Free Questions for DOP-C01 by go4braindumps

Shared by Camacho on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During metric analysis, your team has determined that the company's website during peak hours is experiencing response times 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.

Options:

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 betterfine-grain insight.

B- IncreaseyourAutoScalinggroup'snumberofmaxservers.

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.

Answer:

B, D

Explanation:

Option B makes sense because maybe the max servers is low hence the application cannot handle the peak load.

Option D helps in ensuring Autoscaling can scale the group on the right metrics.

For more information on Autoscaling health checks, please refer to the below document link: from AWS

http://docs.aws.a mazon.com/autoscaling/latest/userguide/healthcheck.html

Question 2

Question Type: MultipleChoice

You 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?

Options:

A- Re-deploy your infrastructure usingan 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 Scalinggroup 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

Explanation:

Auto Scaling helps you ensure that you have the correct number of Amazon CC2 instances available to handle the load for your application. You create collections of

CC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Auto Scaling ensures that your group

never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Auto Scaling ensures that yourgroup never goes

above this size. If you specify the desired capacity, either when you create the group or at any time thereafter. Auto Scaling ensures that yourgroup has this many

instances. If you specify scaling policies, then Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

Option A and B are invalid because Autoscaling is required to solve the issue to ensure the application can handle high traffic loads.

Option D is invalid because there is no Autoscaling template.

For more information on Autoscaling, please refer to the below document link: from AWS

http://docs.aws.amazon.com/autoscaling/latest/userguide/Whatl sAutoScaling.html

Question 3

Question Type: MultipleChoice

Your 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-call teams that work different shifts, and the tool should handle notifying the correct teams at the correct times. How should you implement this solution?

Options:

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

Explanation:

Option D fulfils all the requirements

1) First is to create a SNS topic for each group so that the required members get the email addresses.

2) Ensure the application uses the HTTPS endpoint and the SDK to publish messages Option A is invalid because the SQS service is not required.

Option B and C are incorrect. As per the requirement we need to provide notification to only those on-call teams who are working in that particular shift when an alarm is triggered. It need not have to be send to all the on-call teams of the company. With Option B & C, since we are not configuring the SNS topic for each on call team the notifications will be send to all the on-call teams. Hence these 2 options are invalid. For more information on setting up notifications, please refer to the below document link: from AWS

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_SetupSNS.html

Question 4

Question Type: **MultipleChoice**

You have an ELB setup in AWS with EC2 instances running behind it. You have been requested to monitor the incoming connections to the ELB. Which of the below options can suffice this requirement?

Options:

A- UseAWSCIoudTrail with your load balancer

B- Enable access logs on the load balancer

C- Use a CloudWatch Logs Agent

D- Create a custom metric CloudWatch filter on your load balancer

Answer:

B

Explanation:

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.

Option A is invalid because this service will monitor all AWS services

Option C and D are invalid since CLB already provides a logging feature.

For more information on ELB access logs, please refer to the below document link: from AWS

http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection. html

Question 5

Question Type: MultipleChoice

Which Auto Scaling process would be helpful when testing new instances before sending traffic to them, while still keeping them in your Auto Scaling Group?

Options:

A- Suspend the process AZ Rebalance

B- Suspend the process Health Check

C- Suspend the process Replace Unhealthy

D- Suspend the process AddToLoadBalancer

Answer:

D

Explanation:

If you suspend Ad dTo Load Balancer, Auto Scaling launches the instances but does not add them to the load balancer or target group. If you resume

the AddTo Load Balancer process. Auto Scaling resumes adding instances to the load balancer or target group when they are launched. However, Auto Scaling does

not add the instances that were launched while this process was suspended. You must register those instances manually.

Option A is invalid because this just balances the number of CC2 instances in the group across the Availability Zones in the region

Option B is invalid because this just checks the health of the instances. Auto Scaling marks an instance as unhealthy if Amazon CC2 or Clastic Load Balancing tells

Auto Scaling that the instance is unhealthy.

Option C is invalid because this process just terminates instances that are marked as unhealthy and later creates new instances to replace them.

For more information on process suspension, please refer to the below document link: from AWS

http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html

Question 6

Question Type: **MultipleChoice**

Your application stores sensitive information on an EBS volume attached to your EC2 instance. How can you protect your information? Choose two answers from the options given below

Options:

A- Unmount the EBS volume, take a snapshot and encrypt the snapshot. Re-mount the Amazon EBS volume

B- It is not possible to encrypt an EBS volume, you must use a lifecycle policy to transfer data to S3 for encryption.

C- Copy the unencrypted snapshot and check the box to encrypt the new snapshot. Volumes restored from this encrypted snapshot will also be encrypted.

D- Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete the old Amazon EBS volume *t

Answer:

C, D

Explanation:

These steps are given in the AWS documentation

To migrate data between encrypted and unencrypted volumes

1) Create your destination volume (encrypted or unencrypted, depending on your need).

2) Attach the destination volume to the instance that hosts the data to migrate.

3) Make the destination volume available by following the procedures in Making an Amazon EBS Volume Available for Use. For Linux instances, you can create a mount point at /mnt/destination and mount the destination volume there.

4) Copy the data from your source directory to the destination volume. It may be most convenient to use a bulk-copy utility for this.

To encrypt a volume's data by means of snapshot copying

1) Create a snapshot of your unencrypted CBS volume. This snapshot is also unencrypted.

2) Copy the snapshot while applying encryption parameters. The resulting target snapshot is encrypted.

3) Restore the encrypted snapshot to a new volume, which is also encrypted.

For more information on EBS Encryption, please refer to the below document link: from AWS

http://docs.aws.a mazon.com/AWSEC2/latest/UserGuide/ EBSEncryption.html