DOP-C01 Q&As

AWS Certified DevOps Engineer - Professional (DOP-C01)

Pass Amazon DOP-C01 Exam with 100% Guarantee

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

https://www.leads4pass.com/aws-devops-engineer-professional.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

A DevOps Engineer must automate a weekly process of identifying unnecessary permissions on a per- user basis, across all users in an AWS account. This process should evaluate the permissions currently granted to each user by examining the user\\'s attached IAM access policies compared to the permissions the user has actually used in the past 90 days. Any differences in the comparison would indicate that the user has more permissions than are required. A report of the deltas should be sent to the Information Security team for further review and IAM user access policy revisions, as required. Which solution is fully automated and will produce the MOST detailed deltas report?

A. Create an AWS Lambda function that calls the IAM Access Advisor API to pull service permissions granted on a user-by-user basis for all users in the AWS account. Ensure that Access Advisor is configured with a tracking period of 90 days. Invoke the Lambda function using an Amazon CloudWatch Events rule on a weekly schedule. For each record, by user, by service, if the Access Advisor Last Accesses field indicates a day count instead of "Not accesses in the tracking period," this indicates a delta compared to what is in the user\\'s currently attached access polices. After Lambda has iterated through all users in the AWS account, configure it to generate a report and send the report using Amazon SES.

B. Configure an AWS CloudTrail trail that spans all AWS Regions and all read/write events, and point this trail to an Amazon S3 bucket. Create Amazon Athena table and specify the S3 bucket ARN in the CREATE TABLE query. Create an AWS Lambda function that accesses the Athena table using the SDK, which performs a SELECT, ensuring that the WHERE clause includes userIdentity, eventName, and eventTime. Compare the results against the user\\'s currently attached IAM access policies to determine any deltas. Configure an Amazon CloudWatch Events schedule to automate this process to run once a week. Configure Amazon SES to send a consolidated report to the Information Security team.

C. Configure VPC Flow Logs on all subnets across all VPCs in all regions to capture user traffic across the entire account. Ensure that all logs are being sent to a centralized Amazon S3 bucket, so all flow logs can be consolidated and aggregated. Create an AWS Lambda function that is triggered once a week by an Amazon CloudWatch Events schedule. Ensure that the Lambda function parses the flow log files for the following information: IAM user ID, subnet ID, VPC ID, Allow/Reject status per API call, and service name. Then have the function determine the deltas on a user-by-user basis. Configure the Lambda function to send the consolidated report using Amazon SES.

D. Create an Amazon ES cluster and note its endpoint URL, which will be provided as an environment variable into a Lambda function. Configure an Amazon S3 event on a AWS CloudTrail trail destination S3 bucket and ensure that the event is configured to send to a Lambda function. Create the Lambda function to consume the events, parse the input from JSON, and transform it to an Amazon ES document format. POST the documents to the Amazon ES cluster\\'s endpoint by way of the passed-in environment variable. Make sure that the proper indexing exists in Amazon ES and use Apache Lucene queries to parse the permissions on a user-by-user basis. Export the deltas into a report and have Amazon ES send the reports to the Information Security team using Amazon SES every week.

Correct Answer: B

QUESTION 2

You have just recently deployed an application on EC2 instances behind an ELB. After a couple of weeks, customers are complaining on receiving errors from the application. You want to diagnose the errors and are trying to get errors from the ELB access logs. But the ELB access logs are empty. What is the reason for this.

A. You do not have the appropriate permissions to access the logs

B. You do not have your CloudWatch metrics correctly configured

C. ELB Access logs are only available for a maximum of one week

D. Access logging is an optional feature of Elastic Load Balancing that is disabled by default

Correct Answer: D

Clastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Cach log contains information such as the time the request was received, the client\\'s IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues. Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer. Clastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify. You can disable access logging at any time.

QUESTION 3

You have been given a business requirement to retain log files for your application for 10 years. You need to regularly retrieve the most recent logs for troubleshooting. Your logging system must be cost-effective, given the large volume of

logs.

What technique should you use to meet these requirements?

A. Store your log in Amazon CloudWatch Logs.

B. Store your logs in Amazon Glacier.

C. Store your logs in Amazon S3, and use lifecycle policies to archive to Amazon Glacier.

D. Store your logs in HDFS on an Amazon EMR cluster.

E. Store your logs on Amazon EBS, and use Amazon EBS snapshots to archive them.

Correct Answer: C

QUESTION 4

A company is using Amazon EC2 for various workloads. Company policy requires that instances be managed centrally to standardize configurations. These configurations include standard logging, metrics, security assessments, and weekly patching.

How can the company meet these requirements? (Choose three.)

A. Use AWS Config to ensure all EC2 instances are managed by Amazon Inspector.

B. Use AWS Config to ensure all EC2 instances are managed by AWS Systems Manager.

C. Use AWS Systems Manager to install and manage Amazon Inspector, Systems Manager Patch Manager, and the Amazon CloudWatch agent on all instances.

D. Use Amazon Inspector to install and manage AWS Systems Manager, Systems Manager Patch Manager, and the Amazon CloudWatch agent on all instances.

E. Use AWS Systems Manager maintenance windows with Systems Manager Run Command to schedule Systems Manager Patch Manager tasks. Use the Amazon CloudWatch agent to schedule Amazon Inspector assessment runs.

F. Use AWS Systems Manager maintenance windows with Systems Manager Run Command to schedule Systems Manager Patch Manager tasks. Use Amazon CloudWatch Events to schedule Amazon Inspector assessment runs.

Correct Answer: BDE

QUESTION 5

A DevOps engineer is implementing governance controls for a company that requires its infrastructure to be housed within the United States. The engineer must restrict which Regions can be used, and ensure an alert is sent as soon as possible if any activity outside the governance policy takes place. The controls should be automatically enabled on any new Region outside the United States.

Which combination of actions will meet these requirements? (Choose two.)

A. Create an AWS Organizations SCP that denies access to all non-global services in non-US Regions. Attach the policy to the root of the organization.

B. Configure AWS CloudTrail to send logs to Amazon CloudWatch Logs and enable it for all Regions. Use a CloudWatch Logs metric filter to send an alert on any service activity in non-US Regions.

C. Use an AWS Lambda function that checks for AWS service activity and deploy it to all Regions. Write an Amazon CloudWatch Events rule that runs the Lambda function every hour, sending an alert if activity is found in a non-US Region.

D. Use an AWS Lambda function to query Amazon Inspector to look for service activity in non-US Regions and send alerts if any activity is found.

E. Write an SCP using the aws:RequestedRegion condition key limiting access to US Regions. Apply the policy to all users, groups, and roles.

Correct Answer: BC