Exam Amazon DOP-C02 Experience & DOP-C02 Latest Study Materials

What's more, part of that 2Pass4sure DOP-C02 dumps now are free: https://drive.google.com/open?id=11FJVOAeEc4MRDhSwKqNjZy_g657vuOhk

2Pass4sure You can modify settings of practice test in terms of DOP-C02 practice questions types and mock exam duration. Both DOP-C02 exam practice tests (web-based and desktop) save your every attempt and present result of the attempt on the spot. Actual exam environments of web-based and desktop Amazon DOP-C02 Practice Test help you overcome exam fear.

Amazon DOP-C02 (AWS Certified DevOps Engineer - Professional) Certification Exam is a highly sought-after certification for those looking to establish themselves in the field of DevOps engineering. AWS Certified DevOps Engineer - Professional certification is designed to test the skills and knowledge necessary for professionals to manage and operate distributed application systems using AWS tools and services.

>> Exam Amazon DOP-C02 Experience <<

DOP-C02 Latest Study Materials | DOP-C02 Pdf Files

New AWS Certified DevOps Engineer - Professional DOP-C02 study guide and latest learning materials and practice materials have been provide for customers. 2Pass4sure is a good platform that has been providing reliable, true, updated, and free AWS Certified DevOps Engineer - Professional DOP-C02 Exam Questions. The AWS Certified DevOps Engineer - Professional DOP-C02 exam fee is affordable, in order to success in your career, you need to pass AWS Certified DevOps Engineer - Professional exam.

Amazon AWS Certified DevOps Engineer - Professional Sample Questions (Q131-Q136):

NEW QUESTION # 131
A company deploys a web application on Amazon EC2 instances that are behind an Application Load Balancer (ALB). The company stores the application code in an AWS CodeCommit repository. When code is merged to the main branch, an AWS Lambda function invokes an AWS CodeBuild project. The CodeBuild project packages the code, stores the packaged code in AWS CodeArtifact, and invokes AWS Systems Manager Run Command to deploy the packaged code to the EC2 instances. Previous deployments have resulted in defects, EC2 instances that are not running the latest version of the packaged code, and inconsistencies between instances.
Which combination of actions should a DevOps engineer take to implement a more reliable deployment solution? (Select TWO.)

- A. Create an AWS CodeDeploy application and a deployment group to deploy the packaged code to the EC2 instances. Configure the ALB for the deployment group.
- B. Create a pipeline in AWS CodePipeline that uses the CodeCommit repository as a source provider.
  Create separate pipeline stages that run a CodeBuild project to build and then test the application. In the pipeline, pass the CodeBuild project output artifact to an AWS CodeDeploy action.
- C. Create individual Lambda functions that use AWS CodeDeploy instead of Systems Manager to run build, test, and deploy

actions.

- D. Create an Amazon S3 bucket. Modify the CodeBuild project to store the packages in the S3 bucket instead of in CodeArtifact. Use deploy actions in CodeDeploy to deploy the artifact to the EC2 instances.
- E. Create a pipeline in AWS CodePipeline that uses the CodeCommit repository as a source provider. Configure pipeline stages that run the CodeBuild project in parallel to build and test the application. In the pipeline, pass the CodeBuild project output artifact to an AWS CodeDeploy action.

Answer: A,E

Explanation:
Explanation
To implement a more reliable deployment solution, a DevOps engineer should take the following actions:
* Create a pipeline in AWS CodePipeline that uses the CodeCommit repository as a source provider.
Configure pipeline stages that run the CodeBuild project in parallel to build and test the application. In the pipeline, pass the CodeBuild project output artifact to an AWS CodeDeploy action. This action will improve the deployment reliability by automating the entire process from code commit to deployment, reducing human errors and inconsistencies. By running the build and test stages in parallel, the pipeline can also speed up the delivery time and provide faster feedback. By using CodeDeploy as the deployment action, the pipeline can leverage the features of CodeDeploy, such as traffic shifting, health checks, rollback, and deployment configuration123
* Create an AWS CodeDeploy application and a deployment group to deploy the packaged code to the EC2 instances. Configure the ALB for the deployment group. This action will improve the deployment reliability by using CodeDeploy to orchestrate the deployment across multiple EC2 instances behind an ALB. CodeDeploy can perform blue/green deployments or in-place deployments with traffic shifting, which can minimize downtime and reduce risks. CodeDeploy can also monitor the health of the instances during and after the deployment, and automatically roll back if any issues are detected. By configuring the ALB for the deployment group, CodeDeploy can register and deregister instances from the load balancer as needed, ensuring that only healthy instances receive traffic45 The other options are not correct because they do not improve the deployment reliability or follow best practices. Creating separate pipeline stages that run a CodeBuild project to build and then test the application is not a good option because it will increase the pipeline execution time and delay the feedback loop. Creating individual Lambda functions that use CodeDeploy instead of Systems Manager to run build, test, and deploy actions is not a valid option because it will add unnecessary complexity and cost to the solution. Lambda functions are not designed for long-running tasks such as building or deploying applications. Creating an Amazon S3 bucket and modifying the CodeBuild project to store the packages in the S3 bucket instead of in CodeArtifact is not a necessary option because it will not affect the deployment reliability. CodeArtifact is a secure, scalable, and cost-effective package management service that can store and share software packages for application development67 References:
* 1: What is AWS CodePipeline? - AWS CodePipeline
* 2: Create a pipeline in AWS CodePipeline - AWS CodePipeline
* 3: Deploy an application with AWS CodeDeploy - AWS CodePipeline
* 4: What is AWS CodeDeploy? - AWS CodeDeploy
* 5: Configure an Application Load Balancer for your blue/green deployments - AWS CodeDeploy
* 6: What is AWS Lambda? - AWS Lambda
* 7: What is AWS CodeArtifact? - AWS CodeArtifact

NEW QUESTION # 132
A company needs a strategy for failover and disaster recovery of its data and application. The application uses a MySQL database and Amazon EC2 instances. The company requires a maximum RPO of 2 hours and a maximum RTO of 10 minutes for its data and application at all times.
Which combination of deployment strategies will meet these requirements? (Select TWO.)

- A. Set up the application in two AWS Regions. Configure AWS Global Accelerator to point to Application Load Balancers (ALBs) in both Regions. Add both ALBs to a single endpoint group. Use health checks and Auto Scaling groups in each Region.
- B. Create an Amazon Aurora global database in two AWS Regions as the data store. In the event of a failure, promote the secondary Region to the primary for the application. Update the application to use the Aurora cluster endpoint in the secondary Region.
- C. Set up the application in two AWS Regions. Use Amazon Route 53 failover routing that points to Application Load Balancers in both Regions. Use health checks and Auto Scaling groups in each Region.
- D. Create an Amazon Aurora cluster in multiple AWS Regions as the data store. Use a Network Load Balancer to balance the database traffic in different Regions.
- E. Create an Amazon Aurora Single-AZ cluster in multiple AWS Regions as the data store. Use Aurora's automatic recovery capabilities in the event of a disaster.

Answer: A,B

Explanation:
To meet the requirements of failover and disaster recovery, the company should use the following deployment strategies:
Create an Amazon Aurora global database in two AWS Regions as the data store. In the event of a failure, promote the secondary Region to the primary for the application. Update the application to use the Aurora cluster endpoint in the secondary Region. This strategy can provide a low RPO and RTO for the data, as Aurora global database replicates data with minimal latency across Regions and allows fast and easy failover12. The company can use the Amazon Aurora cluster endpoint to connect to the current primary DB cluster without needing to change any application code1.
Set up the application in two AWS Regions. Configure AWS Global Accelerator to point to Application Load Balancers (ALBs) in both Regions. Add both ALBs to a single endpoint group. Use health checks and Auto Scaling groups in each Region. This strategy can provide high availability and performance for the application, as AWS Global Accelerator uses the AWS global network to route traffic to the closest healthy endpoint3. The company can also use static IP addresses that are assigned by Global Accelerator as a fixed entry point for their application1. By using health checks and Auto Scaling groups, the company can ensure that their application can scale up or down based on demand and handle any instance failures4.
The other options are incorrect because:
Creating an Amazon Aurora Single-AZ cluster in multiple AWS Regions as the data store would not provide a fast failover or disaster recovery solution, as the company would need to manually restore data from backups or snapshots in another Region in case of a failure.
Creating an Amazon Aurora cluster in multiple AWS Regions as the data store and using a Network Load Balancer to balance the database traffic in different Regions would not work, as Network Load Balancers do not support cross-Region routing. Moreover, this strategy would not provide a consistent view of the data across Regions, as Aurora clusters do not replicate data automatically between Regions unless they are part of a global database.
Setting up the application in two AWS Regions and using Amazon Route 53 failover routing that points to Application Load Balancers in both Regions would not provide a low RTO, as Route 53 failover routing relies on DNS resolution, which can take time to propagate changes across different DNS servers and clients.
Moreover, this strategy would not provide deterministic routing, as Route 53 failover routing depends on DNS caching behavior, which can vary depending on different factors.

NEW QUESTION # 133
An ecommerce company is receiving reports that its order history page is experiencing delays in reflecting the processing status of orders. The order processing system consists of an AWS Lambda function that uses reserved concurrency. The Lambda function processes order messages from an Amazon Simple Queue Service (Amazon SQS) queue and inserts processed orders into an Amazon DynamoDB table. The DynamoDB table has auto scaling enabled for read and write capacity.
Which actions should a DevOps engineer take to resolve this delay? (Choose two.)

- A. Check the Throttles metric for the Lambda function. Increase the Lambda function timeout.
- B. Check the WriteThrottleEvents metric for the DynamoDB table. Increase the maximum write capacity units (WCUs) for the table's scaling policy.
- C. Check the NumberOfMessagesSent metric for the SQS queue. Increase the SQS queue visibility timeout.
- D. Check the ApproximateAgeOfOldestMessage metnc for the SQS queue Configure a redrive policy on the SQS queue.
- E. Check the ApproximateAgeOfOldestMessage metric for the SQS queue. Increase the Lambda function concurrency limit.

Answer: B,E

NEW QUESTION # 134
A DevOps engineer must implement a solution that immediately terminates Amazon EC2 instances in Auto Scaling groups when cryptocurrency mining activity is detected.
Which solution will meet these requirements with the LEAST development effort?

- A. Configure Amazon Route 53 to send query logs directly to Amazon CloudWatch Logs. Create an AWS Lambda function that runs every 5 minutes and checks the query logs for domains related to cryptocurrency activity. If the domains are found, terminate the identified EC2 instances.
- B. Configure VPC Flow Logs to send flow logs to an Amazon S3 bucket. Create an AWS Lambda function that runs every 5 minutes and invokes an Amazon Athena query to find IP addresses associated with cryptocurrency activity. If the IP addresses are found, terminate the identified EC2 instances.
- C. Enable Amazon GuardDuty. Monitor EC2 findings. Create an Amazon EventBridge rule with GuardDuty as the event source. Create an AWS Lambda function that is triggered by the EventBridge rule. Configure the Lambda function to parse

the event and terminate the identified EC2 instances.

- D. Enable AWS Security Hub. Monitor EC2 findings. Create an Amazon EventBridge rule with Security Hub as the event source. Create an AWS Lambda function that is triggered by the EventBridge rule.Configure the Lambda function to parse the event and terminate the identified EC2 instances.

Answer: C

Explanation:
The requirement is to immediately detect and terminate EC2 instances involved in cryptocurrency mining with the least development effort. Amazon GuardDuty is the AWS-native service specifically designed to detect malicious activities such as crypto-mining by continuously analyzing CloudTrail events, VPC Flow Logs, and DNS logs. GuardDuty includes managed threat intelligence and predefined findings like CryptoCurrency:EC2/BitcoinTool.B!DNS and CryptoCurrency:EC2/BitcoinTool.B!IP, which directly identify mining behavior without custom detection logic.
Option C leverages this built-in capability. Once GuardDuty is enabled, findings are automatically generated when mining activity is detected. These findings are sent to Amazon EventBridge in near real time. An EventBridge rule can filter for cryptocurrency-related findings and trigger an AWS Lambda function. The Lambda function can then identify the affected EC2 instance and terminate it or adjust the Auto Scaling group to replace it. This approach requires minimal custom code and no log parsing, scheduled jobs, or analytics pipelines.
Options A and B rely on custom log analysis, periodic execution, and maintaining lists of mining domains or IPs, which significantly increases complexity and response time. Option D uses AWS Security Hub, which aggregates findings from GuardDuty and other services but is not intended for immediate, low-latency remediation.
Therefore, Option C provides the fastest detection, immediate response, and lowest development overhead using AWS-managed threat detection services.

NEW QUESTION # 135
A company is developing a new application. The application uses AWS Lambda functions for its compute tier. The company must use a canary deployment for any changes to the Lambda functions. Automated rollback must occur if any failures are reported.
The company's DevOps team needs to create the infrastructure as code (IaC) and the CI/CD pipeline for this solution.
Which combination of steps will meet these requirements? (Choose three.)

- A. Create an Amazon CloudWatch composite alarm for all the Lambda functions. Configure an evaluation period and dimensions for Lambda. Configure the alarm to enter the ALARM state if any errors are detected or if there is insufficient data.
- B. Create an AWS CodeCommit repository. Create an AWS CodePipeline pipeline. Use the CodeCommit repository in a new source stage that starts the pipeline. Create an AWS CodeDeploy deployment group that is configured for canary deployments with a DeploymentPreference type of Canary10Percent10Minutes. Upload the AWS CloudFormation template and source code to the CodeCommit repository. In the CodeCommit repository, create an appspec.yml file that includes the commands to deploy the CloudFormation template.
- C. Create an Amazon CloudWatch alarm for each Lambda function. Configure the alarms to enter the ALARM state if any errors are detected. Configure an evaluation period, dimensions for each Lambda function and version, and the namespace as AWS/Lambda on the Errors metric.
- D. Create an AWS CloudFormation template for the application. Define each Lambda function in the template by using the AWS::Lambda::Function resource type. In the template, include a version for the Lambda function by using the AWS::Lambda::Version resource type. Declare the CodeSha256 property. Configure an AWS::Lambda::Alias resource that references the latest version of the Lambda function.
- E. Create an AWS Serverless Application Model (AWS SAM) template for the application. Define each Lambda function in the template by using the AWS::Serverless::Function resource type. For each function, include configurations for the AutoPublishAlias property and the DeploymentPreference property. Configure the deployment configuration type to LambdaCanary10Percent10Minutes.
- F. Create an AWS CodeCommit repository. Create an AWS CodePipeline pipeline. Use the CodeCommit repository in a new source stage that starts the pipeline. Create an AWS CodeBuild project to deploy the AWS Serverless Application Model (AWS SAM) template. Upload the template and source code to the CodeCommit repository. In the CodeCommit repository, create a buildspec.yml file that includes the commands to build and deploy the SAM application.

Answer: C,E,F

Explanation:
The requirement is to create the infrastructure as code (IaC) and the CI/CD pipeline for the Lambda application that uses canary deployment and automated rollback. To do this, the DevOps team needs to use the following steps:
Create an AWS Serverless Application Model (AWS SAM) template for the application. AWS SAM is a framework that simplifies

the development and deployment of serverless applications on AWS. AWS SAM allows customers to define Lambda functions and other resources in a template by using a simplified syntax.
For each Lambda function, the DevOps team can include configurations for the AutoPublishAlias property and the DeploymentPreference property. The AutoPublishAlias property specifies the name of the alias that points to the latest version of the function. The DeploymentPreference property specifies how CodeDeploy deploys new versions of the function. By configuring the deployment configuration type to LambdaCanary10Percent10Minutes, the DevOps team can enable canary deployment with 10% of traffic shifted to the new version every 10 minutes.
Create an AWS CodeCommit repository. Create an AWS CodePipeline pipeline. Use the CodeCommit repository in a new source stage that starts the pipeline. Create an AWS CodeBuild project to deploy the AWS SAM template. CodeCommit is a fully managed source control service that hosts Git repositories.
CodePipeline is a fully managed continuous delivery service that automates the release process of software applications. CodeBuild is a fully managed continuous integration service that compiles source code and runs tests. By using these services, the DevOps team can create a CI/CD pipeline for the Lambda application. The pipeline should use the CodeCommit repository as the source stage, where the DevOps team can upload the SAM template and source code. The pipeline should also use a CodeBuild project as the build stage, where the SAM template can be built and deployed.
Create an Amazon CloudWatch alarm for each Lambda function. Configure the alarms to enter the ALARM state if any errors are detected. Configure an evaluation period, dimensions for each Lambda function and version, and the namespace as AWS/Lambda on the Errors metric. CloudWatch is a service that monitors and collects metrics from AWS resources and applications.
CloudWatch alarms are actions that are triggered when a metric crosses a specified threshold. By creating CloudWatch alarms for each Lambda function, the DevOps team can monitor the health and performance of each function version during deployment. By configuring the alarms to enter the ALARM state if any errors are detected, the DevOps team can enable automated rollback if any failures are reported.

NEW QUESTION # 136
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New DOP-C02 dumps are available on Google Drive shared by 2Pass4sure: https://drive.google.com/open?id=11FJVOAeEc4MRDhSwKqNjZy_g657vuOhk