AWS Solutions Architect (IAM)

Total points 9/9

Check out https://T3chFlicks.org for our content!

✓ An EC2 Instance hosts an application that accesses a DynamoDB table. This EC2 Instance is currently running in production. What would be a secure way for the EC2 Instance to access the DynamoDB table? 1/1

● A. Use IAM Roles with permissions to use DynamoDB and assign it to the EC2 Instance ✓

○ B. Use KMS Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

○ C. Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

○ D. Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance.

Feedback

Answer - A
Always assign a role to the EC2 Instance to ensure secure access to AWS resources from EC2 Instances.
For more information on IAM Roles, please refer to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html An IAM role is similar to a user; it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, an IAM role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that normally don't have access to your AWS resources. Note: You can attach IAM role to the existing EC2 instance. To know more, please visit the following URL: https://aws.amazon.com/about-aws/whats-new/2017/02/new-attach-an-iam-role-to-your-existing-amazon-ec2-instance/",

✓ A concern raised in your company is that developers could potentially delete production EC2 resources. What would you do to help alleviate this concern? (SELECT TWO) 2/2

☑ A. Tag the production instances with production-identifying tag and add resource-level permissions to the developers with an explicit deny on the terminate API call to instances with the production tag. ✓

☑ B. Create a separate AWS account and move the developers to that account. ✓

□ C. Modify the IAM policy on the production users to require MFA before deleting EC2 instances, and disable MFA access to the employee.

□ D. Modify the IAM policy on the developers to require MFA before deleting EC2 instances

Feedback

Answers – A and B
Creating a separate AWS account for developers will help the organization to facilitate the highest level of resource and security isolation.

The AWS documentation gives us a clear picture of the scenarios when we need to consider creating multiple accounts. When to Create Multiple Accounts
While there is no one-size-fits-all answer for how many AWS accounts a particular customer should have, most companies will want to create more than one AWS account because multiple accounts provide the highest level of resource and security isolation. Answering “yes” to any of the following questions is a good indication that you should consider creating additional AWS accounts:

Does the business require administrative isolation between workloads?

Administrative isolation by account provides the most straightforward approach for granting independent administrative groups different levels of administrative control over AWS resources based on the workload, development lifecycle, business unit (BU) or data sensitivity.

Does the business require limited visibility and discoverability of workloads? Accounts provide a natural boundary for visibility and discoverability. Workloads cannot be accessed or viewed unless an administrator of the account enables access to users managed in another account.

Does the business require isolation to minimize the blast radius?
Blast-radius isolation by account provides a mechanism for limiting the impact of a critical event such as a security breach in case of the unavailability of AWS Region or Availability Zone, account suspensions, etc. Separate accounts help define boundaries and provide natural blast-radius isolation.

Does the business require strong isolation of recovery and/or auditing data?
Businesses that are required to control access and visibility to auditing data due to regulatory requirements can isolate their recovery data and/or auditing data in an account separate from where they run their workloads (e.g., writing CloudTrail logs to a different account).

For more information, please check the URL below: https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Security_Strategy.pdf

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define. For more information on tagging AWS resources, please refer to the below URL:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

The question says that the developers should not have the option to delete production-based resources.
So, option A and B completely keep the developers away from production resources.
You wish to use MFA, which means developers can delete the production-based resources if they know MFA code which is not recommended.
AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on the top of your user name and password.
With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. Organizations have good control over newly created accounts rather than old AWS accounts. Because they can easily monitor and maintain (few) assigned permissions on accounts and they delete those accounts once the required task will be done.

✓ A company has set up an Amazon Aurora cluster. They have a Lambda function which needs to insert records into a DynamoDB table. The Amazon Aurora cluster needs to invoke the Lambda. Which of the following are required for the system to work correctly (Choose TWO) 2/2

☐ A. Ensure that the Lambda function has an IAM Role assigned to it which can be used to invoke functions on Amazon Aurora

☑ B. Ensure that the Amazon Aurora cluster has an IAM Role which allows it to invoke Lambda functions ✓

☐ C. Allow the Lambda function to allow outbound communication to Amazon Aurora

☑ D. Allow the Amazon Aurora cluster to allow outbound communication to the Lambda function ✓

Feedback

Answer – B and D
The below snapshot from the AWS Documentation shows what are the different steps required to ensure that the Lambda function has access to Amazon Aurora
Options A and C are incorrect since the configurations need to be the other way around
For more information on invoking AWS Lambda using Aurora, please refer to the below URL
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html#AuroraMySQL.Integrating.LambdaAccess

✓ You have a dockerized application which you plan to deploy to an ECS cluster. Te application gets configuration files from an S3 bucket, the ECS containers should have the AmazonS3ReadOnlyAccess permission. What is the correct method to configure the IAM permission? 1/1

○ A. Add an environment to the ECS cluster configuration to allow the S3 read only access.

○ B. Add the AmazonS3ReadOnlyAccess permission to the IAM entity that creates the ECS cluster.

○ C. Modify the user data of ECS instances to assume an IAM role that has the AmazonS3ReadOnlyAccess permission.

● D. Attach the AmazonS3ReadOnlyAccess policy to the ECS container instance IAM role. Attach this role when creating the ECS cluster ✓

Feedback

Correct Answer – D ECS containers have access to permissions that are supplied to the container instance role. Details please check the ECS documentation in https://docs.aws.amazon.com/AmazonECS/latest/developerguide/instance_IAM_role.html.
Option A is incorrect: Because ECS cluster uses the container instance IAM role instead of environment variables to control its permissions.
Option B is incorrect: Because the IAM entity that creates the ECS cluster does not pass its permissions to the ECS cluster. You need to configure an IAM role and attach it to the ECS cluster.
Option C is incorrect: This is not the correct method to configure IAM permissions for an ECS cluster.
Option D is CORRECT: After the AmazonS3ReadOnlyAccess policy is attached to the IAM role, the ECS instances can use the role to get objects from S3.

✓ You are going to deploy an application on Amazon EC2 that must call AWS APIs. Which method would you use to allow the application access to the APIs in a secure way? 1/1

○ A. Pass API credentials to the instance using Instance userdata.

○ B. Store API credentials as an object in Amazon S3

○ C. Embed the API credentials into your application.

● D. Assign IAM roles to the EC2 Instances ✓

Feedback

Answer - D
You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. It is not a good practice to use IAM credentials for a production-based application. However, it is a good practice to use IAM Roles.

✓ You have created a Lambda function that will write data to a DynamoDB table. What must be in place to ensure that the Lambda function can interact with the DynamoDB table?

1/1

● A. Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges. ✓

○ B. Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.

○ C. Ensure the Access keys are embedded in the AWS Lambda function.

○ D. Ensure the IAM user password is embedded in the AWS Lambda function.

Feedback

Answer – A
AWS Documentation mentions the following to support this requirement: Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

✓ There are production and development instances running in a VPC. You need to ensure that people responsible for the development instances do not have access to work on production instances for better security. What is the best way to accomplish this using policies? 1/1

○ A. Launch the development and production instances in separate VPCs and use VPC Peering.

○ B. Create an IAM group with a condition that allows access to only those instances which are used for production or development.

○ C. Launch the development and production instances in different Availability Zones and use Multi-Factor Authentication.

● D. Define the tags on the Development and production servers and add a condition to the IAM Policy which allows access to specific tags. ✓

Feedback

Answer – D You can easily add tags to define which instances are the production instances and which ones are development instances. These tags can then be used while controlling access via an IAM Policy. For more information on tagging your resources, please refer to the link below. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html Note: It can be done with the help of option B as well. However, the question is looking for the \"best way to fulfill the requirement using policies\". By using the option D, you can reduce the usage of different IAM Policies on each instance.

Would you like to sign up for T3chFlicks Newsletters? (Put your email here)

....