SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive data-base credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same pri-vate subnet. The VPC has a Secrets Manager VPC endpoint. A security engineer discovers that the secret cannot rotate. The security engi-neer determines that the VPC endpoint is working as intended. The Amazon Cloud-Watch logs contain the following error:

"setSecret: Unable to log into database".

Which solution will resolve this error?

A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the struc-ture that the database requires.

B. Ensure that the security group that is attached to the Lambda function al-lows outbound connections to the EC2 instance. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.

C. Use the Secrets Manager list-secrets command in the AWS CLI to list the secret. Identify the database credentials. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the se-cret.

D. Add an internet gateway to the VPC. Create a NAT gateway in a public sub-net. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

Correct Answer: B

This answer is correct because ensuring that the security groups allow bidirectional communication between the Lambda function and the EC2 instance will resolve the error. The error indicates that the Lambda function cannot connect to the database, which might be due to firewall rules blocking the traffic. By allowing outbound connections from the Lambda function and inbound connections to the EC2 instance, the security engineer can enable the rotation function to access and update the database credentials.

QUESTION 2

A developer signed in to a new account within an IAM Organization organizational unit (OU) containing multiple accounts. Access to the Amazon $3 service is restricted with the following SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

How can the security engineer provide the developer with Amazon $3 access without affecting other account?

A. Move the SCP to the root OU of organization to remove the restriction to access Amazon $3.

B. Add an IAM policy for the developer, which grants $3 access.

C. Create a new OU without applying the SCP restricting $3 access. Move the developer account to this new OU.

D. Add an allow list for the developer account for the $3 service.

Correct Answer: C

QUESTION 3

Amazon GuardDuty has detected communications to a known command and control endpoint from a company\\'s Amazon EC2 instance. The instance was found to be running a vulnerable version of a common web framework. The company\\'s security operations team wants to quickly identity other compute resources with the specific version of that framework installed.

Which approach should the team take to accomplish this task?

A. Scan all the EC2 instances for noncompliance with IAM Config. Use Amazon Athena to query IAM CloudTrail logs for the framework installation

B. Scan all the EC2 instances with the Amazon Inspector Network Reachability rules package to identity instances running a web server with RecognizedPortWithListener findings

C. Scan all the EC2 instances with IAM Systems Manager to identify the vulnerable version of the web framework

D. Scan an the EC2 instances with IAM Resource Access Manager to identify the vulnerable version of the web framework

Correct Answer: C

To quickly identify other compute resources with the specific version of the web framework installed, the team should do the following:

Scan all the EC2 instances with AWS Systems Manager to identify the vulnerable version of the web framework. This allows the team to use AWS Systems Manager Inventory to collect and query information about the software installed on

their EC2 instances, and to filter the results by software name and version.

QUESTION 4

A security engineer recently rotated the host keys for an Amazon EC2 instance. The security engineer is trying to access the EC2 instance by using the EC2 Instance. Connect feature. However, the security engineer receives an error (or failed host key validation. Before the rotation of the host keys EC2 Instance Connect worked correctly with this EC2 instance.

What should the security engineer do to resolve this error?

A. Import the key material into AWS Key Management Service (AWS KMS).

B. Manually upload the new host key to the AWS trusted host keys database.

C. Ensure that the AmazonSSMManagedInstanceCore policy is attached to the EC2 instance profile.

D. Create a new SSH key pair for the EC2 instance.

Correct Answer: B

To set up a CloudFront distribution for an S3 bucket that hosts a static website, and to allow only specified IP addresses to access the website, the following steps are required: Create a CloudFront origin access identity (OAI), which is a special CloudFront user that you can associate with your distribution. An OAI allows you to restrict access to your S3 content by using signed URLs or signed cookies. For more information, see Using an origin access identity to restrict access to your Amazon S3 content. Create the S3 bucket policy so that only the OAI has access. This will prevent users from accessing the website directly by using S3 URLs, as they will receive an Access Denied error. To do this, use the AWS Policy Generator to create a bucket policy that grants s3:GetObject permission to the OAI, and attach it to the S3 bucket. For more information, see Restricting access to Amazon S3 content by using an origin access identity. Create an AWS WAF web ACL and add an IP set rule. AWS WAF is a web application firewall service that lets you control access to your web applications. An IP set is a condition that specifies a list of IP addresses or IP address ranges that requests originate from. You can use an IP set rule to allow or block requests based on the IP addresses of the requesters. For more information, see Working with IP match conditions. Associate the web ACL with the CloudFront distribution. This will ensure that the web ACL filters all requests for your website before they reach your origin. You can do this by using the AWS WAF console, API, or CLI. For more information, see Associating or disassociating a web ACL with a CloudFront distribution. This solution will meet the requirements of allowing only specified IP addresses to access the website and preventing direct access by using S3 URLs. The other options are incorrect because they either do not create a CloudFront distribution for the S3 bucket (A), do not use an OAI to restrict access to the S3 bucket ? or do not use AWS WAF to block traffic from outside the specified IP addresses (D).

Verified References: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-ip-conditions.html

---

QUESTION 5

A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.

The company issues a new security policy that contains the following requirements:

1.

No AWS account should use a VPC within the AWS account for workloads.

2.

The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.

3.

No AWS account should be able to modify another AWS account\\'s application resources within the centrally managed VPC.

4.

The centrally managed VPC should reside in an existing AWS account that is named Account-A within an organization.

The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.

Which solution will complete the security setup to meet these requirements?

A. Use a CloudFormation template in the member accounts to launch workloads. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.

B. Use a transit gateway in the VPC within Account-A. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.

C. Use AWS Resource Access Manager (AWS RAM) to share Account-A\\'s VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.

D. Create a peering connection between Account-A and the remaining member accounts. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Correct Answer: C

Use AWS Resource Access Manager (AWS RAM) to share Account-A\\'s VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.

This answer is correct because AWS RAM is a service that helps you securely share your AWS resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types. One of the supported resource types is VPC subnets, which means you can share the subnets in Account-A\\'s VPC with the other member accounts using AWS RAM. This way, you can meet the requirements of using a centrally managed VPC, avoiding duplicate VPCs in each account, and launching workloads in shared subnets. You can also control the access to the shared subnets by using IAM policies and resource-based policies3, which can prevent one account from modifying another account\\'s resources. The other options are incorrect because:

A. Using a CloudFormation template in the member accounts to launch workloads and using the Fn::ImportValue function to obtain the subnet ID values is not a solution, because Fn::ImportValue can only import values that have been exported by another stack within the same region. This means that you cannot use Fn::ImportValue to reference the subnet IDs that are exported by Account-A\\'s CloudFormation template, unless all the member accounts are in the same region as Account-A. This option also does not avoid creating duplicate VPCs in each account, which is one of the requirements.

B. Using a transit gateway in the VPC within Account-A and configuring the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads is not a solution, because a transit gateway does not allow you to launch workloads in another account\\'s subnets. A transit gateway is a network transit hub that enables you to route traffic between your VPCs and on-premises networks, but it does not enable you to share subnets across accounts. D. Creating a peering connection between Account-A and the remaining member accounts and configuring the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads is not a solution, because a VPC peering connection does not allow you to launch workloads in another account\\'s subnets. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately, but it does not enable you to share subnets across accounts.

References:

1: What is AWS Resource Access Manager?

2: Shareable AWS resources

3: Managing permissions for shared resources

4: Fn::ImportValue

5: What is a transit gateway?

6: What is VPC peering?