Amazon DOP-C02対応一発合格

さらに、JPTestKing DOP-C02ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1lL59WqhzG3v9N4SilwYMuoRcHd0YN-1H

JPTestKingを通してAmazon DOP-C02試験に合格することがやすくて、Amazon DOP-C02試験をはじめて受ける方はJPTestKingの商品を選んで無料なサンプル（例年の試験問題集と解析）をダウンロードしてから、楽に試験の現場の雰囲気を体験することができます。オンラインにいろいろなAmazon DOP-C02試験集があるですけれども、弊社の商品は一番高品質で低価額で、試験の問題が絶えず切れない更新でテストの内容ともっとも真実と近づいてお客様の合格が保証いたします。それほかに、弊社の商品を選んで、勉強の時間も長くではありません。できるだけ早くAmazon DOP-C02認定試験「AWS Certified DevOps Engineer - Professional」を通ろう。

AWS認定DevOpsエンジニア - プロフェッショナル試験は、継続的な統合と配信、コードとしてのインフラストラクチャ、監視、ロギングなど、DevOpsに関連するさまざまな分野で候補者の知識とスキルをテストするように設計されています。この試験では、複数の選択と複数の反応の質問、および候補者が実際の状況に知識を適用する必要があるシナリオベースの質問で構成されています。試験の長さは180分で、費用は300ドルです。

Amazon DOP-C02認定試験では、構成管理、監視とロギング、継続的な統合と配信、セキュリティとコンプライアンス、インフラストラクチャなど、コードとしてのインフラストラクチャなど、さまざまなトピックをカバーしています。この認定の候補者は、DevOpsの原則と実践を使用してAWSサービスとシステムを設計、管理、および保守する能力についてテストされます。

>> DOP-C02テスト難易度 <<

DOP-C02試験の準備方法｜ユニークなDOP-C02テスト難易度試験｜更新するAWS Certified DevOps Engineer - Professional資格復習テキスト

我々JPTestKingは最も頼もしいアフターサービスを提供します。あなたはAmazonのDOP-C02問題集をご購入になってから、我々は一年間の無料更新サービスを提供します。その一年の間、我々の専門家たちは毎日DOP-C02問題集の更新を検査しています。もし更新されたら、すぐにお客様を知らせます。お客様の持っているのはずっと最新版のですから、安心でDOP-C02試験を準備することができます。

Amazon AWS Certified DevOps Engineer - Professional 認定 DOP-C02 試験問題 (Q287-Q292):

質問 # 287
A company uses Amazon EC2 as its primary compute platform. A DevOps team wants to audit the company's EC2 instances to check whether any prohibited applications have been installed on the EC2 instances.
Which solution will meet these requirements with the MOST operational efficiency?

- A. Configure AWS Systems Manager on each instance Use Systems Manager Inventory Create AWS Config rules that monitor changes from Systems Manager Inventory to identify prohibited applications.
- B. Configure AWS Systems Manager on each instance. Use Systems Manager Inventory. Filter a trail in AWS CloudTrail for Systems Manager Inventory events to identify prohibited applications.
- C. Designate Amazon CloudWatch Logs as the log destination for all application instances Run an automated script across all

instances to create an inventory of installed applications Configure the script to forward the results to CloudWatch Logs Create a CloudWatch alarm that uses filter patterns to search log data to identify prohibited applications.

- D. Configure AWS Systems Manager on each instance Use AWS Systems Manager Inventory Use Systems Manager resource data sync to synchronize and store findings in an Amazon S3 bucket Create an AWS Lambda function that runs when new objects are added to the S3 bucket. Configure the Lambda function to identify prohibited applications.

正解：D

解説：
Configure AWS Systems Manager on Each Instance:
AWS Systems Manager provides a unified interface for managing AWS resources. Install the Systems Manager agent on each EC2 instance to enable inventory management and other features.
Use AWS Systems Manager Inventory:
Systems Manager Inventory collects metadata about your instances and the software installed on them. This data includes information about applications, network configurations, and more.
Enable Systems Manager Inventory on all EC2 instances to gather detailed information about installed applications.
Use Systems Manager Resource Data Sync to Synchronize and Store Findings in an Amazon S3 Bucket:
Resource Data Sync aggregates inventory data from multiple accounts and regions into a single S3 bucket, making it easier to query and analyze the data.
Configure Resource Data Sync to automatically transfer inventory data to an S3 bucket for centralized storage.
Create an AWS Lambda Function that Runs When New Objects are Added to the S3 Bucket:
Use an S3 event to trigger a Lambda function whenever new inventory data is added to the S3 bucket.
The Lambda function can parse the inventory data and check for the presence of prohibited applications.
Configure the Lambda Function to Identify Prohibited Applications:
The Lambda function should be programmed to scan the inventory data for any known prohibited applications and generate alerts or take appropriate actions if such applications are found.
Example Lambda function in Python
import json
import boto3
def lambda_handler(event, context):
s3 = boto3.client('s3')
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
response = s3.get_object(Bucket=bucket, Key=key)
inventory_data = json.loads(response['Body'].read().decode('utf-8'))
prohibited_apps = ['app1', 'app2']
for instance in inventory_data['Instances']:
for app in instance['Applications']:
if app['Name'] in prohibited_apps:
# Send notification or take action
print(f"Prohibited application found: {app['Name']} on instance {instance['InstanceId']}") return {'statusCode': 200, 'body': json.dumps('Check completed')} By leveraging AWS Systems Manager Inventory, Resource Data Sync, and Lambda, this solution provides an efficient and automated way to audit EC2 instances for prohibited applications.
References:
AWS Systems Manager Inventory
AWS Systems Manager Resource Data Sync
S3 Event Notifications
AWS Lambda

質問 # 288
A company is using an AWS CodeBuild project to build and package an application. The packages are copied to a shared Amazon S3 bucket before being deployed across multiple AWS accounts.
The buildspec.yml file contains the following:

```
version: 0.2
phases:
  build:
    commands:
      - go build -o myapp
  post_build:
    commands:
      - aws s3 cp --acl authenticated-read myapp s3://artifacts/
```


The DevOps engineer has noticed that anybody with an AWS account is able to download the artifacts.
What steps should the DevOps engineer take to stop this?

- A. Create an S3 bucket policy that grants read access to the relevant AWS accounts and denies read access to the principal "*".
- B. Modify the post_build command to use --acl public-read and configure a bucket policy that grants read access to the relevant AWS accounts only.
- C. Modify the post_build command to remove --acl authenticated-read and configure a bucket policy that allows read access to the relevant AWS accounts only.
- D. Configure a default ACL for the S3 bucket that defines the set of authenticated users as the relevant AWS accounts only and grants read-only access.

正解：C

解説：
When setting the flag authenticated-read in the command line, the owner gets FULL_CONTROL. The AuthenticatedUsers group (Anyone with an AWS account) gets READ access. Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html

質問 # 289
A DevOps team uses AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy to deploy an application.
The application is a REST API that uses AWS Lambda functions and Amazon API Gateway Recent deployments have introduced errors that have affected many customers.
The DevOps team needs a solution that reverts to the most recent stable version of the application when an error is detected. The solution must affect the fewest customers possible.
Which solution Will meet these requirements With the MOST operational efficiency?

- A. Set the deployment configuration in CodeDepIoy to LambdaAllAtOnce Configure automatic rollbacks on the deployment group Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway Configure the deployment group to roll back when the number of alarms meets the alarm threshold
- B. Set the deployment configuration in CodeDeploy to LambdaCanaryIOPercentIOMinutes Configure manual rollbacks on the deployment group Create a metric filter on an Amazon CloudWatch log group for API Gateway to monitor HTTP Bad Gateway errors. Configure the metric filter to Invoke a new Lambda function that stops the current eployment and starts the most recent successful deployment
- C. Set the deployment configuration in CodeDeploy to LambdaCanary10Percent10Minutes. Configure automatic rollbacks on the deployment group Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway Configure the deployment group to roll back when the number of alarms meets the alarm threshold
- D. Set the deployment configuration in CodeDeploy to LambdaAllAtOnce Configure manual rollbacks on the deployment group. Create an Amazon Simple Notification Service (Amazon SNS) topc to send notifications every time a deployrnent fads. Configure the SNS topc to Invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment

正解：C

解説：
Option A is incorrect because setting the deployment configuration to LambdaAllAtOnce means that the new version of the application will be deployed to all Lambda functions at once, affecting all customers. This does not meet the requirement of affecting the fewest customers possible. Moreover, configuring automatic rollbacks on the deployment group is not operationally efficient, as it requires manual intervention to fix the errors and redeploy the application.
Option B is correct because setting the deployment configuration to LambdaCanary10Percent10Minutes means that the new version

of the application will be deployed to 10 percent of the Lambda functions first, and then to the remaining 90 percent after 10 minutes. This minimizes the impact of errors on customers, as only 10 percent of them will be affected by a faulty deployment. Configuring automatic rollbacks on the deployment group also meets the requirement of reverting to the most recent stable version of the application when an error is detected. Creating a CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway is a valid way to monitor the health of the application and trigger a rollback if needed.
Option C is incorrect because setting the deployment configuration to LambdaAllAtOnce means that the new version of the application will be deployed to all Lambda functions at once, affecting all customers. This does not meet the requirement of affecting the fewest customers possible. Moreover, configuring manual rollbacks on the deployment group is not operationally efficient, as it requires human intervention to stop the current deployment and start a new one. Creating an SNS topic to send notifications every time a deployment fails is not sufficient to detect errors in the application, as it does not monitor the API Gateway responses.
Option D is incorrect because configuring manual rollbacks on the deployment group is not operationally efficient, as it requires human intervention to stop the current deployment and start a new one. Creating a metric filter on a CloudWatch log group for API Gateway to monitor HTTP Bad Gateway errors is a valid way to monitor the health of the application, but invoking a new Lambda function to perform a rollback is unnecessary and complex, as CodeDeploy already provides automatic rollback functionality.
References:
AWS CodeDeploy Deployment Configurations
[AWS CodeDeploy Rollbacks]
Amazon CloudWatch Alarms

質問 # 290
A DevOps engineer is implementing governance controls for a company that requires its infrastructure to be housed within the United States. The engineer must restrict which AWS Regions can be used, and ensure an alert is sent as soon as possible if any activity outside the governance policy takes place. The controls should be automatically enabled on any new Region outside the United States (US).
Which combination of actions will meet these requirements? (Select TWO.)

- A. Use an AWS Lambda function that checks for AWS service activity and deploy it to all Regions. Write an Amazon EventBridge rule that runs the Lambda function every hour, sending an alert if activity is found in a non-US Region.
- B. Write an SCP using the aws: RequestedRegion condition key limiting access to US Regions. Apply the policy to all users, groups, and roles
- C. Create an AWS Organizations SCP that denies access to all non-global services in non-US Regions. Attach the policy to the root of the organization.
- D. Use an AWS Lambda function to query Amazon Inspector to look for service activity in non-US Regions and send alerts if any activity is found.
- E. Configure AWS CloudTrail to send logs to Amazon CloudWatch Logs and enable it for all Regions. Use a CloudWatch Logs metric filter to send an alert on any service activity in non-US Regions.

正解：C、E

解説：
To implement governance controls that restrict AWS service usage to within the United States and ensure alerts for any activity outside the governance policy, the following actions will meet the requirements:
A). Create an AWS Organizations SCP that denies access to all non-global services in non-US Regions. Attach the policy to the root of the organization. This action will effectively prevent users and roles in all accounts within the organization from accessing services in non-US Regions12.
B). Configure AWS CloudTrail to send logs to Amazon CloudWatch Logs and enable it for all Regions. Use a CloudWatch Logs metric filter to send an alert on any service activity in non-US Regions. This action will allow monitoring of all AWS Regions and will trigger alerts if any activity is detected in non-US Regions, ensuring that the governance team is notified as soon as possible3.
AWS Documentation on Service Control Policies (SCPs) and how they can be used to manage permissions and restrict access based on Regions12.
AWS Documentation on monitoring CloudTrail log files with Amazon CloudWatch Logs to set up alerts for specific activities3.

質問 # 291
A company is using AWS CodePipeline to deploy an application. According to a new guideline, a member of the company's security team must sign off on any application changes before the changes are deployed into production. The approval must be recorded and retained.
Which combination of actions will meet these requirements? (Select TWO.)

- A. Create an AWS CloudTrail trail to deliver logs to Amazon S3.
- B. Configure CodePipeline to write actions to an Amazon S3 bucket at the end of each pipeline stage.
- C. Configure CodePipeline to write actions to Amazon CloudWatch Logs.
- D. Create a CodePipeline manual approval action before the deployment step. Create a policy that grants the security team access to approve manual approval stages.
- E. Create a CodePipeline custom action to invoke an AWS Lambda function for approval. Create a policy that gives the security team access to manage CodePipeline custom actions.

正解：A、D

解説：
To meet the new guideline for application deployment, the company can use a combination of AWS CodePipeline and AWS CloudTrail. A manual approval action in CodePipeline allows the security team to review and approve changes before they are deployed. This action can be configured to pause the pipeline until approval is granted, ensuring that no changes move to production without the necessary sign-off. Additionally, by creating an AWS CloudTrail trail, all actions taken within CodePipeline, including approvals, are recorded and delivered to an Amazon S3 bucket. This provides an audit trail that can be retained for compliance and review purposes.
Reference:
AWS CodePipeline's manual approval action provides a way to ensure that a member of the security team can review and approve changes before they are deployed1.
AWS CloudTrail integration with CodePipeline allows for the recording and retention of all pipeline actions, including approvals, which can be stored in Amazon S3 for record-keeping2.

質問 # 292
.....

□ ウェブサイト☀ jp.fast2test.com □☀□を開き、➥ DOP-C02 □を検索して無料でダウンロードしてください DOP-C02受験記対策

- bbs.t-firefly.com, www.stes.tyc.edu.tw, pixabay.com, www.stes.tyc.edu.tw, www.connectantigua.com, recordtycoon.com, pastebin.com, bbs.t-firefly.com, 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, bbs.t-firefly.com, Disposable vapes

さらに、JPTestKing DOP-C02ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1lL59WqhzG3v9N4SilwYMuoRcHd0YN-1H