



Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

AWS Config cannot deliver configuration snapshots to Amazon S3. Which TWO actions will remediate this issue?

- A. Verify the S3 bucket policy allows config.amazonaws.com.
- B. Verify the IAM role has s3:GetBucketAcl and s3:PutObject permissions.
- C. Verify the S3 bucket can assume the IAM role.
- D. Verify IAM policy allows AWS Config to write logs.
- E. Modify AWS Config API permissions.

Answer: AB

NEW QUESTION 2

A company uses AWS Organizations to manage an organization that consists of three workload OUs: Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.

The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails.

The error message reports insufficient IAM permissions.

What is the FIRST step that a security engineer should take to troubleshoot this issue?

- A. Review the AWS CloudTrail logs in the account in the Production O
- B. Search for any failed API calls from CloudFormation during the deployment attempt.
- C. Remove all the SCPs that are attached to the Production O
- D. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
- E. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
- F. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

Answer: A

NEW QUESTION 3

A security team manages a company's AWS Key Management Service (AWS KMS) customer managed keys. Only members of the security team can administer the KMS keys. The company's application team has a software process that needs temporary access to the keys occasionally. The security team needs to provide the application team's software process with access to the keys.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Export the KMS key material to an on-premises hardware security module (HSM). Give the application team access to the key material.
- B. Edit the key policy that grants the security team access to the KMS keys by adding the application team as principal
- C. Revert this change when the application team no longer needs access.
- D. Create a key grant to allow the application team to use the KMS key
- E. Revoke the grant when the application team no longer needs access.
- F. Create a new KMS key by generating key material on premise
- G. Import the key material to AWS KMS whenever the application team needs access
- H. Grant the application team permissions to use the key.

Answer: C

NEW QUESTION 4

A company's security engineer receives an abuse notification from AWS indicating that malware is being hosted from the company's AWS account. The security engineer discovers that an IAM user created a new Amazon S3 bucket without authorization.

Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Select THREE.)

- A. Encrypt all AWS CloudTrail logs.
- B. Turn on Amazon GuardDuty.
- C. Change the password for all IAM users.
- D. Rotate or delete all AWS access keys.
- E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
- F. Delete any resources that are unrecognized or unauthorized.

Answer: BDF

NEW QUESTION 5

A company needs to identify the root cause of security findings and investigate IAM roles involved in those findings. The company has enabled VPC Flow Logs, Amazon GuardDuty, and AWS CloudTrail.

Which solution will meet these requirements?

- A. Use Amazon Detective to investigate IAM roles and visualize findings.
- B. Use Amazon Inspector and CloudWatch dashboards.
- C. Export GuardDuty findings to S3 and analyze with Athena.
- D. Use Security Hub custom actions to investigate IAM roles.

Answer: A

NEW QUESTION 6

A company has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs

manually.

The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically scaling architecture to result in the loss of any log files when instances are scaled in.

Which combination of steps should a security engineer take to meet these requirements MOST cost-effectively? (Select TWO.)

- A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.
- B. Configure AWS Glue and Amazon Athena to query the log files.
- C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
- D. Configure Amazon CloudWatch Logs Insights to query the log files.
- E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Answer: CD

NEW QUESTION 7

A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to access the company's AWS resources.

Which additional step will meet these requirements?

- A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
- B. Add a StringEquals condition to the IAM role policy for the EC2 instance profil
- C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoic
- D. Tag each generated invoice with the ID of its corresponding client.
- E. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permission
- F. Use the credentials to generate the pre-signed URLs.
- G. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucke
- H. Embed the keys into the scrip
- I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 8

A company needs to deploy AWS CloudFormation templates that configure sensitive database credentials. The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.

Which solution will meet the requirements?

- A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.
- B. Use encrypted parameters in the CloudFormation template.
- C. Use SecureString parameters to reference Secrets Manager.
- D. Use SecureString parameters encrypted by AWS KMS.

Answer: A

NEW QUESTION 9

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket. A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

- A. Download the data from the existing S3 bucket to a new EC2 instanc
- B. Then delete the data from the S3 bucke
- C. Re-encrypt the data with a client-based ke
- D. Upload the data to a new S3 bucket.
- E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewal
- F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
- G. Revoke the IAM role??s active session permission
- H. Update the S3 bucket policy to deny access to the IAM rol
- I. Remove the IAM role from the EC2 instance profile.
- J. Disable the current ke
- K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new ke
- L. Schedule the compromised key for deletion.

Answer: C

NEW QUESTION 10

A company experienced a security incident caused by a vulnerable container image that was pushed from an external CI/CD pipeline into Amazon ECR.

Which solution will prevent vulnerable images from being pushed?

- A. Enable ECR enhanced scanning with Lambda blocking.
- B. Use Amazon Inspector with EventBridge and Lambda.
- C. Integrate Amazon Inspector into the CI/CD pipeline using SBOM generation and fail the pipeline on critical findings.
- D. Enable basic continuous ECR scanning.

Answer: C

NEW QUESTION 10

A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet. The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC. Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

- A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
- B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
- C. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
- D. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.
- E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.

Answer: AD

NEW QUESTION 15

An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs. Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was invoked was not current.

Answer: A

NEW QUESTION 19

A company uses AWS IAM Identity Center to manage access to its AWS accounts. The accounts are in an organization in AWS Organizations. A security engineer needs to set up delegated administration of IAM Identity Center in the organization's management account.

Which combination of steps should the security engineer perform in IAM Identity Center before configuring delegated administration? (Select THREE.)

- A. Grant least privilege access to the organization's management account.
- B. Create a new IAM Identity Center directory in the organization's management account.
- C. Set up a second AWS Region in the organization's management account.
- D. Create permission sets for use only in the organization's management account.
- E. Create IAM users for use only in the organization's management account.
- F. Create user assignments only in the organization's management account.

Answer: BDF

NEW QUESTION 23

A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key. Which solution will meet these requirements?

- A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
- B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
- C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
- D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 28

A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region that uses an AWS KMS customer managed key. The company must copy a DB snapshot to the us-west-1 Region but cannot access the encryption key across Regions.

What should the company do to properly encrypt the snapshot in us-west-1?

- A. Store the customer managed key in AWS Secrets Manager in us-west-1.
- B. Create a new customer managed key in us-west-1 and use it to encrypt the snapshot.
- C. Create an IAM policy to allow access to the key in us-east-1 from us-west-1.
- D. Create an IAM policy that allows RDS in us-west-1 to access the key in us-east-1.

Answer: B

NEW QUESTION 29

A security engineer needs to prepare Amazon EC2 instances for quarantine during a security incident. AWS Systems Manager Agent (SSM Agent) is installed, and a script exists to install and update forensic tools.

Which solution will quarantine EC2 instances during a security incident?

- A. Track SSM Agent versions with AWS Config.
- B. Configure Session Manager to deny external connections.
- C. Store the script in Amazon S3 and grant read access.
- D. Configure IAM permissions for the SSM Agent to run the script as a Systems Manager Run Command document.

Answer: D

NEW QUESTION 30

A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets. Which solution will meet these requirements?

- A. Enable AWS Confi
- B. Create a proactive AWS Config Custom Policy rul
- C. Create aGuard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition ke
- D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
- E. Enable AWS Confi
- F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybri
- G. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- H. Configure automatic remediatio
- I. Set the runbook as the target of the rule.
- J. Enable Amazon Inspecto
- K. Create a custom AWS Lambda rul
- L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- M. Set the Lambda function as the target of the rule.
- N. Create an AWS CloudTrail trai
- O. Enable S3 data events on the trai
- P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 32

A security engineer discovers that a company's user passwords have no required minimum length. The company uses the following identity providers (IdPs):

- AWS Identity and Access Management (IAM) federated with on-premises Active Directory
- Amazon Cognito user pools that contain the user database for an AWS Cloud application Which combination of actions should the security engineer take to implement a required minimum password length? (Select TWO.)

- A. Update the password length policy in the IAM configuration.
- B. Update the password length policy in the Amazon Cognito configuration.
- C. Update the password length policy in the on-premises Active Directory configuration.
- D. Create an SCP in AWS Organizations to enforce minimum password length.
- E. Create an IAM policy with a minimum password length condition.

Answer: BC

NEW QUESTION 36

A consultant agency needs to perform a security audit for a company's production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account. The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.

Which solution will provide the consultant agency with access that meets these requirements?

- A. Create an IAM grou
- B. Create an IAM user for each consultan
- C. Add each user to the grou
- D. Turn on MFA for each consultant.
- E. Configure Amazon Cognito on the company's production account to authenticate against the consultant agency's identity provider (IdP). Add MFA to a Cognito user pool.
- F. Create an IAM role in the consultant agency's AWS accoun
- G. Define a trust policy that requires MF
- H. In the trust policy, specify the company's production account as the principa
- I. Attach the trust policy to the role.
- J. Create an IAM role in the company's production accoun
- K. Define a trust policy that requires MF
- L. In the trust policy, specify the consultant agency's AWS account as the principa
- M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 40

A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.

Which solution will meet these requirements MOST quickly?

- A. Log in to the AWS account by using read-only credential
- B. Review the GuardDuty finding for details about the IAM credentials that were use
- C. Use the IAM console to add a DenyAll policy to the IAM principal.
- D. Log in to the AWS account by using read-only credential
- E. Review the GuardDuty finding to determine which API calls initiated the findin
- F. Use Amazon Detective to review the API calls in context.
- G. Log in to the AWS account by using administrator credential
- H. Review the GuardDuty finding for details about the IAM credentials that were use
- I. Use the IAM console to add a DenyAll policy to the IAM principal.
- J. Log in to the AWS account by using read-only credential
- K. Review the GuardDuty finding to determine which API calls initiated the findin
- L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Answer: B

NEW QUESTION 43

A company stores infrastructure and application code in web-based, third-party, Git- compatible code repositories outside of AWS. The company wants to give the code repositories the ability to securely authenticate and assume an existing IAM role within the company's AWS account by using OpenID Connect (OIDC). Which solution will meet these requirements?

- A. Create an OIDC identity provider (IdP) by using AWS Identity and Access Management (IAM) federatio
- B. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- C. Use AWS Identity and Access Management (IAM) Roles Anywhere to create a trust anchor that uses OID
- D. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- E. Set up an account instance of AWS IAM Identity Cente
- F. Configure access to the code repositories as a customer managed OIDC applicatio
- G. Grant the application access to the IAM role.
- H. Use AWS Resource Access Manager (AWS RAM) to create a new resource share that uses OID
- I. Limit the resource share to the specified code repositorie
- J. Grant the IAM role access to the resource share.

Answer: A

NEW QUESTION 46

A company detects bot activity targeting Amazon Cognito user pool endpoints. The solution must block malicious requests while maintaining access for legitimate users. Which solution meets these requirements?

- A. Enable Amazon Cognito threat protection.
- B. Restrict access to authenticated users only.
- C. Associate AWS WAF with the Cognito user pool.
- D. Monitor requests with CloudWatch.

Answer: A

NEW QUESTION 49

A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster. Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Config managed rule to detect unencrypted RDS storag
- B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- C. Configure the Lambda function to delete the unencrypted resource.
- D. Create an AWS Config managed rule to detect unencrypted RDS storag
- E. Configure a manual remediation action to invoke an AWS Lambda functio
- F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
- H. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- I. Configure the Lambda function to delete the unencrypted resource.
- J. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
- K. Configure the rule to invoke an AWS Lambda functio
- L. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: A

NEW QUESTION 51

A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days. Which solution will meet these requirements?

- A. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
- B. Remove IAM policies and query logs in Security Hub.
- C. Remove permission sets and query logs using CloudWatch Logs Insights.
- D. Disable the user in IAM Identity Center and query the organizational event data store.

Answer: D

NEW QUESTION 53

A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic. Which solution will meet these requirements with the LEAST implementation effort?

- A. Enable AWS Confi
- B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
- C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a patter
- D. Program the Lambda function to send notifications to the SNS topic.
- E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive dat
- F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- G. Enable Amazon GuardDut

- H. Configure AWS CloudTrail S3 data event
- I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Answer: C

NEW QUESTION 56

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The solution must involve the least amount of effort and maintain normal operations during implementation. What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group
- B. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the ALB
- C. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB
- D. Update security groups on the EC2 instances to prevent direct access from the internet.
- E. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin
- F. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution
- G. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- H. Obtain the latest source code for the platform and make the necessary update
- I. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
- J. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL databases
- K. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances.

Answer: A

NEW QUESTION 60

A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

- A. Delegate Amazon Macie and Security Hub administration.
- B. Use Amazon Inspector with Security Hub.
- C. Use Inspector with Trusted Advisor.
- D. Use Macie with Trusted Advisor.

Answer: A

NEW QUESTION 64

A company runs a public web application on Amazon EKS behind Amazon CloudFront and an Application Load Balancer (ALB). A security engineer must send a notification to an existing Amazon SNS topic when the application receives 10,000 requests from the same end-user IP address within any 5-minute period. Which solution will meet these requirements?

- A. Configure CloudFront standard logging and CloudWatch Logs metric filters.
- B. Configure VPC Flow Logs and CloudWatch Logs metric filters.
- C. Configure an AWS WAF web ACL with an ASN match rule and CloudWatch alarms.
- D. Configure an AWS WAF web ACL with a rate-based rule
- E. Associate it with CloudFront
- F. Create a CloudWatch alarm to notify SNS.

Answer: D

NEW QUESTION 65

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution must also handle volatile traffic patterns. Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
- D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Answer: C

NEW QUESTION 70

A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM. Which solution will meet this requirement?

- A. Identify the Regional cluster ARN for the database
- B. Use the ARN to restore the Regional cluster by using the restore to point in time feature
- C. Set a target time 5 days ago at 3:14 PM.
- D. Identify the Regional cluster ARN for the database
- E. List snapshots that have been taken of the cluster
- F. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
- G. List all snapshots that have been taken of all the company's RDS database
- H. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- I. Identify the Regional cluster ARN for the database
- J. Use the ARN to restore the Regional cluster by using the restore to point in time feature

K. Set a target time 14 days ago.

Answer: A

NEW QUESTION 72

A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to authenticate all S3 API calls with AWS credentials. Which solution will provide the application with AWS credentials?

- A. Use Amazon Cognito identity pools and the GetId API.
- B. Use Amazon Cognito identity pools and AssumeRoleWithWebIdentity.
- C. Use Amazon Cognito user pools with ID tokens.
- D. Use Amazon Cognito user pools with access tokens.

Answer: B

NEW QUESTION 74

A company uses AWS Organizations and has an SCP at the root that prevents sharing resources with external accounts. The company now needs to allow only the marketing account to share resources externally while preventing all other accounts from doing so. All accounts are in the same OU. Which solution will meet these requirements?

- A. Create a new SCP in the marketing account to explicitly allow sharing.
- B. Edit the existing SCP to add a condition that excludes the marketing account.
- C. Edit the SCP to include an Allow statement for the marketing account.
- D. Use a permissions boundary in the marketing account.

Answer: B

NEW QUESTION 78

.....

Relate Links

100% Pass Your SCS-C03 Exam with Exam Bible Prep Materials

<https://www.exambible.com/SCS-C03-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>