



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 development team uses AVMS Cloud Formation to deploy its application resources The team must use for an changes to the environment The team cannot use AWS Management Console or the AWS CLI to make manual changes directly.

The team uses a developer IAM role to access the environment The role is configured with the Admnistratoraccess managed policy. The company has created a new Cloudformationdeployment IAM role that has the following policy.

{ ersion": "2012-10-17" 'Statement": (Allow ACT1 lasticloadbalancing: ibda: "Resourc } 1 }

The company wants ensure that only CloudFormation can use the new role. The development team cannot make any manual changes to the deployed resources.

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

A. Remove the AdministratorAccess policy. Assign the ReadOnlyAccess managed IAM policy to the developer role. Instruct the developers to use the CloudFormationDeployment role as a CloudFormation service role when the developers deploy new stacks.

B. Update the trust of CloudFormationDeployment role to allow the developer IAM role to assume the CloudFormationDepoyment role.

C. Configure the IAM to be to get and pass the CloudFormationDeployment role if cloudformation actions for resources,

D. Update the trust Of the CloudFormationDepoyment role to anow the cloudformation.amazonaws.com AWS principal to perform the iam:AssumeR01e action

E. Remove me Administratoraccess policy. Assign the ReadOnly/Access managed IAM policy to the developer role Instruct the developers to assume the CloudFormatondeployment role when the developers new stacks

F. Add an IAM policy to CloudFormationDeplyment to allow cloudformation * on an Add a policy that allows the iam.PassR01e action for ARN of if iam PassedT0Service equal cloudformation.amazonaws.com



Correct Answer: ADF

A comprehensive and detailed explanation is: Option A is correct because removing the AdministratorAccess policy and assigning the ReadOnlyAccess managed IAM policy to the developer role is a valid way to prevent the developers from making any manual changes to the deployed resources. The AdministratorAccess policy grants full access to all AWS resources and actions, which is not necessary for the developers. The ReadOnlyAccess policy grants read-only access to most AWS resources and actions, which is sufficient for the developers to view the status of their stacks. Instructing the developers to use the CloudFormationDeployment role as a CloudFormation service role when they deploy new stacks is also a valid way to ensure that only CloudFormation can use the new role. A CloudFormation service role is an IAM role that allows CloudFormation to make calls to resources in a stack on behalf of the user1. The user can specify a service role when they create or update a stack, and CloudFormation will use that role\\'s credentials for all operations that are performed on that stack1. Option B is incorrect because updating the trust of CloudFormationDeployment role to allow the developer IAM role to assume the CloudFormationDeployment role is not a valid solution. This would allow the developers to manually assume the CloudFormationDeployment role and perform actions on the deployed resources, which is not what the company wants. The trust of CloudFormationDeployment role should only allow the cloudformation.amazonaws.com AWS principal to assume the role, as in option D. Option C is incorrect because configuring the IAM user to be able to get and pass the CloudFormationDeployment role if cloudformation actions for resources is not a valid solution. This would allow the developers to manually pass the CloudFormationDeployment role to other services or resources, which is not what the company wants. The IAM user should only be able to pass the CloudFormationDeployment role as a service role when they create or update a stack with CloudFormation, as in option A. Option D is correct because updating the trust of CloudFormationDeployment role to allow the cloudformation.amazonaws.com AWS principal to perform the iam:AssumeRole action is a valid solution. This allows CloudFormation to assume the CloudFormationDeployment role and access resources in other services on behalf of the user2. The trust policy of an IAM role defines which entities can assume the role2. By specifying cloudformation.amazonaws.com as the principal, you grant permission only to CloudFormation to assume this role. Option E is incorrect because instructing the developers to assume the CloudFormationDeployment role when they deploy new stacks is not a valid solution. This would allow the developers to manually assume the CloudFormationDeployment role and perform actions on the deployed resources, which is not what the company wants. The developers should only use the CloudFormationDeployment role as a service role when they deploy new stacks with CloudFormation, as in option A. Option F is correct because adding an IAM policy to CloudFormationDeployment that allows cloudformation:* on all resources and adding a policy that allows the iam: PassRole action for ARN of CloudFormationDeployment if iam:PassedToService equals cloudformation.amazonaws.com are valid solutions. The first policy grants permission for CloudFormationDeployment to perform any action with any resource using cloudformation.amazonaws.com as a service principal3. The second policy grants permission for passing this role only if it is passed by cloudformation.amazonaws.com as a service principal4. This ensures that only CloudFormation can use this role. References:

- 1: AWS CloudFormation service roles
- 2: How to use trust policies with IAM roles
- 3: AWS::IAM::Policy
- 4: IAM: Pass an IAM role to a specific AWS service

QUESTION 2

As CloudTrail sends a notification each time a log file is written to the Amazon S3 bucket, an account that is very active can generate a large number of notifications. If you subscribe using email or SMS, you may end up receiving a large volume of messages. Which of the following should you use to handle notifications programmatically?

- A. Amazon Kinesis Firehose
- B. Amazon Simple Queue Service (Amazon SQS)



- C. Amazon Simple Email Service (Amazon SES)
- D. Amazon AppStream

Correct Answer: B

As CloudTrail sends a notification each time a log file is written to the Amazon S3 bucket, an account that\\'s very active can generate a large number of notifications. If you subscribe using email or SMS, you can end up receiving more messages than you can handle. AWS recommends that you subscribe using Amazon Simple Queue Service (Amazon SQS), which lets you handle notifications programmatically.

Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/getting_notifications_configuration.html

QUESTION 3

A growing company manages more than 50 accounts in an organization in AWS Organizations. The company has configured its applications to send logs to Amazon CloudWatch Logs.

A DevOps engineer needs to aggregate logs so that the company can quickly search the logs to respond to future security incidents. The DevOps engineer has created a new AWS account for centralized monitoring.

Which combination of steps should the DevOps engineer take to make the application logs searchable from the monitoring account? (Select THREE.)

A. In the monitoring account, download an AWS CloudFormation template from CloudWatch to use in Organizations. Use CloudFormation StackSets in the organization\\'s management account to deploy the CloudFormation template to the entire organization.

B. Create an AWS CloudFormation template that defines an IAM role. Configure the role to allow logs-amazonaws.com to perform the logs:Link action if the aws:ResourceAccount property is equal to the monitoring account ID. Use CloudFormation StackSets in the organization\\'s management account to deploy the CloudFormation template to the entire organization.

C. Create an IAM role in the monitoring account. Attach a trust policy that allows logs.amazonaws.com to perform the iam:CreateSink action if the aws:PrincipalOrgld property is equal to the organization ID.

D. In the organization\\'s management account, enable the logging policies for the organization.

E. use CloudWatch Observability Access Manager in the monitoring account to create a sink. Allow logs to be shared with the monitoring account. Configure the monitoring account data selection to view the Observability data from the organization ID.

F. In the monitoring account, attach the CloudWatchLogsReadOnlyAccess AWS managed policy to an IAM role that can be assumed to search the logs.

Correct Answer: BCF

To aggregate logs from multiple accounts in an organization, the DevOps engineer needs to create a cross-account subscription that allows the monitoring account to receive log events from the sharing accounts.

To enable cross-account subscription, the DevOps engineer needs to create an IAM role in each sharing account that grants permission to CloudWatch Logs to link the log groups to the destination in the monitoring account. This can be done

using a CloudFormation template and StackSets to deploy the role to all accounts in the organization.



The DevOps engineer also needs to create an IAM role in the monitoring account that allows CloudWatch Logs to create a sink for receiving log events from other accounts. The role must have a trust policy that specifies the organization ID

as a condition.

Finally, the DevOps engineer needs to attach the CloudWatchLogsReadOnlyAccess policy to an IAM role in the monitoring account that can be used to search the logs from the cross-account subscription.

References:

- 1: Cross-account log data sharing with subscriptions
- 2: Create an IAM role for CloudWatch Logs in each sharing account
- 3: AWS CloudFormation StackSets
- 4: Create an IAM role for CloudWatch Logs in your monitoring account
- 5: CloudWatchLogsReadOnlyAccess policy

QUESTION 4

A company has deployed a critical application in two AWS Regions. The application uses an Application Load Balancer (ALB) in both Regions. The company has Amazon Route 53 alias DNS records for both ALBs.

The company uses Amazon Route 53 Application Recovery Controller to ensure that the application can fail over between the two Regions. The Route 53 ARC configuration includes a routing control for both Regions. The company uses Route 53 ARC to perform quarterly disaster recovery (DR) tests.

During the most recent DR test, a DevOps engineer accidentally turned off both routing controls. The company needs to ensure that at least one routing control is turned on at all times.

Which solution will meet these requirements?

A. In Route 53 ARC, create a new assertion safety rule. Apply the assertion safety rule to the two routing controls. Configure the rule with the ATLEAST type with a threshold of 1.

B. In Route 53 ARC, create a new gating safety rule. Apply the assertion safety rule to the two routing controls. Configure the rule with the OR type with a threshold of 1.

C. In Route 53 ARC, create a new resource set. Configure the resource set with an AWS::Route53::HealthCheck resource type. Specify the ARNs of the two routing controls as the target resource. Create a new readiness check for the resource set.

D. In Route 53 ARC, create a new resource set. Configure the resource set with an AWS::Route53RecoveryReadiness::DNSTargetResource resource type. Add the domain names of the two Route 53 alias DNS records as the target resource. Create a new readiness check for the resource set.

Correct Answer: A

A is correct: assertion rule to make sure that atleast on gate is always open. This rules are basically things that users cannot do or only allow to do

B: This gating rule is basically an on-off swith for a set of ARCs. If there is a controller that we dont want to turn off,



specify this rule. This rule might help us achive the goal of the question. However, this requires we specify the exact name of the controller that should not be turned off. Meanwhile, the question requires that any controller can be turned off but at least one must be up and running. Therefore, this is not the right option

QUESTION 5

A DevOps engineer at a company is supporting an AWS environment in which all users use AWS IAM Identity Center (AWS Single Sign-On). The company wants to immediately disable credentials of any new IAM user and wants the security team to receive a notification.

Which combination of steps should the DevOps engineer take to meet these requirements? (Choose three.)

A. Create an Amazon EventBridge rule that reacts to an IAM CreateUser API call in AWS CloudTrail.

B. Create an Amazon EventBridge rule that reacts to an IAM GetLoginProfile API call in AWS CloudTrail.

C. Create an AWS Lambda function that is a target of the EventBridge rule. Configure the Lambda function to disable any access keys and delete the login profiles that are associated with the IAM user.

D. Create an AWS Lambda function that is a target of the EventBridge rule. Configure the Lambda function to delete the login profiles that are associated with the IAM user.

E. Create an Amazon Simple Notification Service (Amazon SNS) topic that is a target of the EventBridge rule. Subscribe the security team\\'s group email address to the topic.

F. Create an Amazon Simple Queue Service (Amazon SQS) queue that is a target of the Lambda function. Subscribe the security team\\'s group email address to the queue.

Correct Answer: ACE

Latest DOP-C02 Dumps

DOP-C02 PDF Dumps

DOP-C02 Practice Test