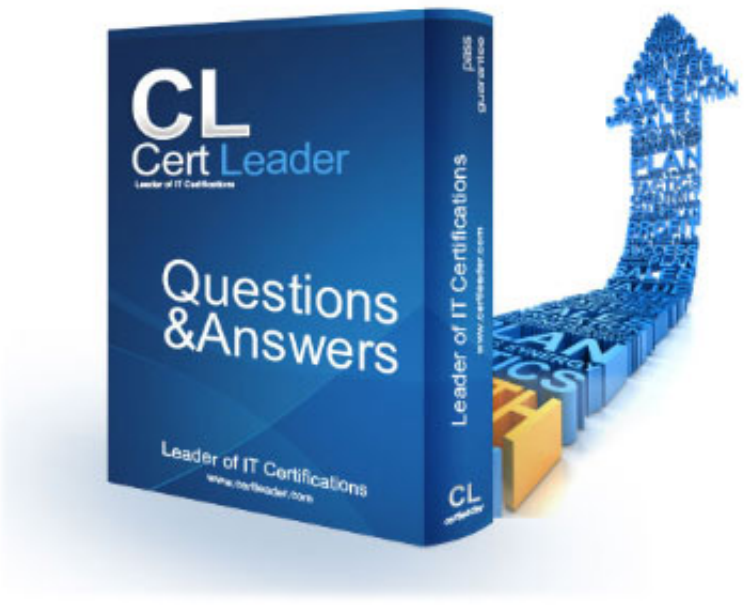
SOA-C02 Dumps

AWS Certified SysOps Administrator - Associate (SOA-C02)

https://www.certleader.com/SOA-C02-dumps.html



NEW QUESTION 1
A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created. Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company's security team needs the ability to trace the integrity of each file.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivere
B. Configure the Lambda function to compute an MD5 hash check on the file and store the result in anAmazon DynamoDB tabl
C. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.
D. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucke
E. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon 53 object.The security team can use the information in the tag to verify the integrity of the delivered files.
F. Enable the CloudTrail file integrity feature on an Amazon S3 bucke
G. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
H. Enable the CloudTrail file integrity feature on the trai
I. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

Answer: C

NEW QUESTION 2
A company has an Amazon RDS DB instance. The company wants to implement a caching service while maintaining high availability. Which combination of actions will meet these requirements? (Choose two.)

A. Add Auto Discovery to the data store.
B. Create an Amazon ElastiCache for Memcached data store.
C. Create an Amazon ElastiCache for Redis data store.
D. Enable Multi-AZ for the data store.
E. Enable Multi-threading for the data store.

Answer: AD

NEW QUESTION 3
An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, an Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.
To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

A. EBS General Purpose SSD volumes
B. RDS PostgreSQL database
C. Amazon EFS file systems
D. S3 objects within a bucket

Answer: B

NEW QUESTION 4
A data storage company provides a service that gives users the ability to upload and download files as needed. The files are stored in Amazon S3 Standard and must be immediately retrievable for 1 year. Users access files frequently during the first 30 days after the files are stored. Users rarely access files after 30 days. The company's SysOps administrator must use S3 Lifecycle policies to implement a solution that maintains object availability and minimizes cost. Which solution will meet these requirements?

A. Move objects to S3 Glacier after 30 days.
B. Move objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
C. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
D. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) immediately.

Answer: C

NEW QUESTION 5
A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.
What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.
B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

Answer: B

NEW QUESTION 6
A company wants to be alerted through email when IAM CreateUser API calls are made within its AWS account. Which combination of actions should a SysOps administrator take to meet this requirement? (Choose two.)

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS CloudTrail as the event source and IAM CreateUser as the specific API call for the event pattern.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with Amazon CloudSearch as the event source and IAM CreateUser as the specific API call for the event pattern.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS IAM Access Analyzer as the event source and IAM CreateUser as the specific

API call for the event pattern.
D. Use an Amazon Simple Notification Service (Amazon SNS) topic as an event target with an email subscription.
E. Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

Answer: CD

NEW QUESTION 7
A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.
Which action should a SysOps administrator take to resolve this issue?

A. Configure the CloudFront distribution behavior to forward the User-Agent header.
B. Configure the CloudFront distribution origin setting
C. Add a User-Agent header to the list of origin custom headers.
D. Enable IPv6 on the AL
E. Update the CloudFront distribution origin settings to use the dualstack endpoint.
F. Enable IPv6 on the CloudFront distributio
G. Update the Route 53 record to use the dualstack endpoint.

Answer: C

NEW QUESTION 8
A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP Layer 7 status codes from the web application.
Which log sources contain the status codes? (Choose two.)

A. VPC Flow Logs
B. AWS CloudTrail logs
C. ALB access logs
D. CloudFront access logs
E. RDS logs

Answer: CD

NEW QUESTION 9
A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket.
Which parameters should be specified to accomplish this in the MOST efficient manner?

A. Specify “*” as the principal and PrincipalOrgId as a condition.
B. Specify all account numbers as the principal.
C. Specify PrincipalOrgId as the principal.
D. Specify the organization’s master account as the principal.

Answer: A

NEW QUESTION 10
A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system checks are failing.
What should the administrator do first to resolve this issue?

A. Reboot the EC2 instance so it can be launched on a new host.
B. Stop and then start the EC2 instance so that it can be launched on a new host.
C. Terminate the EC2 instance and relaunch it.
D. View the AWS CloudTrail log to investigate what changed on the EC2 instance.

Answer: B

NEW QUESTION 10
A company hosts a web application on an Amazon EC2 instance in a production VPC. Client connections to the application are failing. A SysOps administrator inspects the VPC flow logs and finds the following entry:
2 111122223333 eni-<###> 192.0.2.15 203.0.113.56 40711 443 6 1 40 1418530010 1418530070 REJECT OK
What is a possible cause of these failed connections?

A. A security group is denying traffic on port 443.
B. The EC2 instance is shut down.
C. The network ACL is blocking HTTPS traffic.
D. The VPC has no internet gateway attached.

Answer: A

NEW QUESTION 11
A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.
What type of record should be set in Route 53 to point the website’s apex domain name (for example, “company.com”) to the Application Load Balancer?

A. CNAME
B. SOA
C. TXT
D. ALIAS

Answer: D

NEW QUESTION 13
A SysOps administrator needs to design a high-traffic static website. The website must be highly available and must provide the lowest possible latency to users across the globe. Which solution will meet these requirements?

A. Create an Amazon S3 bucket, and upload the website content to the S3 bucke
B. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origi
C. Use Amazon Route 53 to create a DNS record thatuses a geolocation routing policy to route traffic to the correct CloudFront distribution based on where the request originates.
D. Create an Amazon S3 bucket, and upload the website content to the S3 bucke
E. Create an Amazon CloudFront distribution, and set the S3 bucket as the origi
F. Use Amazon Route 53 to create an alias record that points to the CloudFrontdistribution.
G. Create an Application Load Balancer (ALB) and a target grou
H. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target grou
I. Store the website content on the EC2 instance
J. Use AmazonRoute 53 to create an alias record that points to the ALB.
K. Create an Application Load Balancer (ALB) and a target group in two Region
L. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target grou
M. Store the website content on the EC2instance
N. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct ALB based on where the request originates.

Answer: A

NEW QUESTION 14
A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer.
What should a SysOps administrator do to collect this information? (Choose two.)

A. Activate the createdBy tag in the account.
B. Analyze the usage with Amazon CloudWatch dashboards.
C. Analyze the usage with Cost Explorer.
D. Configure AWS Trusted Advisor to track resource usage.
E. Create a billing alarm in AWS Budgets.

Answer: AC

NEW QUESTION 17
A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The administrator has been tasked with reconfiguring the infrastructure to support this approach.
How can the administrator accomplish this with the LEAST administrative overhead?

A. Use Amazon CloudFront to log the URL and forward the request.
B. Use Amazon CloudFront to rewrite the header based on the microservice and forward the request.
C. Use an Application Load Balancer (ALB) and do path-based routing.
D. Use a Network Load Balancer (NLB) and do path-based routing.

Answer: C

NEW QUESTION 19
A SysOps Administrator is using AWS KMS with AWS-generated key material to encrypt an Amazon EBS volume in a company's AWS environment. The Administrator wants to rotate the KMS keys using automatic key rotation, and needs to ensure that the EBS volume encrypted with the current key remains readable.
What should be done to accomplish this?

A. Back up the current KMS key and enable automatic key rotation.
B. Create a new key in AWS KMS and assign the key to Amazon EBS.
C. Enable automatic key rotation of the EBS volume key in AWS KMS.
D. Upload ne key material to the EBS volume key in AWS KMS to enable automatic key rotation for the volume.

Answer: C

Explanation:
References:https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

NEW QUESTION 20
A company has just launched a gamification feature on its mobile app that stores the score of the players to a DynamoDB table. You have been tasked to design a solution to trigger a Lambda function whenever the LeaderBoard attribute of the PlayerScore table is updated. The Lambda function would post a congratulatory message on a social media network.
What's the best solution that can be implemented to trigger the Lambda function on specific events?

A. Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function
B. Create a CloudWatch alarm and automatically trigger the Lambda function
C. Use Amazon Simple Notification Service to trigger Lambda function
D. Use AWS Device Farm

Answer: A

Explanation:
Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function is the correct answer.
Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.
If you enable DynamoDB Streams on a table, you can associate the stream Amazon Resource Name (ARN) with an AWS Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records.
Create a CloudWatch alarm and automatically trigger the Lambda function is incorrect. Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.
You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached, but can't monitor changes in DynamoDB table data.
Use Amazon Simple Notification Service to trigger Lambda function is incorrect. Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. Subscribers (that is, web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (that is, Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.
The Amazon SNS answer can be considered as correct but requires more configuration and is not the best solution.
Use AWS Device Farm is incorrect. Device Farm is an app testing service that you can use to test and interact with your Android, iOS, and web apps on real, physical phones and tablets that are hosted by Amazon Web Services (AWS).
There are two main ways to use Device Farm:
* 1. Automated testing of apps using a variety of testing frameworks.
* 2. Remote access of devices onto which you can load, run and interact with apps in real-time.
The Device Farm can't trigger Lambda functions.

NEW QUESTION 21
A company wants to automate the process of patching managed instances and applying patches for operating systems and applications.
Which service should a SysOps administrator use to meet this requirement?

A. AWS Systems Manager Patch Manager
B. AWS Systems Manager Patch Upgrader
C. AWS Systems Manager Patch Processor
D. AWS Systems Manager Patch Automation

Answer: A

Explanation:
AWS Systems Manager Patch Manager is the correct answer. AWS Systems Manager Patch Manager automates the process of patching managed instances with both security-related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. (On Windows Server, application support is limited to updates for Microsoft applications.) You can use Patch Manager to install Service Packs on Windows instances and perform minor version upgrades on Linux instances.
Patch Manager uses patch baselines, which include rules for auto-approving patches within days of their release, as well as a list of approved and rejected patches. You can install patches on a regular basis by scheduling patching to run as a Systems Manager maintenance window task. You can also install patches individually or to large groups of instances by using Amazon EC2 tags.
The rest answers are fictitious AWS services.

NEW QUESTION 24
Which of the following AWS service is a security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization?

A. AWS Shield
B. AWS Secrets Manager
C. AWS WAF
D. AWS Firewall Manager

Answer: D

Explanation:
AWS Firewall Manager is the correct answer. AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization. As new applications are created, Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules. Now you

have a single service to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across your entire infrastructure.
Using AWS Firewall Manager, you can easily roll out AWS WAF rules for your Application Load Balancers, API Gateways, and Amazon CloudFront distributions. Similarly, you can create AWS Shield Advanced protections for your Application Load Balancers, ELB Classic Load Balancers, Elastic IP Addresses and CloudFront distributions. Finally, with AWS Firewall Manager, you can enable security groups for your Amazon EC2 and ENI resource types in Amazon VPCs.
Benefits
* 1. Simplify management of firewall rules across your accounts
* 2. Ensure compliance of existing and new applications
* 3. Easily deploy managed rules across accounts
* 4. Enable rapid response to internet attacks
AWS Secrets Manager is incorrect. AWS Secrets Manager helps you to securely encrypt, store, and retrieve credentials for your databases and other services. Instead of hardcoding credentials in your apps, you can make calls to Secrets Manager to retrieve your credentials whenever needed. Secrets Manager helps you protect access to your IT resources and data by enabling you to rotate and manage access to your secrets.
AWS Shield is incorrect. AWS provides two levels of protection against DDoS attacks: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services. For added protection against DDoS attacks, AWS offers AWS Shield Advanced.
AWS WAF is incorrect. AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions or an Application Load Balancer. You can also use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses that requests originate from or values in the requests.

NEW QUESTION 28
A company is using IAM with Amazon EC2 to control whether users can perform a task using specific Amazon EC2 API actions and whether they can use specific AWS resources. A SysOps administrator attempts to launch an instance with a role, but he gets an AccessDenied error.
Which actions should the SysOps administrator take to fix this issue?

A. Modify the bucket policy to allow root user access from the Amazon S3 console or the AWS CLI
B. Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name
C. Verify that you have the identity-based policy permission to call the action and resource that youhave requested
D. Verify that your temporary security credentials haven't expired

Answer: B

Explanation:
Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name is the correct answer. When you attempt to launch an instance with a role and get an AccessDenied error check the following:
* 1. Launch an instance without an instance profile. This will help ensure that the problem is limited to IAM roles for Amazon EC2 instances.
* 2. If you are making requests as an IAM user, verify that you have the following permissions:ec2:RunInstances with a wildcard resource (“*”)iam:PassRole with the resource matching the role ARN (for example, arn:aws:iam::999999999999:role/ExampleRoleName)
* 3. Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name or a valid instance profile ARN.
* 4. Call the IAM GetInstanceProfile action to ensure that the instance profile has a role. Empty instance profiles will fail with an AccessDenied error.

NEW QUESTION 29
A company for compliance purposes needs to assess how well its resource configurations comply with internal practices, industry guidelines, and regulations.
Which tool should a SysOps administrator use to meet these requirements?

A. AWS Security Hub
B. AWS Shield
C. AWS Health
D. AWS Config

Answer: D

Explanation:
AWS Config is the correct answer. AWS Config can be used to assess how well your resource configurations comply with internal practices, industry guidelines, and regulations.
AWS Security Hub is incorrect. AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices.
Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.
AWS Shield is incorrect. AWS provides two levels of protection against DDoS attacks: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services.
For added protection against DDoS attacks, AWS offers AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, Amazon CloudFront distributions, and Amazon Route 53 hosted zones.
AWS Health is incorrect. AWS Health provides personalized information about events that can affect your AWS infrastructure, guides you through scheduled changes, and accelerates the troubleshooting

of issues that affect your AWS resources and accounts.

NEW QUESTION 33
A SysOps Administrator has implemented an Auto Scaling group with a step scaling policy. The Administrator notices that the additional instances have not been included in the aggregated metrics. Why are the additional instances missing from the aggregated metrics?

A. The warm-up period has not expired
B. The instances are still in the boot process
C. The instances have not been attached to the Auto Scaling group
D. The instances are included in a different set of metrics

Answer: B

NEW QUESTION 36

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 38
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SOA-C02 Exam with Our Prep Materials Via below:

https://www.certleader.com/SOA-C02-dumps.html