SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

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

https://www.leads4pass.com/aws-certified-security-specialty.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

An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key. How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

A. Analyze AWS CloudTrail for activity.

B. Analyze Amazon CloudWatch Logs for activity.

C. Download and analyze the IAM Use report from AWS Trusted Advisor.

D. Analyze the resource inventory in AWS Config for IAM user activity.

E. Download and analyze a credential report from IAM.

Correct Answer: AE

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

QUESTION 2

A company is developing a mobile shopping web app. The company needs an environment that is configured to encrypt all resources in transit and at rest.

A security engineer must develop a solution that will encrypt traffic in transit to the company\\'s Application Load Balancer and Amazon API Gateway resources. The solution also must encrypt traffic at rest for Amazon S3 storage.

What should the security engineer do to meet these requirements?

A. Use AWS Certificate Manager (ACM) for encryption in transit. Use AWS Key Management Service for encryption at rest.

B. Use AWS Certificate Manager (ACM) for encryption in transit and encryption at rest.

C. Use AWS Key Management Service for encryption in transit. Use AWS Certificate Manager (ACM) for encryption at rest.

D. Use AWS Key Management Service for encryption in transit and encryption at rest.

Correct Answer: A

QUESTION 3

You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?

Please select:

A. Save the API credentials to your PHP files.

B. Don\\'t save your API credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.

C. Save your API credentials in a public Github repository.

D. Pass API credentials to the instance using instance userdata.

Correct Answer: B

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it\\'s challenging to securely distribute credentials to each instance. especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials. IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you manage the security credentials that the applications use. Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access For more information on IAM Roles, please visit the below URL:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

The correct answer is: Don\\'t save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it

---

QUESTION 4

A company plans to move most of its IT infrastructure to AWS. The company wants to leverage its existing on-premises Active Directory as an identity provider for AWS. Which steps should be taken to authenticate to AWS services using the company\\'s on- premises Active Directory? (Choose three).

A. Create IAM roles with permissions corresponding to each Active Directory group.

B. Create IAM groups with permissions corresponding to each Active Directory group.

C. Create a SAML provider with IAM.

D. Create a SAML provider with Amazon Cloud Directory.

E. Configure AWS as a trusted relying party for the Active Directory

F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

Correct Answer: ACE

https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/

QUESTION 5

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

A. Use the AWS Trusted Advisor to see what can be done.

B. Use VPC Flow logs to diagnose the traffic

C. Use AWS WAF to analyze the traffic

D. Use AWS Guard Duty to analyze the traffic

Correct Answer: B

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application The AWS Documentation mentions the following VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors. For more information on AWS Security, please visit the following URL: https://aws.amazon.com/answers/networking/vpc-security-capabilities> The correct answer is: Use VPC Flow logs to diagnose the traffic