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.pass4itsure.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

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?

Please select:

A. Use the AWS Systems Manager Parameter Store

B. Use the AWS Systems Manager Run Command

C. Use the AWS Inspector

D. Use AWS Config

Correct Answer: B

The AWS Documentation mentions the following AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost. Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance. Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/executeremote-commands.htmll The correct answer is: Use the AWS Systems Manager Run Command

QUESTION 2

Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

Please select:

A. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.

B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.

C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.

D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.

Correct Answer: B

On the AWS Blog site the following information is present to help on this context

The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can

access AWS by using their existing credentials. This means that your users don\\'t need to maintain yet another user name and password just to access AWS resources. Option A.C and D are all invalid because in this sort of

configuration, you

have to use SAML to enable single sign on.

For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:

https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldap-and-shibboleth/

The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.

QUESTION 3

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.

Which solution will meet these requirements?

A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

B. Create an origin access identity (OAI). Associate the OAI with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.

C. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.

D. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Correct Answer: C

QUESTION 4

A company\\'s policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company\\'s security team However, an audit revealed that an API key is steed with the source code of an AWS Lambda function m an AWS CodeCommit repository in the DevOps account

How should the security learn securely store the API key?

A. Create a CodeCommit repository in the security account using AWS Key Management Service (AWS KMS) for encryption. Require the development team to migrate the Lambda source code to this repository.

B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key. Create a presigned URL for the S3 key, and specify the URL in a Lambda environmental variable in the AWS CloudFormation template. Update the Lambda function code to retrieve the key using the URL and call the API.

C. Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management

Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API.

D. Create an encrypted environment variable for the Lambda function to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime.

Correct Answer: C

QUESTION 5

After multiple compromises of its Amazon EC2 instances, a company\\'s Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.

B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.

C. Download and run the EC2Rescue for Windows Server utility from AWS.

D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Correct Answer: B

Reference: https://www.giac.org/paper/gcfa/13310/digital-forensic-analysis-amazon-linux-ec2-instances/123500