AWS_SCS-C00 Exam

Volume: 80 Questions

Question: 1
You are configuring a new VPC for one of your clients for a cloud migration project, and only a public subnet will be in place. After you have created your VPC, you created a new subnet, a new internet gateway, and attached your internet gateway to your VPC. When you launched your first instance into your VPC, you realized that you aren't able to connect to the instance, even if it is configured with an elastic IP. What should be done to get this instance internet connectivity?

A. A NACL should be created that allows all outbound traffic.

B. A NAT instance should be created, and all traffic should be forwarded to NAT instance.

C. A route should be created as 0.0.0.0/0 with your internet gateway as the target.

D. Attach another ENI to the instance and connect via the new ENI.

Answer: C

Explanation: All traffic should be routed via internet gateway, so a route should be created with 0.0.0.0/0 as a source, and with your Internet Gateway as the target.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

Question: 2
To directly manage your CloudTrail security layer, you can use ____ for your CloudTrail log files.

A. SCE-S3

B. SSE-S3

C. SCE-KMS

D. SSE-KMS

Answer: D

Explanation: By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3). To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS–managed keys (SSE-KMS) for your CloudTrail log files.
Reference:

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

Question: 3
You have been contracted to start building the latest and greatest mobile chat app. The schedule for this development and delivery is time critical. What correct mix of AWS services/components should you consider using to ensure that your mobile chat app can be productionised on time, ensuring that the mobile chat app can authenticate and authorise users.

A. Configure Amazon Cognito together with IAM Roles and Policies, leverage the AWS Mobile SDK within the mobile chat app to perform user authentication and authorisation

B. Create auto scaling group of EC2 instances with custom and specialised authentication and authorisation logic using SSL and JWT tokens to perform user authentication and authorisation

C. Create auto scaling group of EC2 instances with SAML 2.0 service endpoint, setup and install a custom LDAP directory, configure SSO within the mobile app to use the SAML 2.0 service endpoint to perform user authentication and authorisation

D. Configure Amazon CloudFront in association with AWS WAF to perform user authentication and authorisation

Answer: A

Explanation: Answer "Configure Amazon Cognito together with IAM Roles and Policies, leverage the AWS Mobile SDK within the mobile chat app to perform user authentication and authorisation" is correct. The question highlights that the "development and delivery is time critical" - therefore the best approach time wise is to use the fit for purpose managed services provided by AWS - in this case Amazon Cognito, IAM Roles and Policies, and the AWS Mobile SDK.
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc_cognito.html

Question: 4
Your customer will be storing critical data in S3 buckets. In addition to a highly restrictive bucket policy, they would like to encrypt the data prior to loading it to the buckets and avoid storing master keys off premises. Which of the following options would it be best to leverage to encrypt the data given the requirements?

A. SSE-KMS

B. SSE-S3

C. KMS–Managed CMK

D. Client-Side Master Key

Answer: D

Explanation: Given the requirement to encrypt the data prior to loading it to the S3 buckets, server side solutions like SSE-S3 and SSE-KMS would not meet the requirements. While a KMS-Managed CMK would allow for client-side encryption, it would not keep master key out of AWS. Using a Client-Side Master Key would allow for client-side encryption and keep the master key out of AWS.
Reference:
http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

Question: 5
You have been requested to review and document an existing IAM policy that has been attached to via an IAM Role to instance .

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AttachVolume",
"ec2:DetachVolume"
],
"Resource": [
"arn:aws:ec2:us-west-1:123456789012:volume/*",
"arn:aws:ec2:us-west-1:123456789012:instance/*"
],
"Condition": {
"ArnEquals": {
"ec2:SourceInstanceARN":
"arn:aws:ec2:us-west-1:123456789012:instance/i-0a57a24800d7d6ce9"
}
}
}
]
}
```

Which of the following statements are false regarding the policy (select 2)

A. The policy disallows the EC2 instance i-0a57a24800d7d6ce9 to detach volumes from other instances

B. The policy allows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9

C. The policy allows the EC2 instance i-0a57a24800d7d6ce9 to attach volumes to other instances

D. The policy disallows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9

Answer: A,D

Explanation: Answers "The policy disallows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9" and "The policy disallows the EC2 instance i-0a57a24800d7d6ce9 to detach volumes from other instances" are the correct false answers . The quick approach to answer this question is to consider the Effect attribute which is set to Allow, meaning there are no explicit deny/disallows in the policy. The only other consideration within the question is the answer "The policy allows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9", here although the policy is implying that the permissions are granted only when the source instance id is i-0a57a24800d7d6ce9, the policy as a whole still allows this instance to attach EBS volumes to itself.
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_ec2_volumes-instance.html

Question: 6
You have an application that is generating a log file every 5 minutes and you need to store these log files appropriately. The requirements for storing the log files are:
. They should be quickly retrievable when needed, as they may be required only for verification in case of some major issue.
. They logs will need to be accessed frequently, as all log data is retrieved and compiled from the files into a bi-monthly.
. Cost should also be minimized for the storage service as much as possible.
Which of the storage options below is the best choice to meet these requirements?

A. Amazon S3 Standard

B. Amazon S3 Standard - Infrequent Access

C. Amazon Glacier

D. Amazon S3-RRS

Answer: A

Explanation: Amazon S3 stores objects according to their storage class. There are technically four major storage classes: Standard, Standard - Infrequent Access, Reduced Redundancy Storage (RRS) and Glacier.
Standard is for Amazon S3 and provides very high durability. Standard - Infrequent Access is designed for with a minimum data amount required and paid storage for at least 30 days. Glacier is for archival and the files are not available over the internet. Reduced Redundancy Storage is for less critical files.
Until recently, Reduced Redundancy was a little cheaper as it provides less durability in comparison to S3's other storage options. However, Standard is now the cheaper option.
For example, Reduced Redundancy Storage is now $0.024 per GB for the first TB of storage, and $0.0236 per GB for the next 49 TB. Standard is $0.023 per GB for the first 50 TB.
While in the past S3 RRS would be ideal, now S3 Standard is the better choice when considering both durability and cost. So the best choice is S3 Standard Storage class
Reference: https://aws.amazon.com/s3/pricing/

Question: 7
How does the following Amazon S3 bucket policy improve the security of your S3 bucket?

```
{
"Version":"2012-10-17",
"Id":"BucketPolicy",
"Statement":[{
"Sid":"ConditionalObjectUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::YourBucket/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}]
}
```

A. By ensuring that all objects being uploaded into your S3 bucket are encrypted.

B. By denying access to objects uploaded by IAM users without the proper permissions.

C. By denying access to IAM users without the correct string attachment.

D. By ensuring that all objects in your S3 bucket are automatically encrypted.

Answer: A

Explanation: This policy denies uploads of objects that are not encrypted, thus ensuring that all objects being uploaded are encrypted. Note that this doesn't cause objects already in the bucket to be encrypted.
Reference: https://d0.awsstatic.com/whitepapers/aws-kms-best-practices.pdf

Question: 8
You've taken over management of your company's AWS cloud environment. You know very little about the environment and have been provided very little documentation. You have been given access to the environment and begin a discovery and documentation process. You begin by looking at the route table. Without seeing the specific route table, what information do you know it contains about the subnets in the VPC? (Choose 2 answers)

A. Subnets that do not direct traffic to an Internet Gateway are private.

B. Subnets that direct traffic to an Internet Gateway are public.

C. The subnets region is indicated.

D. The default mask of the subnet can be identified.

Answer: A,B

Explanation: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.
Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table. When you add an Internet gateway, an egress-only Internet gateway, a virtual private gateway, a NAT device, a peering connection, or a VPC endpoint in your VPC, you must update the route table for any subnet that uses these gateways or connections.
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

Question: 9
An error has occurred in your company's application and you are trying to retrace what happened. You come across this entry in the company's CloudTrail logs. What events have happened, according to this log entry? (Choose 2 answers)

```
{
"eventVersion": "1.02",
"userIdentity": {
"type": "IAMUser",
"principalId": "AIDACKCEVSQ6C2EXAMPLE",
"arn": "arn:aws:iam::086441151436:user/AWSCloudTrail",
"accountId": "086441151436",
"accessKeyId": "AKIAI44QH8DHBEXAMPLE",
"userName": "AWSCloudTrail",
"sessionContext": {"attributes": {
"mfaAuthenticated": "false",
"creationDate": "2015-11-11T21:15:33Z"
}},
"invokedBy": "internal.amazonaws.com"
},
"eventTime": "2015-11-11T21:15:33Z",
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKey",
"awsRegion": "us-west-2",
"sourceIPAddress": "internal.amazonaws.com",
"userAgent": "internal.amazonaws.com",
"requestParameters": {
"keyId": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailCMK",
"encryptionContext": {
"aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/Default",
"aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/AWSLogs/111122223333/"
},
"keySpec": "AES_256"
},
"responseElements": null,
"requestID": "581f1f11-88b9-11e5-9c9c-595a1fb59ac0",
"eventID": "3cdb2457-c035-4890-93b6-181832b9e766",
"readOnly": true,
"resources": [{
"ARN":
"arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
"accountId": "111122223333"
}],
"eventType": "AwsServiceEvent",
"recipientAccountId": "111122223333"
}
```


A. CloudTrail called the AWS KMS GenerateDataKey API.

B. The public portion of the CMK is arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailCMK.

C. AWS KMS created a data key under a specific CMK.

D. The user's pre-defined GenerateDataKey Java function was called by AWSCloudTrail.

Answer: A,C

Explanation: "resources": [{
"ARN":
"arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
"accountId": "111122223333"
}]
indicates that AWS KMS created a data key under a specific CMK.
"arn": "arn:aws:iam::086441151436:user/AWSCloudTrail"
[...]
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKey",
indicate that CloudTrail called the AWS KMS GenerateDataKey API.
Reference: http://docs.aws.amazon.com/kms/latest/developerguide/services-cloudtrail.html

Question: 10
Amazon Inspector could be used to assess target resources for potential security issues. What defines the rules against which target resources are being evaluated?

A. Amazon Inspector has a pre-defined set of rules, grouped into packages. Each Assessment Template defines which rules packages to be included in the test. Instances are being evaluated against rules packages included in the assessment template.

B. Amazon Inspector Rules could be defined based on organization policy and grouped into packages. Packages are applied during assessment test and target resources are being evaluated against all rules in applied packages.

C. Amazon Inspector has a pre-defined set of rules that cover best practices, during assessment run. Rules are determined based on AWS Resource type.

D. Amazon Inspector has a pre-defined set of rules. During assessment template creation, you can choose which rules to include in your test. These rules are grouped into package and associated with the assessment template.

Answer: A

Explanation: Amazon Inspector defines a fixed set of rules packages that are maintained by AWS and not editable, during the creation of Assessment Template you can choose one or more rules package to include in your assessment and all assessment targets will be evaluated against rules in all included packages.
Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html

Question: 11
Complete the following statement:
AWS IAM provides credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation.
You can generate an IAM credential report as often as once every _____.

A. 12 hours

B. 24 hours

C. 8 hours

D. 4 hours

Answer: D

Explanation: Answer "4 hours" is correct. You can generate a credential report as often as once every four hours. When you request a report, IAM first checks whether a report for the AWS account has been generated within the past four hours. If so, the most recent report is downloaded. If the most recent report for the account is older than four hours, or if there are no previous reports for the account, IAM generates and downloads a new report.
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html?icmpid=docs_iam_console

Question: 12
You need a simple and secure way to remotely execute commands or run scripts against AWS EC2 instances or on-premises servers. Which command would you use?

A. Run Command

B. remoteRun

C. executeScript

D. State Manager

Answer: A

Explanation: The Run Command can be used to remotely execute commands against EC2 instances or on-premises servers.
Reference: https://aws.amazon.com/ec2/systems-manager/faqs/

Question: 13
When creating metric filters in CloudWatch for your CloudTrail logs, you must create a _____ which determines what exactly you want CloudWatch to monitor and extract from your CloudTrail log files.

A. Filter string

B. Filter pattern

C. Search string

D. Search pattern

Answer: B

Explanation: When creating these metric filters, you must create a filter pattern which determines what exactly you want CloudWatch to monitor and extract from your files. These filter patterns are fully customizable strings, but as a result a very specific pattern syntax is required. So if you are creating these for the first time you must understand the correct syntax
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html

Question: 14
In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

A. Data persists in the instance store.

B. Data in the instance store will be lost.

C. Data is deleted from the instance store for security reasons.