Quiz: IAM

Chandra Lingam,

1. Identity and Access Management is used to control:
   A. Access to specific AWS services
   B. Actions user can perform on specific AWS services
   C. Multi Factor Authentication on Users
   D. Identity federation
   E. All the above
2. You would like to give administrative privileges to your AWS resources. What is the recommended approach?
   A. Use Root account and credentials
   B. Create one admin account and share with the pool of developers
   C. Each user must have their own account and credentials with Multi factor authentication enabled
   D. Any of the above
3. If IAM users create AWS resources, who is responsible for paying the bills?
   A. IAM User Account
   B. IAM Group Account
   C. IAM Role Account
   D. Root Account
4. You have an application running in your data center and application needs to access S3. You created an IAM user account for this application and granted necessary policy permissions to access S3. What additional steps need to be completed for your application to access S3?
   A. Assign a password for this account
   B. Assign Access Key credentials for the user account
   C. Either Password or Access Key Credentials
5. Your company already has a corporate directory that is Security Assertion Markup Language 2.0 compliant for maintaining identities of the employees. If your employees need access to AWS Services, you need to:
   A. Create corresponding identities in IAM and link them with corporate directory
   B. Use Identity federation and configure your corporate directory to provide single sign on access to AWS Management Console
   C. Create corresponding IAM identities with matching password as one-time setup and synchronize automatically from that point onward with corporate directory
   D. Any of the above would work
6. You company has a Finance department user named Alice. You use IAM to manage your users. You delete the user after Alice left the organization.
   After few months, another person named Alice joined the organization's IT department. Now you created a new IAM account with the same name Alice.
   S3 has a finance bucket that granted access to original Alice using the ARN: *arn:aws:iam::123456789012:user/Alice*; this permission still exists as part of bucket level policy.
   The newly joined Alice also has the same ARN; would she be able to access the S3 finance bucket?

A. Yes

B. No

7. In your web application, you allow users to register with their existing identifies with external internet identity providers like Amazon, Google, Facebook and other OpenID Connect compatible identity providers. Once authenticated, your users should be able to access specific AWS services related to your application. Which one of these choices is recommended on AWS?

A. Verify user identity with external providers from your web application. Once user is authorized, use application credentials to access AWS Services

B. Verify identity of the user using Cognito service. Authorized users are mapped to IAM role defined and they will gain temporary privileges defined in that role

C. Verify identity of the user using Cognito service. Once user identity is verified, Cognito grants permanent access credentials to user. These credentials can be revoked anytime by your web application

D. Create corresponding User identities in IAM and grant them necessary privileges

8. When you create a new IAM user, default privileges the user has are:

A. Read access to services excluding Billing

B. Read access

C. Any actions or resources that are not explicitly allowed are denied

D. Any actions or resources that are not explicitly denied are allowed by default

9. Can IAM User belong to more than one IAM Group?

A. Yes

B. No

10. Can you add IAM Group as a child of another IAM Group?

A. Yes

B. No

Answers:

1. E – IAM allows you limit access to a service, actions that are allowed or denied, MFA, Identity Federation
2. C – Credentials must not be shared. Each user must have their own account and credentials. MFA must be enabled for administrative actions.
3. D – Root account is responsible for resources under the account
4. B - Access Key + Secret Access Key credentials allow you to make SDK/API calls to AWS Services
5. B - SAML 2.0 based federation. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization
6. B - Each user has a unique ID. Policies internally map to the unique ID when storing permissions. ARN is transformed to the user's unique principal ID when the policy is saved. This helps mitigate the risk of someone escalating their privileges by removing and recreating the user.
7. B - Cognito service is useful for identify federation and maps authenticated users to a role. Users are granted temporary credentials to access the resources
8. C - Users are granted access to explicitly allowed resources. Default deny applies to all other resources

9. A - IAM User can belong to multiple groups
10. B – IAM does not allow nesting or hierarchy of groups