DUMPSARENA

AWS Certified Security - Specialty (SCS-C01)

Amazon AWS AWS-Certified-Security-Specialty-SCS-C01

Version Demo

Total Demo Questions: 20

Total Premium Questions: 820

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.

B. Move the web servers to private subnets without public IP addresses.

C. Configure AWS WAF to provide DDoS attack protection for the ALB.

D. Require all inbound network traffic to route through a bastion host in the private subnet.

E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

ANSWER: B C

QUESTION NO: 2

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

A. IAM CloudTrail

B. Amazon Athena

C. IAM Key Management Service (IAM KMS)

D. VPC Flow Logs

E. IAM Firewall Manager

F. Security groups

ANSWER: A D F

Explanation:

https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_IAM_Console_and_CLI/Lab_Guide.md

QUESTION NO: 3

A company plans to create individual child accounts within an existing organization in IAM Organizations for each of its DevOps teams. IAM CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized IAM account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the IAM account root user.

B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the IAM account root user in the source account.

C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

ANSWER: D

QUESTION NO: 4

A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.

During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.

Which combination of options can the company use to meet these requirements? (Select TWO.)

A. Create a snapshot of the DB instance. Copy the snapshot to a new snapshot, and enable encryption for the copy process. Use the new snapshot to restore the DB instance.

B. Modify the configuration of the DB instance by enabling encryption. Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.

C. Use IAM Key Management Service (IAM KMS) to create a new default IAM managed awa/rds key. Select this key as the encryption key for operations with Amazon RDS.

D. Use IAM Key Management Service (IAM KMS] to create a new CMK. Select this key as the encryption key for operations with Amazon RDS.

E. Create a snapshot of the DB instance. Enable encryption on the snapshoVUse the snapshot to restore the DB instance.

ANSWER: C E

QUESTION NO: 5

A Security Engineer is trying to determine whether the encryption keys used in an IAM service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

A. Read the IAM Customer Agreement.

B. Use IAM Artifact to access IAM compliance reports.

C. Post the question on the IAM Discussion Forums.

D. Run IAM Config and evaluate the configuration outputs.

ANSWER: B

Explanation:

https://IAM.amazon.com/artifact/

Third-party auditors assess the security and compliance of IAM Key Management Service as part of multiple IAM compliance programs. These include SOC, PCI, FedRAMP, HIPPA, and others. The compliance document is found in IAM Artifact.

QUESTION NO: 6

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

- A trusted forensic environment must be provisioned.
- Automated response processes must be orchestrated.

Which AWS services should be included in the plan? (Choose two.)

A. AWS CloudFormation

B. Amazon GuardDuty

C. Amazon Inspector

D. Amazon Macie

E. AWS Step Functions

ANSWER: A B

Explanation:

Reference: https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/

QUESTION NO: 7

A recent security audit found that AWS CloudTrail logs are insufficiently protected from tampering and unauthorized access. Which actions must the Security Engineer take to access these audit findings? (Choose three.)

A. Ensure CloudTrail log file validation is turned on.

B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage.

C. Use an S3 bucket with tight access controls that exists in a separate account.

D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.

E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files.

F. Encrypt the CloudTrail log files with server-side encryption AWS KMS-managed keys (SSE-KMS).

ANSWER: A B F

Explanation:

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

QUESTION NO: 8

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside IAM (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an IAM account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

B. Block outbound access to public S3 endpoints on the proxy server.

C. Configure Network ACLs on Server X to deny access to S3 endpoints.

D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.

E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

ANSWER: A B

QUESTION NO: 9

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:

• Data must be encrypted in transit.

• Data must be encrypted at rest.

• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.

Which combination of steps would meet the requirements? (Choose two.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.

B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.

C. Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.

D. Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.

E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms".

F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

ANSWER: B C

Explanation:

Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the KMS key would need to have privileges granted to it for users outside of AWS.

QUESTION NO: 10

An application uses Amazon Cognito to manage end users' permissions when directly accessing IAM resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues.

Which approach will meet these requirements and priorities?

A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.

B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.

C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.

D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

ANSWER: D

Explanation:

https://IAM.amazon.com/blogs/IAM/new-amazon-cognito-groups-and-fine-grained-role-based-access-control-2/

QUESTION NO: 11

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and IAM STS in specific accounts.

What is a scalable and efficient approach to meet this requirement?

A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```

B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
{
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Deny ",
               "Resource": "*"
          }
     ]
}
```

C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```

D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
{
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Deny ",
               "Resource": "*"
          }
     ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: A

Explanation:

It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

QUESTION NO: 12

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?

Please select:

A. Trigger an IAM Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.

B. Query the Trusted Advisor API for all best practice security checks and check for "action recommened" status.

C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.

D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

ANSWER: D

Explanation:

Option B is incorrect because querying Trusted Advisor API's are not possible

Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.

Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

Insecure Server Protocols

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

For more information, please refer to below URL:
https://docs.IAM.amazon.eom/mspector/latest/userguide/inspector_runtime-behavior-analysis.html#insecure-protocols

(

The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Submit your Feedback/Queries to our Experts

QUESTION NO: 13

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the Internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Choose three.)

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured.

B. The internet gateway of the VPC has been misconfigured.

C. The security group denies outbound traffic on ephemeral ports.

D. The route table is missing a route to the internet gateway.

E. The NACL denies outbound traffic on ephemeral ports.

F. The host-based firewall is denying SSH traffic.

ANSWER: B D F

Explanation:

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html

QUESTION NO: 14

There is a requirement for a company to transfer large amounts of data between IAM and an on-premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

Please select:

A. Provision a Direct Connect connection to an IAM region using a Direct Connect partner.

B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.

C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.

D. Create a VPC peering connection between IAM and the Customer gateway.

ANSWER: A

Explanation:

IAM Direct Connect makes it easy to establish a dedicated network connection from your premises to IAM. Using IAM Direct Connect you can establish private connectivity between IAM and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

Options B and C are invalid because these options will not reduce network latency

Options D is invalid because this is only used to connect 2 VPC's

For more information on IAM direct connect, just browse to the below URL:

https://IAM.amazon.com/directconnect

The correct answer is: Provision a Direct Connect connection to an IAM region using a Direct Connect partner. omit your Feedback/Queries to our Experts

QUESTION NO: 15

A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The IAM account number is 111122223333, and the bucket name Is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be Implemented

Which statement should the security specialist include in the policy?

A.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-server-side-encryption": "AES256"
        }
    }
}
```

B.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

C.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    }
}
```

D.

```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringNotLikeIfExists": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
        }
    }
}
```

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

QUESTION NO: 16

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an IAM Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

Please select:

A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.

B. Give root access to your Apache servers to the developers.

C. Give read-only access to your developers to the Apache servers.

D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

ANSWER: D

Explanation:

One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.

The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.

Options A,B and C are all invalid because you should not give access to the developers on the Apache se

For more information on S3, please refer to the below link

https://IAM.amazon.com/documentation/s3j

The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Submit vour Feedback/Queries to our Experts

QUESTION NO: 17

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flIAM. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

Please select:

A. Use IAM Config to ensure that the servers have no critical flIAM.

B. Use IAM inspector to ensure that the servers have no critical flIAM.

C. Use IAM inspector to patch the servers

D. Use IAM SSM to patch the servers

ANSWER: B D

Explanation:

The IAM Documentation mentions the following on IAM Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on IAM. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the IAM Config service is not used to check the vulnerabilities on servers

Option C is invalid because the IAM Inspector service is not used to patch servers

For more information on IAM Inspector, please visit the following URL:

https://IAM.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL:

https://docs.IAM.amazon.com/systems-manager/latest/APIReference/Welcome.html

The correct answers are: Use IAM Inspector to ensure that the servers have no critical flIAM.. Use IAM SSM to patch the servers

(

QUESTION NO: 18

A company's application team needs to host a MySQL database on IAM. According to the company's security policy, all data that is stored on IAM must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.

The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.

Which solution will meet these requirements?

A. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM Key Management Service (IAM KMS) custom key store that is backed by IAM CloudHSM for key management.

B. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM managed CMK in IAM Key Management Service (IAM KMS) for key management.

C. Host the database on an Amazon EC2 instance. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use a customer managed CMK in IAM Key Management Service (IAM KMS) for key management.

D. Host the database on an Amazon EC2 instance. Use Transparent Data Encryption (TDE) for encryption and key management.

ANSWER: B

QUESTION NO: 19

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is

triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table?

Please select:

A. Create a VPC endpoint for DynamoDB within a VPC. Configure the Lambda function to access resources in the VPC.

B. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the poll to the DynamoDB table.

C. Create an IAM user with permissions to write to the DynamoDB table. Store an access key for that user in the Lambda environment variables.

D. Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

ANSWER: D

Explanation:

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The IAM Documentation additionally mentions the following

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 IAM 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 IAM 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), IAM Lambda polls these streams on your behalf. IAM 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.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resources policies are present for resources such as S3 and KMS, but not IAM Lambda

Option C is invalid because IAM Roles should be used and not IAM Users

For more information on the Lambda permission model, please visit the below URL:

https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

QUESTION NO: 20

A company is running third-party WAF software on AWS. The company's security team discovers that the third-party WAF software has vulnerabilities that can lead to server-side request forgery (SSRF) attacks. Because of this discovery, the security team mandates that the entire AWS infrastructure must use version 2 of the instance metadata service (IMDSv2).

At the planned completion of the implementation of IMDSv2, the security team uses the Amazon CloudWatch metric Amazon EC2:MetadataNoToken and determines that hundreds of old IMDSv1 requests still are occurring each day. The security team is willing to risk the availability of the company's application to finish this implementation.

Which combination of steps should the security team take to complete the migration to IMDSv2 in the AWS environment? (Choose two.)

A. Write and enforce an IAM policy that denies the ec2:runinstances action when the ec2:MetadataHttpTokens condition key is not set to required.

B. Use the ec2 modify-instance-metadata-options command from the AWS CLI with the http-put-response-hop-limit 0 option.

C. Use the ec2 modify-instance-metadata-options command from the AWS CLI with the --http-tokens required option.

D. Modify instance security groups to deny all outbound HTTP traffic to 169.254.169.254.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` curl
http://169.254.169.254/latest/meta-data/profile -H "X-aws-ec2-metadata-token: $TOKEN"
```

ANSWER: C E

Explanation:

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html