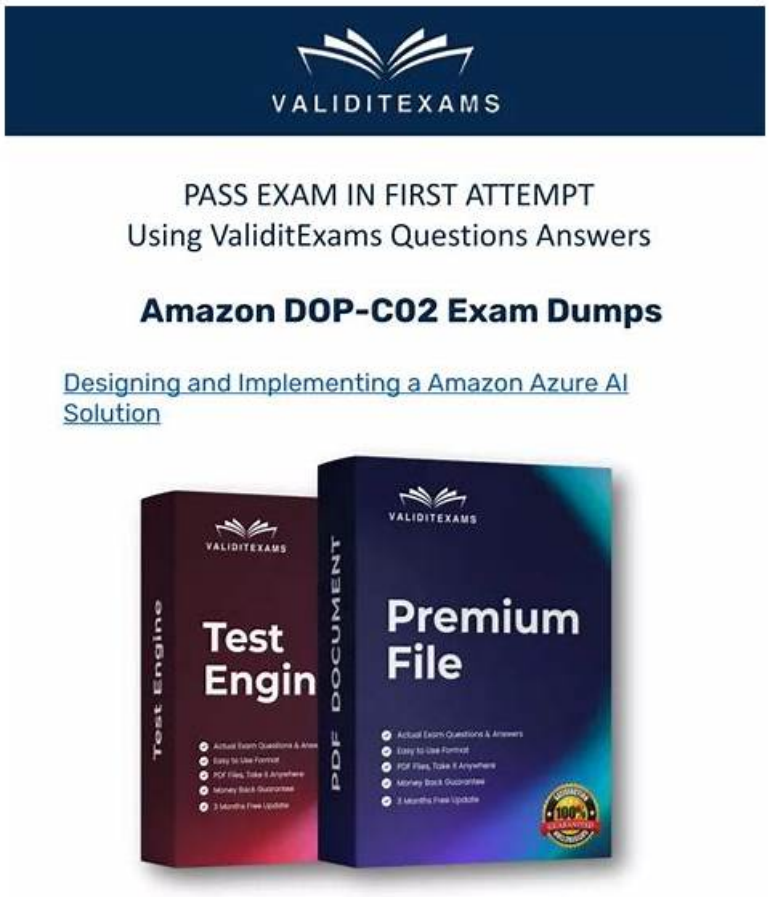
DOP-C02 Valid Exam Book, DOP-C02 Reliable Exam Voucher



What's more, part of that DumpsTests DOP-C02 dumps now are free: https://drive.google.com/open?id=1JWAF5Wa8YuT0cpykpfcCH6xNKzI1PLCy

We have created a number of reports and learning functions for evaluating your proficiency for the Amazon DOP-C02 exam dumps. In preparation, you can optimize Amazon DOP-C02 practice exam time and question type by utilizing our Amazon DOP-C02 Practice Test software. DumpsTests makes it easy to download Amazon DOP-C02 exam questions immediately after purchase. You will receive a registration code and download instructions via email.

Amazon DOP-C02 Exam is a professional-level certification offered by Amazon Web Services (AWS) for individuals who want to demonstrate their expertise in DevOps practices and tools. AWS Certified DevOps Engineer - Professional certification is intended for experienced DevOps professionals who have a deep understanding of the AWS platform and can design, implement, and manage DevOps solutions at scale.

>> DOP-C02 Valid Exam Book <<

Verified Amazon DOP-C02 Online Practice Test Engine

Our DOP-C02 test material is known for their good performance and massive learning resources. In general, users pay great attention to product performance. After a long period of development, our DOP-C02 research materials have a lot of innovation. We can guarantee that users will be able to operate flexibly, and we also take the feedback of users who use the AWS Certified DevOps Engineer - Professional exam dumps seriously. Once our researchers find that these recommendations are possible to implement, we will try to refine the details of the DOP-C02 Quiz guide. Our DOP-C02 quiz guide has been seeking innovation and continuous development.

Amazon AWS Certified DevOps Engineer - Professional Sample Questions (Q199-Q204):

NEW QUESTION # 199
A DevOps administrator is responsible for managing the security of a company's Amazon CloudWatch Logs log groups. The company's security policy states that employee IDs must not be visible in logs except by authorized personnel. Employee IDs follow the pattern of Emp-XXXXXX, where each X is a digit.
An audit discovered that employee IDs are found in a single log file. The log file is available to engineers, but the engineers are not authorized to view employee IDs. Engineers currently have an AWS IAM Identity Center permission that allows logs:* on all resources in the account.
The administrator must mask the employee ID so that new log entries that contain the employee ID are not visible to unauthorized personnel.
Which solution will meet these requirements with the MOST operational efficiency?

- A. Create a new data protection policy on the log group. Add an Emp-\d{6} custom data identifier configuration. Create an IAM policy that has a Deny action for the "Action":"logs:Unmask" permission on the resource. Attach the policy to the engineering accounts.
- B. Create a new data protection policy on the log group. Add managed data identifiers for the personal data category. Create an IAM policy that has a Deny action for the "NotAction":"logs:Unmask" permission on the resource. Attach the policy to the engineering accounts.
- C. Create an Amazon Data Firehose delivery stream that has an Amazon S3 bucket as the destination.Create a Firehose subscription filter on the log group that uses the Firehose delivery stream. Remove the "logs:*" permission on the engineering accounts. Create an Amazon Macie job on the S3 bucket that has an Emp-\d{6} custom identifier.
- D. Create an AWS Lambda function to parse a log file entry, remove the employee ID, and write the results to a new log file. Create a Lambda subscription filter on the log group and select the Lambda function. Grant the lambda:InvokeFunction permission to the log group.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Amazon CloudWatch Logs now supportsdata protection policiesthat can mask sensitive data in logs at ingestion time usingcustom data identifiers. By creating a custom data identifier matching the employee ID pattern (Emp-\d{6}), the administrator can mask those patterns in new log entries automatically.
Assigning an IAM policy that denies the logs:Unmask action to engineers prevents them from seeing unmasked sensitive data, enforcing least privilege access.
This approach is operationally efficient because it uses built-in CloudWatch Logs data protection capabilities without the need for complex custom code or manual log filtering.
Option C requires writing and managing Lambda functions for log transformation, increasing operational overhead. Option D is more complex and reactive rather than preventing the sensitive data exposure. Option B incorrectly references NotAction and managed identifiers that may not match the custom pattern.
Reference:
Amazon CloudWatch Logs Data Protection Policies:"You can create data protection policies with custom data identifiers to mask sensitive information such as employee IDs in log data."(AWS Documentation on CloudWatch Logs Data Protection)

NEW QUESTION # 200
A company's DevOps engineer is creating an AWS Lambda function to process notifications from an Amazon Simple Notification Service (Amazon SNS) topic. The Lambda function will process the notification messages and will write the contents of the notification messages to an Amazon RDS Multi-AZ DB instance.
During testing a database administrator accidentally shut down the DB instance. While the database was down the company lost several of the SNS notification messages that were delivered during that time.
The DevOps engineer needs to prevent the loss of notification messages in the future Which solutions will meet this requirement? (Select TWO.)

- A. Configure an Amazon Simple Queue Service (Amazon SQS> dead-letter queue for the SNS topic.
- B. Subscribe an Amazon Simple Queue Service (Amazon SQS) queue to the SNS topic Configure the Lambda function to process messages from the SQS queue.
- C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination of the Lambda function.
- D. Replace the RDS Multi-AZ DB instance with an Amazon DynamoDB table.

- E. Replace the SNS topic with an Amazon EventBridge event bus Configure an EventBridge rule on the new event bus to invoke the Lambda function for each event.

Answer: A,B

Explanation:
These solutions will meet the requirement because they will prevent the loss of notification messages in the future. An Amazon SQS queue is a service that provides a reliable, scalable, and secure message queue for asynchronous communication between distributed components. You can use an SQS queue to buffer messages from an SNS topic and ensure that they are delivered and processed by a Lambda function, even if the function or the database is temporarily unavailable.
Option C will configure an SQS dead-letter queue for the SNS topic. A dead-letter queue is a queue that receives messages that could not be delivered to any subscriber after a specified number of retries. You can use a dead-letter queue to store and analyze failed messages, or to reprocess them later. This way, you can avoid losing messages that could not be delivered to the Lambda function due to network errors, throttling, or other issues.
Option D will subscribe an SQS queue to the SNS topic and configure the Lambda function to process messages from the SQS queue. This will decouple the SNS topic from the Lambda function and provide more flexibility and control over the message delivery and processing. You can use an SQS queue to store messages from the SNS topic until they are ready to be processed by the Lambda function, and also to retry processing in case of failures. This way, you can avoid losing messages that could not be processed by the Lambda function due to database errors, timeouts, or other issues.

NEW QUESTION # 201
A company's DevOps team manages a set of AWS accounts that are in an organization in AWS Organizations The company needs a solution that ensures that all Amazon EC2 instances use approved AMIs that the DevOps team manages. The solution also must remediate the usage of AMIs that are not approved The individual account administrators must not be able to remove the restriction to use approved AMIs.
Which solution will meet these requirements?

- A. Create an AWS Lambda function that processes AWS CloudTrail events for Amazon EC2 Configure the Lambda function to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps team to the SNS topic. Deploy the Lambda function in each account in the organization Create an Amazon EventBridge rule in each account Configure the EventBridge rules to react to AWS CloudTrail events for Amazon EC2 and to invoke the Lambda function.
- B. Enable AWS Config across the organization Create a conformance pack that uses the approved -amis-by-id AWS Config managed rule with the list of approved AMIs. Deploy the conformance pack across the organization. Configure the rule to run the AWS-StopEC2Instance AWS Systems Manager Automation runbook for the noncompliant EC2 instances.
- C. Use AWS CloudFormation StackSets to deploy an Amazon EventBridge rule to each account. Configure the rule to react to AWS CloudTrail events for Amazon EC2 and to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps team to the SNS topic
- D. Use AWS CloudFormation StackSets to deploy the approved-amis-by-id AWS Config managed rule to each account. Configure the rule with the list of approved AMIs. Configure the rule to run the the AWS-StopEC2Instance AWS Systems Manager Automation runbook for the noncompliant EC2 instances.

Answer: B

Explanation:
Enable AWS Config Across the Organization:
AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. It can be used to assess, audit, and evaluate the configurations of your resources.
Enabling AWS Config across the organization ensures that all accounts are monitored for compliance.
Create a Conformance Pack Using the approved-amis-by-id AWS Config Managed Rule:
A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed across an organization.
The approved-amis-by-id managed rule checks whether running instances are using approved AMIs.
Deploy the Conformance Pack Across the Organization:
Deploying the conformance pack across the organization ensures that all accounts adhere to the policy of using only approved AMIs.
The conformance pack can be deployed via the AWS Management Console, CLI, or SDKs.
Configure the Rule to Run the AWS-StopEC2Instance AWS Systems Manager Automation Runbook for Non-Compliant EC2 Instances:
The AWS-StopEC2Instance runbook can be configured to automatically stop any EC2 instances that are found to be non-

compliant (i.e., not using approved AMIs).
This remediation action ensures that any unauthorized instances are promptly stopped, enforcing the policy without manual intervention.
By following these steps, the solution ensures that all EC2 instances across the organization use approved AMIs, and any non-compliant instances are remediated automatically.
Reference:
AWS Config Conformance Packs
AWS Config Managed Rules
AWS Systems Manager Automation Runbooks

NEW QUESTION # 202
A company's security team requires that all external Application Load Balancers (ALBs) and Amazon API Gateway APIs are associated with AWS WAF web ACLs. The company has hundreds of AWS accounts, all of which are included in a single organization in AWS Organizations. The company has configured AWS Config for the organization. During an audit, the company finds some externally facing ALBs that are not associated with AWS WAF web ACLs.
Which combination of steps should a DevOps engineer take to prevent future violations? (Choose two.)

- A. Delegate Amazon GuardDuty to a security account.
- B. Create an AWS Firewall Manager policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
- C. Configure an AWS Config managed rule to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
- D. Create an Amazon GuardDuty policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
- E. Delegate AWS Firewall Manager to a security account.

Answer: B,E

Explanation:
If instead you want to automatically apply the policy to existing in-scope resources, choose Auto remediate any noncompliant resources. This option creates a web ACL in each applicable account within the AWS organization and associates the web ACL with the resources in the accounts. When you choose Auto remediate any noncompliant resources, you can also choose to remove existing web ACL associations from in-scope resources, for the web ACLs that aren't managed by another active Firewall Manager policy. If you choose this option, Firewall Manager first associates the policy's web ACL with the resources, and then removes the prior associations. If a resource has an association with another web ACL that's managed by a different active Firewall Manager policy, this choice doesn't affect that association.

NEW QUESTION # 203
A company has an AWS Cloud Format ion slack that is deployed in a single AWS account. The company has configured the stack to send event notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
A DevOps engineer must implement an automated solution that applies a tag to the specific Cloud Formation stack instance only after a successful stack update occurs. The DevOps engineer has created an AWS Lambda function that applies and updates this tag (or the specific slack instance.
Which solution will meet these requirements?

- A. Adjust the configuration of the CloudFormation stack to send notifications for only an UPDATE COMPLETE instance status event to the SNS topic. Subscribe the Lambda function to the SNS topic.
- B. Run the AWS-UpdateCloudfomationStack AWS Systems Manager Automation runbook when Systems Manager detects an UPDATE_COMPLETE event for the instance status of the Cloud Formation stack.
  Configure the runbook to invoke the Lambda function.
- C. Create an Amazon EventBridge rule that matches the UPDATE COMPLETE event pattern for the instance status of the CloudFormation stack. Configure the rule to invoke the Lambda function.
- D. Create a custom AWS Config rule that produces a compliance change event if the CloudFormation stack has an UPDATE_COMPLETE instance status. Configure AWS Config to directly invoke the Lambda function to automatically remediate the change event.

Answer: C

Explanation:

* Step 1: Reacting to CloudFormation Stack Events with EventBridgeAWS CloudFormation emits events during the lifecycle of a stack, including the UPDATE_COMPLETE event after a successful stack update. You can use Amazon EventBridge to detect this event and trigger a specific action (such as invoking a Lambda function).
* Action:Create an EventBridge rule that listens for the UPDATE_COMPLETE event for the CloudFormation stack.
* Why:EventBridge allows you to automatically detect CloudFormation stack lifecycle events and take action based on them.
* Step 2: Invoking the Lambda FunctionAfter the EventBridge rule detects the UPDATE_COMPLETE event, it can invoke the pre-configured Lambda function to apply or update the tag on the specific CloudFormation stack instance.
* Action:Configure the EventBridge rule to invoke the Lambda function when the UPDATE_COMPLETE event occurs.
* Why:This automation ensures that the tag is applied immediately after a successful stack update without any manual intervention.

NEW QUESTION # 204

.....

Passing the DOP-C02 exam requires the ability to manage time effectively. In addition to the AWS Certified DevOps Engineer - Professional (DOP-C02) exam study materials, practice is essential to prepare for and pass the Amazon DOP-C02 exam on the first try. It is critical to do self-assessment and learn time management skills. Because the DOP-C02 test has a restricted time constraint, time management must be exercised to get success. Only with enough practice one can answer real Amazon DOP-C02 exam questions in a given amount of time.