Free Questions for SCS-C01 by certscare

Shared by Leonard on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company's application team wants to replace an internal application with a new IAM architecture that consists of Amazon EC2 instances, an IAM Lambda function, and an Amazon S3 bucket in a single IAM Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company's organization in IAM Organizations to restrict the creation of internet gateways. NAT gateways, and egress-only gateways.

Which combination of steps should the application team take to meet these requirements? (Select THREE.)

Options:

A- Create an S3 endpoint that has a full-access policy for the application's VPC.

B- Create an S3 access point for the S3 bucket. Include a policy that restricts the network origin to VPCs.

C- Launch the Lambda function. Enable the block public access configuration.

D- Create a security group that has an outbound rule over port 443 with a destination of the S3 endpomt. Associate the security group with the EC2 instances.

E- Create a security group that has an outbound rule over port 443 with a destination of the S3 access point. Associate the security group with the EC2 instances.

F- Launch the Lambda function in a VPC.

Answer:

A, D, F

Question 2

Question Type: MultipleChoice

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.

How can a security engineer meet this requirement?

Options:

A- Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).

B- Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect toward secrecy (PFS).

C- Create an HTTPS listener that uses the Server Order Preference security feature.

D- Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Answer:

A

Question 3

Question Type: MultipleChoice

A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.

Which solution meets these requirements?

Options:

A- Use IAM Systems Manager Parameter Store to store the database credentiais. Configure automatic rotation of the credentials.

B- Use IAM Secrets Manager to store the database credentials. Configure automat* rotation of the credentials

C- Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.

D- Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the

credentials on a scheduled basts

Answer:

A

Question 4

Question Type: MultipleChoice

A company deploys a set of standard IAM roles in IAM accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented IAM Organizations SCPs to restrict access to critical security services in all company accounts.

All of the company's accounts and OUs within IAM Organizations have a default FullIAMAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and IAM Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":"*",
            "Action":"s3:*",
            "Resource":"arn:aws:s3:::examplebucket/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "10.10.10.0/24"
                    ]
                }
            }
        }
    ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

A)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

B)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

C)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Options:

A- Option

B- Option

C- Option

Answer:

C

Question 5

Question Type: MultipleChoice

A company hosts an application on Amazon EC2 that is subject to specific rules for regulatory compliance. One rule states that traffic to and from the workload must be inspected for network-level attacks. This involves inspecting the whole packet.

To comply with this regulatory rule, a security engineer must install intrusion detection software on a c5n.4xlarge EC2 instance. The engineer must then configure the software to monitor traffic to and from the application instances.

What should the security engineer do next?

Options:

A- Place the network interface in promiscuous mode to capture the traffic.

B- Configure VPC Flow Logs to send traffic to the monitoring EC2 instance using a Network Load Balancer.

C- Configure VPC traffic mirroring to send traffic to the monitoring EC2 instance using a Network Load Balancer.

D- Use Amazon Inspector to detect network-level attacks and trigger an IAM Lambda function to send the suspicious packets to the EC2 instance.

Answer:

D

Question 6

Question Type: MultipleChoice

A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off.

What is the MOST efficient way to implement this solution?

Options:

A- Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.

B- Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonIAM.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.

C- Create an Amazon CloudWatch alarm with a cloudtrail.amazonIAM.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.

D- Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.

Answer:

B

Question 7

Question Type: MultipleChoice

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

Options:

A- Amazon Route 53

B- IAM Certificate Manager (ACM)

C- Amazon S3

D- IAM Shield

E- Elastic Load Balancer

F- Amazon GuardDuty

Answer:

D, E, F

Question 8

Question Type: MultipleChoice

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

A. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

B. Include the following SCP on the development account:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

C. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

D. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

A

Question 9

Question Type: **MultipleChoice**

A security engineer is defining the controls required to protect the IAM account root user credentials in an IAM Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised.

Which combination of controls should the security engineer propose? (Select THREE.)

A)

Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

B)

Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Principal" : "arn:aws:iam::*:root"
            "Action": "*",
            "Resource": [
                "*"
            ]
        }
    ]
}
```

C) Enable multi-factor authentication (MFA) for the root user.

D) Set a strong randomized password and store it in a secure location.

E) Create an access key ID and secret access key, and store them in a secure location.

F) Apply the following permissions boundary to the toot user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

E- Option E

F- Option F

Answer:

A, C, E