**Braindump2go Guarantee All Exams 100% Pass
One Time!**

➢ **Vendor: Amazon**

➢ **Exam Code: AWS-DevOps-Engineer-Professional**

➢ **Exam Name: AWS Certified DevOps Engineer - Professional (DOP-C01)**

➢ **New Updated Questions from Braindump2go (Updated in October/2021)**

Visit Braindump2go and Download Full Version AWS-DevOps-Engineer-Professional Exam Dumps

QUESTION 552
A company manages an application that stores logs in Amazon CloudWatch Logs. The company wants to archive the logs in Amazon S3. Logs are rarely accessed after 90 days and must be retained for 10 years.
Which combination of steps should a DevOps engineer take to meet these requirements? (Choose two.)

A. Configure a CloudWatch Logs subscription filter to use AWS Glue to transfer all logs to an S3 bucket.
B. Configure a CloudWatch Logs subscription filter to use Amazon Kinesis Data Firehose to stream all logs to an S3 bucket.
C. Configure a CloudWatch Logs subscription filter to stream all logs to an S3 bucket.
D. Configure the S3 bucket lifecycle policy to transition logs to S3 Glacier after 90 days and to expire logs after 3.650 days.
E. Configure the S3 bucket lifecycle policy to transition logs to Reduced Redundancy after 90 days and to expire logs after 3.650 days.

Answer: BC
Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/SubscriptionFilters.html

QUESTION 553
A company gives its employees limited rights to AWS. DevOps engineers have the ability to assume an administrator role. For tracking purposes, the security team wants to receive a near-real-time notification when the administrator role is assumed.
How should this be accomplished?

A. Configure AWS Config to publish logs to an Amazon S3 bucket.
Use Amazon Athena to query the logs and send a notification to the security team when the administrator role is assumed.
B. Configure Amazon GuardDuty to monitor when the administrator role is assumed and send a notification to the security team.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) event rule using an AWS Management Console sign-in events event pattern that publishes a message to an Amazon SNS topic if the administrator role is assumed.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) events rule using an AWS API call that uses an AWS CloudTrail event pattern to trigger an AWS Lambda function that publishes a message to an Amazon SNS topic if the administrator role is assumed.

Answer: C
Explanation:

https://docs.aws.amazon.com/eventbridge/latest/userguide/user-guide.pdf

QUESTION 554
A development team manages website deployments using AWS CodeDeploy blue/green deployments. The application is running on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group.
When deploying a new revision, the team notices the deployment eventually fails, but it takes a long time to fail. After further inspection, the team discovers the AllowTraffic lifecycle event ran for an hour and eventually failed without providing any other information. The team wants to ensure failure notices are delivered more quickly while maintaining application availability even upon failure.
Which combination of actions should be taken to meet these requirements? (Choose two.)

A. Change the deployment configuration to CodeDeployDefault.AllAtOnce to speed up the deployment process by deploying to all of the instances at the same time.
B. Create a CodeDeploy trigger for the deployment failure event and make the deployment fail as soon as a single health check failure is detected.
C. Reduce the HealthCheckIntervalSeconds and UnhealthyThresholdCount values within the target group health checks to decrease the amount of time it takes for the application to be considered unhealthy.
D. Use the appspec.yml file to run a script on the AllowTraffic hook to perform lighter health checks on the application instead of making CodeDeploy wait for the target group health checks to pass.
E. Use the appspec,yml file to run a script on the BeforeAllowTraffic hook to perform hearth checks on the application and fail the deployment if the health checks performed by the script are not successful.

Answer: AC

QUESTION 555
A company is running a number of internet-facing APIs that use an AWS Lambda authorizer to control access. A security team wants to be alerted when a large number of requests are failing authorization, as this may indicate API abuse. Given the magnitude of API requests, the team wants to be alerted only if the number of HTTP 403 Forbidden responses goes above 2% of overall API calls.
Which solution will accomplish this?

A. Use the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, and use metric math to create a CloudWatch alarm.
Use the (403Error/Count)*100 mathematical expression when defining the alarm.
Set the alarm threshold to be greater than 2.
B. Write a Lambda function that fetches the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, calculate the percentage of errors, then push a custom metric to CloudWatch named Custorn403Percent.
Create a CloudWatch alarm based on this custom metric. Set the alarm threshold to be greater than 2.
C. Configure Amazon API Gateway to send custom access logs to Amazon CloudWatch Logs.
Create a log filter to produce a custom metric for the HTTP 403 response code named Custom403Error.
Use this custom metric and the default API Gateway Count metric sent to CloudWatch, and use metric match to create a CloudWatch alarm.
Use the (Custom403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.
D. Configure Amazon API Gateway to enable custom Amazon CloudWatch metrics, enable the ALL_STATUS_CODE option, and define an APICustom prefix.
Use CloudWatch metric math to create a CloudWatch alarm.
Use the (APICustom403Error/Count)*100 mathematical expression when defining the alarm.
Set the alarm threshold to be greater than 2.

Answer: C
Explanation:

https://aws.amazon.com/blogs/compute/analyzing-api-gateway-custom-access-logs-for-custom-domain-names/

QUESTION 556
A company uses AWS Organizations to manage multiple accounts. Information security policies require that all unencrypted Amazon EBS volumes be marked as non-compliant. A DevOps engineer needs to automatically deploy the solution and ensure that this compliance check is always present.
With solution will accomplish this?

A. Create an AWS CloudFormation template that defines an AWS Inspector rule to check whether EBS encryption is enabled.
Save the template to an Amazon S3 bucket that has been shared with all accounts within the company.
Update the account creation script pointing to the CloudFormation template in Amazon S3.
B. Create an AWS Config organizational rule to check whether EBS encryption is enabled and deploy the rule using the AWS CLI.
Create and apply an SCP to prohibit stopping and deleting AWS Config across the organization.
C. Create an SCP in Organizations.
Set the policy to prevent the launch of Amazon EC2 instances without encryption on the EBS volumes using a conditional expression.
Apply the SCP to all AWS accounts.
Use Amazon Athena to analyze the AWS CloudTrail output, looking for events that deny an ec2:RunInstances action.
D. Deploy an IAM role to all accounts from a single trusted account.
Build a pipeline with AWS CodePipeline with a stage in AWS Lambda to assume the IAM role, and list all EBS volumes in the account. Publish a report to Amazon S3.

Answer: A

QUESTION 557
A company's application is running on Amazon EC2 instances in an Auto Scaling group. A DevOps engineer needs to ensure there are at least four application servers running at all times. Whenever an update has to be made to the application, the engineer creates a new AMI with the updated configuration and updates the AWS CloudFormation template with the new AMI ID. After the stack finishes, the engineer manually terminates the old instances one by one, verifying that the new instance is operational before proceeding. The engineer needs to automate this process.
Which action will allow for the LEAST number of manual steps moving forward?

A. Update the CloudFormation template to include the UpdatePolicy attribute with the AutoScalingRollingUpdate policy.
B. Update the CloudFormation template to include the UpdatePolicy attribute with the AutoScalingReplacingUpdate policy.
C. Use an Auto Scaling lifecycle hook to verify that the previous instance is operational before allowing the DevOps engineer's selected instance to terminate.
D. Use an Auto Scaling lifecycle hook to confirm there are at least four running instances before allowing the DevOps engineer's selected instance to terminate.

Answer: B