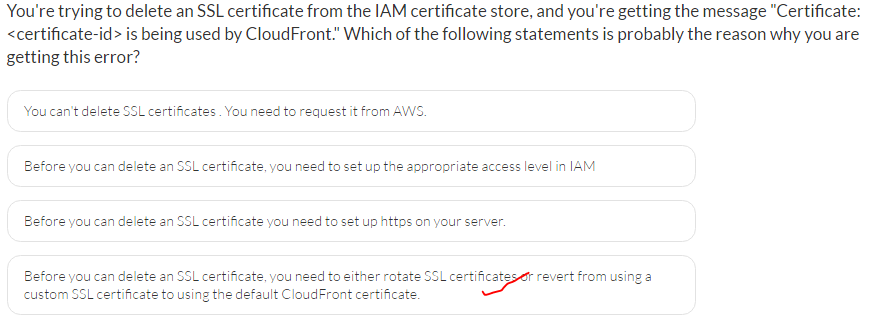


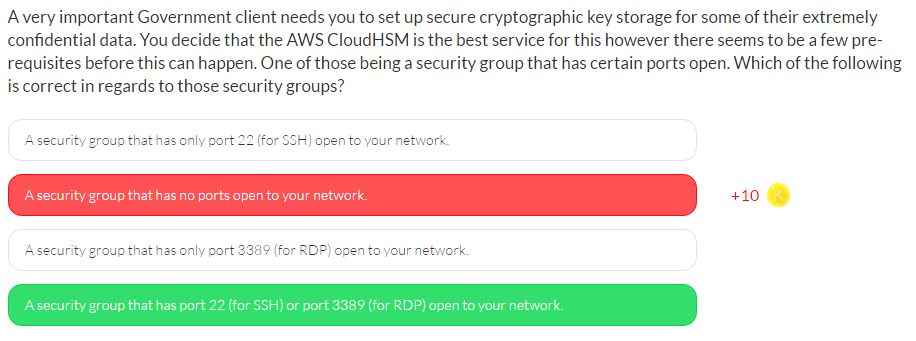


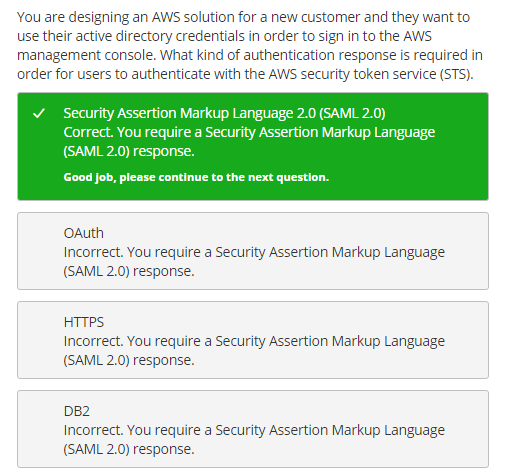


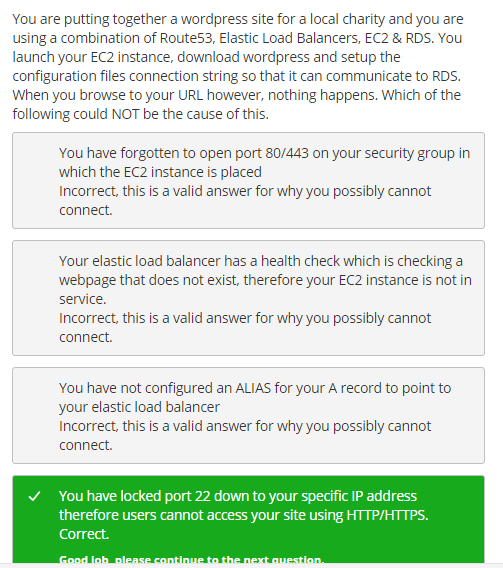




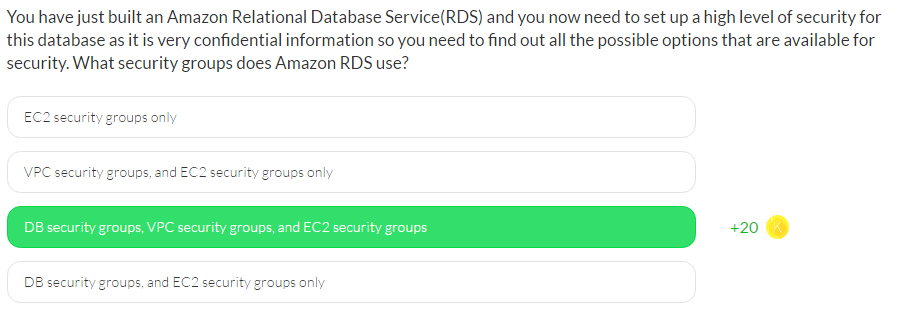


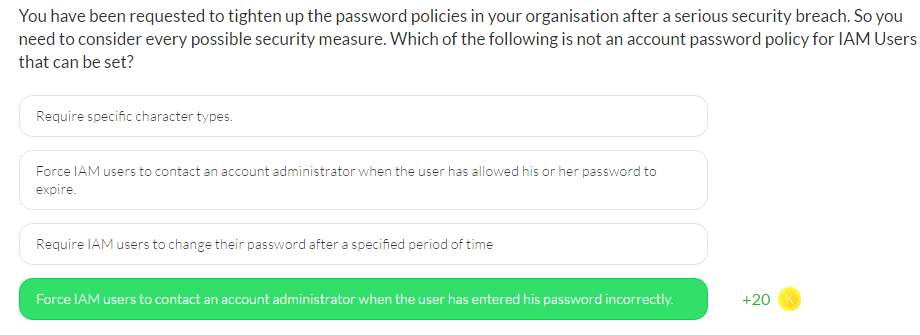


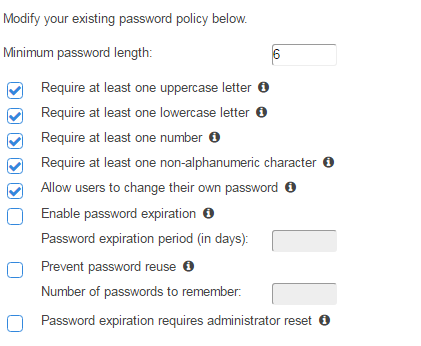


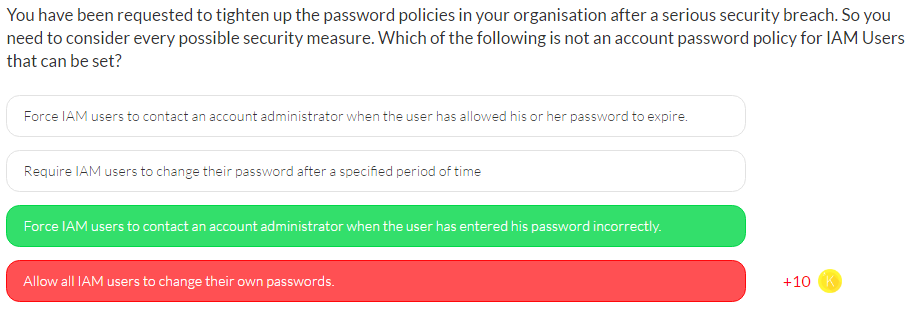


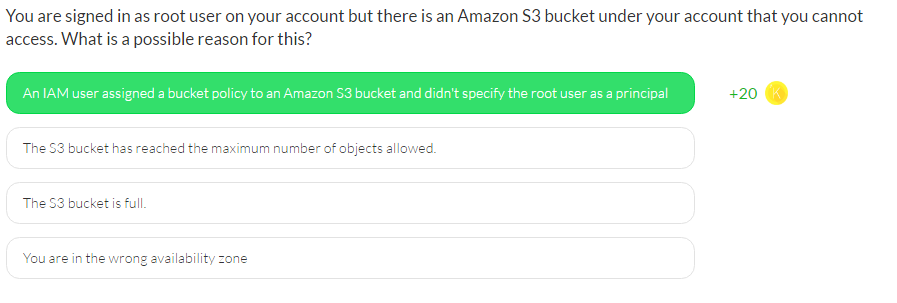
Bcoz Port 22 is for SSH.









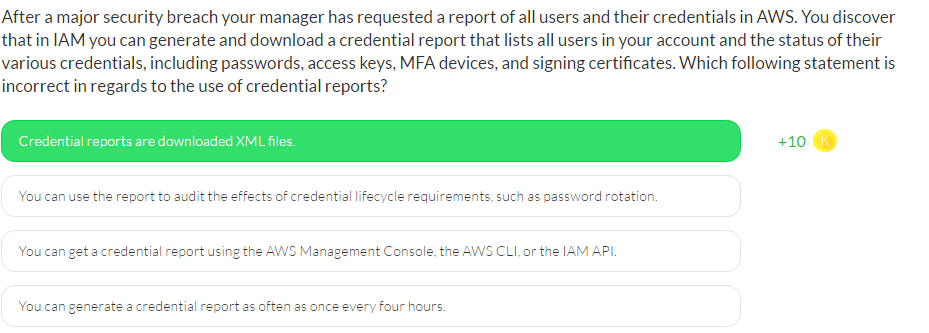


With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

In some cases, you might have an IAM user with full access to IAM and Amazon S3.

If the IAM user assigns a bucket policy to an Amazon S3 bucket and doesn't specify the root user as a principal, the root user is denied access to that bucket.

However, as the root user, you can still access the bucket by modifying the bucket policy to allow root user access



# Directory Service

# KMS

# Cloud HSM

