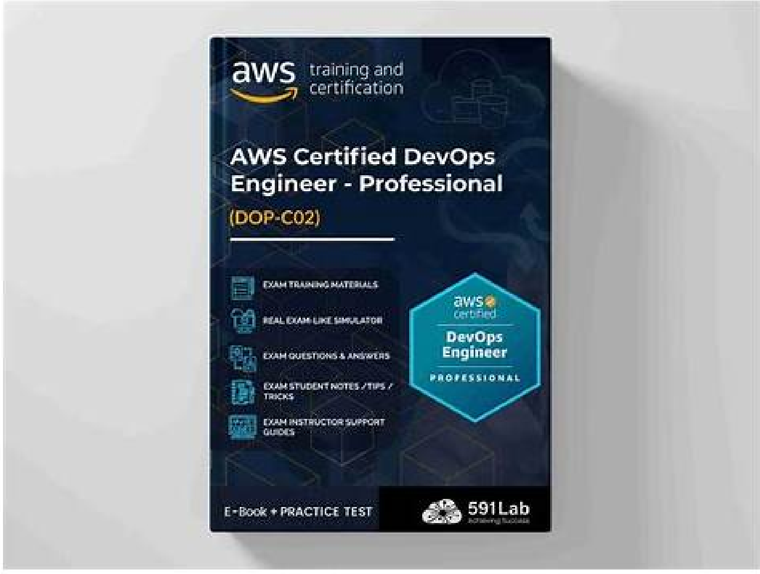
DOP-C02 Valid Exam Vce & DOP-C02 Test Dates



P.S. Free & New DOP-C02 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1E4asUpEdoNRuD9FWerVRlrBUbklDZHtg

You can get help from DumpTorrent Amazon DOP-C02 exam questions and easily pass get success in the Amazon DOP-C02 exam. The DOP-C02 practice exams are real, valid, and updated that are specifically designed to speed up DOP-C02 Exam Preparation and enable you to crack the AWS Certified DevOps Engineer - Professional (DOP-C02) exam successfully.

Amazon DOP-C02 Certification can help professionals advance their careers in the field of DevOps engineering and demonstrate their expertise in managing and operating distributed application systems using AWS tools and services. With the increasing demand for skilled DevOps engineers, earning this certification can open up new career opportunities and increase earning potential.

>> DOP-C02 Valid Exam Vce <<

Hot DOP-C02 Valid Exam Vce | Efficient DOP-C02 Test Dates: AWS Certified DevOps Engineer - Professional

In DumpTorrent's website you can free download study guide, some exercises and answers about Amazon Certification DOP-C02 Exam as an attempt.

Amazon DOP-C02 exam consists of 75 multiple-choice and multiple-response questions, and the exam duration is 180 minutes. DOP-C02 exam fee is $300, and it can be taken at a testing center or online with a remote proctor. DOP-C02 exam covers various topics, such as designing and managing continuous delivery systems, monitoring and logging systems, implementing and managing security and compliance, and troubleshooting issues. Passing DOP-C02 Exam demonstrates that an individual has the knowledge and skills to design, deploy, and manage highly available, scalable, and fault-tolerant systems on AWS.

Amazon AWS Certified DevOps Engineer - Professional Sample Questions (Q390-Q395):

NEW QUESTION # 390
A company is launching an application. The application must use only approved AWS services. The account that runs the application was created less than 1 year ago and is assigned to an AWS Organizations OU.
The company needs to create a new Organizations account structure. The account structure must have an appropriate SCP that supports the use of only services that are currently active in the AWS account.
The company will use AWS Identity and Access Management (IAM) Access Analyzer in the solution.
Which solution will meet these requirements?

- A. Create an SCP that allows the services that IAM Access Analyzer identifies. Create an OU for the account. Move the

account into the new OU. Attach the new SCP to the new OU. Detach the default FullAWSAccess SCP from the new OU.
- B. Create an SCP that allows the services that IAM Access Analyzer identifies. Attach the new SCP to the organization's root.
- C. Create an SCP that allows the services that IAM Access Analyzer identifies. Create an OU for the account. Move the account into the new OU. Attach the new SCP to the management account. Detach the default FullAWSAccess SCP from the new OU.
- D. Create an SCP that denies the services that IAM Access Analyzer identifies. Create an OU for the account. Move the account into the new OIJ. Attach the new SCP to the new OU.

Answer: A

Explanation:
To meet the requirements of creating a new Organizations account structure with an appropriate SCP that supports the use of only services that are currently active in the AWS account, the company should use the following solution:
Create an SCP that allows the services that IAM Access Analyzer identifies. IAM Access Analyzer is a service that helps identify potential resource-access risks by analyzing resource-based policies in the AWS environment. IAM Access Analyzer can also generate IAM policies based on access activity in the AWS CloudTrail logs. By using IAM Access Analyzer, the company can create an SCP that grants only the permissions that are required for the application to run, and denies all other services. This way, the company can enforce the use of only approved AWS services and reduce the risk of unauthorized access12 Create an OU for the account. Move the account into the new OU. An OU is a container for accounts within an organization that enables you to group accounts that have similar business or security requirements. By creating an OU for the account, the company can apply policies and manage settings for the account as a group. The company should move the account into the new OU to make it subject to the policies attached to the OU3 Attach the new SCP to the new OU. Detach the default FullAWSAccess SCP from the new OU. An SCP is a type of policy that specifies the maximum permissions for an organization or organizational unit (OU). By attaching the new SCP to the new OU, the company can restrict the services that are available to all accounts in that OU, including the account that runs the application. The company should also detach the default FullAWSAccess SCP from the new OU, because this policy allows all actions on all AWS services and might override or conflict with the new SCP45 The other options are not correct because they do not meet the requirements or follow best practices. Creating an SCP that denies the services that IAM Access Analyzer identifies is not a good option because it might not cover all possible services that are not approved or required for the application. A deny policy is also more difficult to maintain and update than an allow policy. Creating an SCP that allows the services that IAM Access Analyzer identifies and attaching it to the organization's root is not a good option because it might affect other accounts and OUs in the organization that have different service requirements or approvals.
Creating an SCP that allows the services that IAM Access Analyzer identifies and attaching it to the management account is not a valid option because SCPs cannot be attached directly to accounts, only to OUs or roots.
1: Using AWS Identity and Access Management Access Analyzer - AWS Identity and Access Management
2: Generate a policy based on access activity - AWS Identity and Access Management
3: Organizing your accounts into OUs - AWS Organizations
4: Service control policies - AWS Organizations
5: How SCPs work - AWS Organizations

NEW QUESTION # 391
An AWS CodePipeline pipeline has implemented a code release process. The pipeline is integrated with AWS CodeDeploy to deploy versions of an application to multiple Amazon EC2 instances for each CodePipeline stage.
During a recent deployment the pipeline failed due to a CodeDeploy issue. The DevOps team wants to improve monitoring and notifications during deployment to decrease resolution times.
What should the DevOps engineer do to create notifications. When issues are discovered?

- A. Implement Amazon EventBridge for CodePipeline and CodeDeploy create an Amazon. Inspector assessment target to evaluate code deployment issues and create an Amazon Simple. Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.
- B. Implement Amazon EventBridge for CodePipeline and CodeDeploy create an AWS Lambda function to evaluate code deployment issues, and create an Amazon Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.
- C. Implement Amazon CloudWatch Logs for CodePipeline and CodeDeploy create an AWS Config rule to evaluate code deployment issues, and create an Amazon Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.
- D. Implement AWS CloudTrail to record CodePipeline and CodeDeploy API call information create an AWS Lambda function to evaluate code deployment issues and create an Amazon Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.

Answer: B

Explanation:
Explanation
AWS CloudWatch Events can be used to monitor events across different AWS resources, and a CloudWatch Event Rule can be created to trigger an AWS Lambda function when a deployment issue is detected in the pipeline. The Lambda function can then evaluate the issue and send a notification to the appropriate stakeholders through an Amazon SNS topic. This approach allows for real-time notifications and faster resolution times.

NEW QUESTION # 392
A company wants to migrate its content sharing web application hosted on Amazon EC2 to a serverless architecture. The company currently deploys changes to its application by creating a new Auto Scaling group of EC2 instances and a new Elastic Load Balancer, and then shifting the traffic away using an Amazon Route
53 weighted routing policy.
For its new serverless application, the company is planning to use Amazon API Gateway and AWS Lambda.
The company will need to update its deployment processes to work with the new application. It will also need to retain the ability to test new features on a small number of users before rolling the features out to the entire user base.
Which deployment strategy will meet these requirements?

- A. Use AWS CDK to deploy API Gateway and Lambda functions. When code needs to be changed, update the AWS CloudFormation stack and deploy the new version of the APIs and Lambda functions. Use a Route 53 failover routing policy for the canary release strategy.
- B. Use AWS CloudFormation to deploy API Gateway and Lambda functions using Lambda function versions. When code needs to be changed, update the CloudFormation stack with the new Lambda code and update the API versions using a canary release strategy. Promote the new version when testing is complete.
- C. Use AWS Elastic Beanstalk to deploy API Gateway and Lambda functions. When code needs to be changed, deploy a new version of the API and Lambda functions. Shift traffic gradually using an Elastic Beanstalk blue/green deployment.
- D. Use AWS OpsWorks to deploy API Gateway in the service layer and Lambda functions in a custom layer. When code needs to be changed, use OpsWorks to perform a blue/green deployment and shift traffic gradually.

Answer: B

Explanation:
Explanation
https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverle

NEW QUESTION # 393
A company gives its employees limited rights to AWS DevOps engineers have the ability to assume an administrator role. For tracking purposes, the security team wants to receive a near-real-time notification when the administrator role is assumed.
How should this be accomplished?

- A. Create an Amazon EventBridge events rule using an AWS API call that uses an AWS CloudTrail event pattern to invoke an AWS Lambda function that publishes a message to an Amazon SNS topic if the administrator role is assumed.
- B. Configure AWS Config to publish logs to an Amazon S3 bucket Use Amazon Athena to query the logs and send a notification to the security team when the administrator role is assumed
- C. Configure Amazon GuardDuty to monitor when the administrator role is assumed and send a notification to the security team
- D. Create an Amazon EventBridge event rule using an AWS Management Console sign-in events event pattern that publishes a message to an Amazon SNS topic if the administrator role is assumed

Answer: A

Explanation:
Create an Amazon EventBridge Rule Using an AWS CloudTrail Event Pattern:
* AWS CloudTrail logs API calls made in your account, including actions performed by roles.
* Create an EventBridge rule that matches CloudTrail events where theAssumeRoleAPI call is made to assume the administrator role.
Invoke an AWS Lambda Function:
* Configure the EventBridge rule to trigger a Lambda function whenever the rule's conditions are met.

* The Lambda function will handle the logic to send a notification.
Publish a Message to an Amazon SNS Topic:
* The Lambda function will publish a message to an SNS topic to notify the security team.
* Subscribe the security team's email address to this SNS topic to receive real-time notifications.
Example EventBridge rule pattern:

```
{
"source": ["aws.cloudtrail"],
"detail-type": ["AWS API Call via CloudTrail"],
"detail": {
"eventSource": ["sts.amazonaws.com"],
"eventName": ["AssumeRole"],
"requestParameters": {
"roleArn": ["arn:aws:iam::<account-id>:role/AdministratorRole"]
}
}
}
```

Example Lambda function (Node.js) to publish to SNS:

```
const AWS = require('aws-sdk');
const sns = new AWS.SNS();
exports.handler = async (event) => {
const params = {
Message: `Administrator role assumed: ${JSON.stringify(event.detail)}`, TopicArn: 'arn:aws:sns:<region>:<account-id>:<sns-topic>'
};
await sns.publish(params).promise();
};
```

References:
* Creating EventBridge Rules
* Using AWS Lambda with Amazon SNS

NEW QUESTION # 394
A company has an application that runs on a fleet of Amazon EC2 instances. The application requires frequent restarts. The application logs contain error messages when a restart is required. The application logs are published to a log group in Amazon CloudWatch Logs.
An Amazon CloudWatch alarm notifies an application engineer through an Amazon Simple Notification Service (Amazon SNS) topic when the logs contain a large number of restart-related error messages. The application engineer manually restarts the application on the instances after the application engineer receives a notification from the SNS topic.
A DevOps engineer needs to implement a solution to automate the application restart on the instances without restarting the instances.
Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Lambda function that restarts the application on the instances. Configure the Lambda function as an event destination of the SNS topic.
- B. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Configure an Amazon EventBridge rule that reacts when the CloudWatch alarm enters ALARM state. Specify the runbook as a target of the rule.
- C. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Configure the SNS topic to invoke the runbook.
- D. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Create an AWS Lambda function to invoke the runbook. Configure the Lambda function as an event destination of the SNS topic.

Answer: B

Explanation:
This solution meets the requirements in the most operationally efficient manner by automating the application restart process on the instances without restarting them. When the CloudWatch alarm enters the ALARM state, the EventBridge rule is triggered, which in turn invokes the Systems Manager Automation runbook that contains the script to restart the application on the instances.

NEW QUESTION # 395
......

DOP-C02 Test Dates: https://www.dumptorrent.com/DOP-C02-braindumps-torrent.html