DOP-C02 Q&As

AWS Certified DevOps Engineer - Professional

Pass Amazon DOP-C02 Exam with 100% Guarantee

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

https://www.pass4itsure.com/dop-c02.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 company\\'s application uses a fleet of Amazon EC2 On-Demand Instances to analyze and process data. The EC2 instances are in an Auto Scaling group. The Auto Scaling group is a target group for an Application Load Balancer (ALB).

The application analyzes critical data that cannot tolerate interruption. The application also analyzes noncritical data that can withstand interruption.

The critical data analysis requires quick scalability in response to real-time application demand. The noncritical data analysis involves memory consumption. A DevOps engineer must implement a solution that reduces scale-out latency for the

critical data. The solution also must process the noncritical data.

Which combination of steps will meet these requirements? (Select TWO.)

A. For the critical data, modify the existing Auto Scaling group. Create a warm pool instance in the stopped state. Define the warm pool size. Create a new version of the launch template that has detailed monitoring enabled. use Spot Instances.

B. For the critical data, modify the existing Auto Scaling group. Create a warm pool instance in the stopped state. Define the warm pool size. Create a new version of the launch template that has detailed monitoring enabled. Use On-Demand Instances.

C. For the critical data. modify the existing Auto Scaling group. Create a lifecycle hook to ensure that bootstrap scripts are completed successfully. Ensure that the application on the instances is ready to accept traffic before the instances are registered. Create a new version of the launch template that has detailed monitoring enabled.

D. For the noncritical data, create a second Auto Scaling group that uses a launch template. Configure the launch template to install the unified Amazon CloudWatch agent and to configure the CloudWatch agent with a custom memory utilization metric. Use Spot Instances. Add the new Auto Scaling group as the target group for the ALB. Modify the application to use two target groups for critical data and noncritical data.

E. For the noncritical data, create a second Auto Scaling group. Choose the predefined memory utilization metric type for the target tracking scaling policy. Use Spot Instances. Add the new Auto Scaling group as the target group for the ALB. Modify the application to use two target groups for critical data and noncritical data.

Correct Answer: BD

For the critical data, using a warm pool1 can reduce the scale-out latency by having pre-initialized EC2 instances ready to serve the application traffic. Using On-Demand Instances can ensure that the instances are always available and not

interrupted by Spot interruptions2.

For the noncritical data, using a second Auto Scaling group with Spot Instances can reduce the cost and leverage the unused capacity of EC23. Using a launch template with the CloudWatch agent4 can enable the collection of memory

utilization metrics, which can be used to scale the group based on the memory demand. Adding the second group as a target group for the ALB and modifying the application to use two target groups can enable routing the traffic based on the

data type.

References:

1: Warm pools for Amazon EC2 Auto Scaling

2: Amazon EC2 On-Demand Capacity Reservations

3: Amazon EC2 Spot Instances

4: Metrics collected by the CloudWatch agent

QUESTION 2

A company uses AWS Key Management Service (AWS KMS) keys and manual key rotation to meet regulatory compliance requirements. The security team wants to be notified when any keys have not been rotated after 90 days.

Which solution will accomplish this?

A. Configure AWS KMS to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

B. Configure an Amazon EventBridge event to launch an AWS Lambda function to call the AWS Trusted Advisor API and publish to an Amazon Simple Notification Service (Amazon SNS) topic.

C. Develop an AWS Config custom rule that publishes to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

D. Configure AWS Security Hub to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

Correct Answer: C

https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-determine-compliance-of-aws-kms-key-policies-to-your-specifications/

QUESTION 3

A company manages a multi-tenant environment in its VPC and has configured Amazon GuardDuty for the corresponding AWS account. The company sends all GuardDuty findings to AWS Security Hub.

Traffic from suspicious sources is generating a large number of findings. A DevOps engineer needs to implement a solution to automatically deny traffic across the entire VPC when GuardDuty discovers a new suspicious source.

Which solution will meet these requirements?

A. Create a GuardDuty threat list. Configure GuardDuty to reference the list. Create an AWS Lambda function that will update the threat list. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.

B. Configure an AWS WAF web ACL that includes a custom rule group. Create an AWS Lambda function that will create a block rule in the custom rule group. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.

C. Configure a firewall in AWS Network Firewall. Create an AWS Lambda function that will create a Drop action rule in the firewall policy. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.

D. Create an AWS Lambda function that will create a GuardDuty suppression rule. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.

Correct Answer: C

https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-amazon-guardduty/

QUESTION 4

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 falls, 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.

Witch combination of actions should be taken to meet these requirements? (Choose two.)

A. Change the deployment configuration to CodeDeployDefaultAllAtOnce 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 it the health checks performed by the script are not successful.

Correct Answer: AC

QUESTION 5

Consider the portion of a CloudTrail log file below. Which type of event is being captured?

"eventTime":"2016-07-16T17:35:32Z",

"eventSource":"signin.amazonaws.com",

"eventName":"ConsoleLogin",

"awsRegion":"us-west-1",

"sourceIPAddress":"192.1.2.10",

...

A. AWS console sign-in

B. AWS log off

C. AWS error

D. AWS deployment

Correct Answer: A

CloudTrail records attempts to sign into the AWS Management Console, the AWS Discussion Forums and the AWS Support Center. Note, however, that CloudTrail does not record root sign-in failures.

Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-awsconsole-sign-in-events.html