This page was exported from - Braindump2go Exam Dumps Free Download
Export date: Thu Mar 28 22:11:23 2024 / +0000 GMT

[2017-Feb-NEWHigh Quality AWS Certified DevOps Engineer - Professional Exam VCE Dumps 190Q&As Free Share[Q31-Q40

2017 Feb NEW Amazon AWS Certified DevOps Engineer - Professional Exam Dumps (PDF & VCE) Updated Today!1.|NEW Amazon AWS Certified DevOps Engineer - Professional PDF and VCE Dumps 190Q&As Download: http://www.braindump2go.com/aws-devops-engineer-professional.html2.|NEW Amazon AWS Certified DevOps Engineer - Professional Exam Questions and Answers Download:https://1drv.ms/f/s!AvI7wzKf6QBjgh4jQ6bIe9aoaNlC QUESTION 31The project you are working on currently uses a single AWS CloudFormation template to deploy its AWS infrastructure, which supports a multi-tier web application. You have been tasked with organizing the AWS CloudFormation resources so that they can be maintained in the future, and so that different departments such as Networking and Security can review the architecture before it goes to Production. How should you do this in a way that accommodates each department, using their existing workflows? A. Organize the AWS CloudFormation template so that related resources are next to each other in the template, such as VPC subnets and routing rules for Networking and security groups and IAM information for Security.B. Separate the AWS CloudFormation template into a nested structure that has individual templates for the resources that are to be governed by different departments, and use the outputs from the networking and security stacks for the application template that you controlC. Organize the AWS CloudFormation template so that related resources are next to each other in the template for each department's use, leverage your existing continuous integration tool to constantly deploy changes from all parties to the Production environment, and then run tests for validation.D. Use a custom application and the AWS SDK to replicate the resources defined in the current AWS CloudFormation template, and use the existing code review system to allow other departments to approve changes before altering the application for future deployments. Answer: B QUESTION 32You currently run your infrastructure on Amazon EC2 instances behind an Auto Scaling group> All logs for you application are currently written to ephemeral storage. Recently your company experienced a major bug in code that made it through testing and was ultimately deployed to your fleet. This bug triggered your Auto Scaling group to scale up and back down before you could successfully retrieve the logs off your server to better assist you in troubleshooting the bug.Which technique should you use to make sure you are able to review your logs after your instances have shut down? A. Configure the ephemeral policies on your Auto Scaling group to back up on terminate.B. Configure your Auto Scaling policies to create a snapshot of all ephemeral storage on terminate.C. Install the CloudWatch Logs Agent on your AMI, and configure CloudWatch Logs Agent to stream your logs.D. Install the CloudWatch monitoring agent on your AMI, and set up new SNS alert for CloudWatch metrics that triggers the CloudWatch monitoring agent to backup all logs on the ephemeral drive.E. Install the CloudWatch monitoring agent on your AMI, Update your Auto Scaling policy to enable automated CloudWatch Log copy. Answer: C QUESTION 33Management has reported an increase in the monthly bill from Amazon web services, and they are extremely concerned with this increased cost. Management has asked you to determine the exact cause of this increase.After reviewing the billing report, you notice an increase in the data transfer cost. How can you provide management with a better insight into data transfer use? A. Update your Amazon CloudWatch metrics to use five-second granularity, which will give better detailed metrics that can be combined with your billing data to pinpoint anomalies.B. Use Amazon CloudWatch Logs to run a map-reduce on your logs to determine high usage and data transfer.C. Deliver custom metrics to Amazon CloudWatch per application that breaks down application data transfer into multiple, more specific data points.D. Using Amazon CloudWatch metrics, pull your Elastic Load Balancing outbound data transfer metrics monthly, and include them with your billing report to show which application is causing higher bandwidth usage. Answer: C QUESTION 34During metric analysis, your team has determined that the company's website is experiencing response times during peak hours that are higher than anticipated. You currently rely on Auto Scaling to make sure that you are scaling your environment during peak windows. How can you improve your Auto Scaling policy to reduce this high response time? Choose 2 answers. A. Push custom metrics to CloudWatch to monitor your CPU and network bandwidth from your servers, which will allow your Auto Scaling policy to have better fine-grain insight.B. Increase your Auto Scaling group's number of max servers.C. Create a script that runs and monitors your servers; when it detects an anomaly in load, it posts to an Amazon SNS topic that triggers Elastic Load Balancing to add more servers to the load balancer.D. Push custom metrics to CloudWatch for your application that include more detailed information about your web application, such as how many requests it is handling and how many are waiting to be processed.E. Update the CloudWatch metric used for your Auto Scaling policy, and enable sub-minute granularity to allow auto scaling to trigger faster. Answer: BD QUESTION 35You are responsible for your company's large multi-tiered Windows-based web application running on Amazon EC2 instances situated behind a load balancer. While reviewing metrics, you've started noticing an upwards trend for slow customer page load time. Your manager has asked you to come up with a solution to ensure that customer load time is not affected by too many requests per second.Which technique would

you use to solve this issue? A. Re-deploy your infrastructure using an AWS CloudFormation template. Configure Elastic Load Balancing health checks to initiate a new AWS CloudFormation stack when health checks return failed.B. Re-deploy your infrastructure using an AWS CloudFormation template. Spin up a second AWS CloudFormation stack. Configure Elastic Load Balancing SpillOver functionality to spill over any slow connections to the second AWS CloudFormation stack.C. Re-deploy your infrastructure using AWS CloudFormation, Elastic Beanstalk, and Auto Scaling. Set up your Auto Scaling group policies to scale based on the number of requests per second as well as the current customer load time.D. Re-deploy your application using an Auto Scaling template. Configure the Auto Scaling template to spin up a new Elastic Beanstalk application when the customer load time surpasses your threshold. Answer: C QUESTION 36Your company has multiple applications running on AWS. Your company wants to develop a tool that notifies on-call teams immediately via email when an alarm is triggered in your environment.You have multiple on-cal teams that work different shifts, and the tool should handle notifying the correct teams at the correct times.How should you implement this solution? A. Create an Amazon SNS topic and an Amazon SQS queue. Configure the Amazon SQS queue as a subscriber to the Amazon SNS topic. Configure CloudWatch alarms to notify this topic when an alarm is triggered. Create an Amazon EC2 Auto Scaling group with both minimum and desired Instances configured to 0. Worker nodes in this group spawn when messages are added to the queue. Workers then use Amazon Simple Email Service to send messages to your on call teams.B. Create an Amazon SNS topic and configure your on-call team email addresses as subscribers. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to this new topic.Notifications will be sent to on-call users when a CloudWatch alarm is triggered.C. Create an Amazon SNS topic and configure your on-call team email addresses as subscribers. Create a secondary Amazon SNS topic for alarms and configure your CloudWatch alarms to notify this topic when triggered. Create an HTTP subscriber to this topic that notifies your application via HTTP POST when an alarm is triggered. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to the first topic so that on-call engineers receive alerts.D. Create an Amazon SNS topic for each on-call group, and configure each of these with the team member emails as subscribers. Create another Amazon SNS topic and configure your CloudWatch alarms to notify this topic when triggered. Create an HTTP subscriber to this topic that notifies your application via HTTP POST when an alarm is triggered. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to the correct team topic when on shift. Answer: D QUESTION 37 Your company releases new features with high frequency while demanding high application availability. As part of the application's A/B testing, logs from each updated Amazon EC2 instance of the application need to be analyzed in near real-time, to ensure that the application is working flawlessly after each deployment. If the logs show arty anomalous behavior, then the application version of the instance is changed to a more stable one.Which of the following methods should you use for shipping and analyzing the logs in a highly available manner? A. Ship the logs to Amazon S3 for durability and use Amazon EMR to analyze the logs in a batch manner each hour.B. Ship the logs to Amazon CloudWatch Logs and use Amazon EMR to analyze the logs in a batch manner each hour.C. Ship the logs to an Amazon Kinesis stream and have the consumers analyze the logs in a live manner.D. Ship the logs to a large Amazon EC2 instance and analyze the logs in a live manner.E. Store the logs locally on each instance and then have an Amazon Kinesis stream pull the logs for live analysis. Answer: C QUESTION 38You have a code repository that uses Amazon S3 as a data store. During a recent audit of your security controls, some concerns were raised about maintaining the integrity of the data in the Amazon S3 bucket. Another concern was raised around securely deploying code from Amazon S3 to applications running on Amazon EC2 in a virtual private cloud.What are some measures that you can implement to mitigate these concerns? Choose 2 answers. A. Add an Amazon S3 bucket policy with a condition statement to allow access only from Amazon EC2 instances with RFC 1918 IP addresses and enable bucket versioning.B. Add an Amazon S3 bucket policy with a condition statement that requires multi-factor authentication in order to delete objects and enable bucket versioning.C. Use a configuration management service to deploy AWS Identity and Access Management user credentials to the Amazon EC2 instances. Use these credentials to securely access the Amazon S3 bucket when deploying code.D. Create an Amazon Identity and Access Management role with authorization to access the Amazon 53 bucket, and launch all of your application's Amazon EC2 instances with this role.E. Use AWS Data Pipeline to lifecycle the data in your Amazon S3 bucket to Amazon Glacier on a weekly basis.F. Use AWS Data Pipeline with multi-factor authentication to securely deploy code from the Amazon .5.3 bucket to your Amazon EC2 instances. Answer: BD QUESTION 39You have an application consisting of a stateless web server tier running on Amazon EC2 instances behind load balancer, and are using Amazon RDS with read replicas. Which of the following methods should you use to implement a self-healing and cost-effective architecture? Choose 2 answers. A. Set up a third-party monitoring solution on a cluster of Amazon EC2 instances in order to emit custom CloudWatch metrics to trigger the termination of unhealthy Amazon EC2 instances. B. Set up scripts on each Amazon EC2 instance to frequently send ICMP pings to the load balancer in order to determine which instance is unhealthy and replace it.C. Set up an Auto Scaling group for the web server tier along with an Auto Scaling policy that

uses the Amazon RDS DB CPU utilization CloudWatch metric to scale the instances.D. Set up an Auto Scaling group for the web server tier along with an Auto Scaling policy that uses the Amazon EC2 CPU utilization CloudWatch metric to scale the instances.E. Use a larger Amazon EC2 instance type for the web server tier and a larger DB instance type for the data storage layer to ensure that they don't become unhealthy.F. Set up an Auto Scaling group for the database tier along with an Auto Scaling policy that uses the Amazon RDS read replica lag CloudWatch metric to scale out the Amazon RDS read replicas. G. Use an Amazon RDS Multi-AZ deployment. Answer: AD QUESTION 40Your application is currently running on Amazon EC2 instances behind a load balancer. Your management has decided to use a Blue/Green deployment strategy.How should you implement this for each deployment? A. Set up Amazon Route 53 health checks to fail over from any Amazon EC2 instance that is currently being deployed to.B. Using AWS CloudFormation, create a test stack for validating the code, and then deploy the code to each production Amazon EC2 instance.C. Create a new load balancer with new Amazon EC2 instances, carry out the deployment, and then switch DNS over to the new load balancer using Amazon Route 53 after testing.D. Launch more Amazon EC2 instances to ensure high availability, de-register each Amazon EC2 instance from the load balancer, upgrade it, and test it, and then register it again with the load balancer. Answer: C !!!RECOMMEND!!! 1.|NEW Amazon AWS Certified DevOps Engineer - Professional PDF and VCE Dumps 190Q&As Download:http://www.braindump2go.com/aws-devops-engineer-professional.html2.|NEW Amazon AWS Certified DevOps Engineer - Professional Study Guide Video: YouTube Video: YouTube.com/watch?v=nRhDUfpWQgE