

## Exam Questions DOP-C02

AWS Certified DevOps Engineer - Professional

<https://www.2passeasy.com/dumps/DOP-C02/>



### NEW QUESTION 1

A company uses a single AWS account to test applications on Amazon EC2 instances. The company has turned on AWS Config in the AWS account and has activated the restricted-ssh AWS Config managed rule.

The company needs an automated monitoring solution that will provide a customized notification in real time if any security group in the account is not compliant with the restricted-ssh rule. The customized notification must contain the name and ID of the noncompliant security group.

A DevOps engineer creates an Amazon Simple Notification Service (Amazon SNS) topic in the account and subscribes the appropriate personnel to the topic. What should the DevOps engineer do next to meet these requirements?

- A. Create an Amazon EventBridge rule that matches an AWS Config evaluation result of NON\_COMPLIANT for the restricted-ssh rule
- B. Configure an input transformer for the EventBridge rule
- C. Configure the EventBridge rule to publish a notification to the SNS topic.
- D. Configure AWS Config to send all evaluation results for the restricted-ssh rule to the SNS topic
- E. Configure a filter policy on the SNS topic to send only notifications that contain the text of NON\_COMPLIANT in the notification to subscribers.
- F. Create an Amazon EventBridge rule that matches an AWS Config evaluation result of NON\_COMPLIANT for the restricted-ssh rule
- G. Configure the EventBridge rule to invoke AWS Systems Manager Run Command on the SNS topic to customize a notification and to publish the notification to the SNS topic
- H. Create an Amazon EventBridge rule that matches all AWS Config evaluation results of NON\_COMPLIANT
- I. Configure an input transformer for the restricted-ssh rule
- J. Configure the EventBridge rule to publish a notification to the SNS topic.

**Answer:** A

#### Explanation:

Create an Amazon EventBridge (Amazon CloudWatch Events) rule that matches an AWS Config evaluation result of NON\_COMPLIANT for the restricted-ssh rule. Configure an input transformer for the EventBridge (CloudWatch Events) rule. Configure the EventBridge (CloudWatch Events) rule to publish a notification to the SNS topic. This approach uses Amazon EventBridge (previously known as Amazon CloudWatch Events) to filter AWS Config evaluation results based on the restricted-ssh rule and its compliance status (NON\_COMPLIANT). An input transformer can be used to customize the information contained in the notification, such as the name and ID of the noncompliant security group. The EventBridge (CloudWatch Events) rule can then be configured to publish a notification to the SNS topic, which will notify the appropriate personnel in real-time.

### NEW QUESTION 2

A company requires an RPO of 2 hours and an RTO of 10 minutes for its data and application at all times. An application uses a MySQL database and Amazon EC2 web servers. The development team needs a strategy for failover and disaster recovery.

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

- A. Create an Amazon Aurora cluster in one Availability Zone across multiple Regions as the data store
- B. Use Aurora's automatic recovery capabilities in the event of a disaster
- C. Create an Amazon Aurora global database in two Regions as the data store
- D. In the event of a failure, promote the secondary Region as the primary for the application.
- E. Create an Amazon Aurora multi-master cluster across multiple Regions as the data store
- F. Use a Network Load Balancer to balance the database traffic in different Regions.
- G. Set up the application in two Regions and use Amazon Route 53 failover-based routing that points to the Application Load Balancers in both Regions
- H. Use health checks to determine the availability in a given Region
- I. Use Auto Scaling groups in each Region to adjust capacity based on demand.
- J. Set up the application in two Regions and use a multi-Region Auto Scaling group behind Application Load Balancers to manage the capacity based on demand
- K. In the event of a disaster, adjust the Auto Scaling group's desired instance count to increase baseline capacity in the failover Region.

**Answer:** BD

### NEW QUESTION 3

An application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). A DevOps engineer is using AWS CodeDeploy to release a new version. The deployment fails during the AllowTraffic lifecycle event, but a cause for the failure is not indicated in the deployment logs.

What would cause this?

- A. The application specification
- B. The .yaml file contains an invalid script that runs in the AllowTraffic lifecycle hook.
- C. The user who initiated the deployment does not have the necessary permissions to interact with the ALB.
- D. The health checks specified for the ALB target group are misconfigured.
- E. The CodeDeploy agent was not installed in the EC2 instances that are part of the ALB target group.

**Answer:** C

#### Explanation:

This failure is typically due to incorrectly configured health checks in Elastic Load Balancing for the Classic Load Balancer, Application Load Balancer, or Network Load Balancer used to manage traffic for the deployment group. To resolve the issue, review and correct any errors in the health check configuration for the load balancer. <https://docs.aws.amazon.com/codedeploy/latest/userguide/troubleshooting-deployments.html#troubleshooting-deployments-allowtraffic-no-logs>

### NEW QUESTION 4

A company runs an application on one Amazon EC2 instance. Application metadata is stored in Amazon S3 and must be retrieved if the instance is restarted. The instance must restart or relaunch automatically if the instance becomes unresponsive.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm for the StatusCheckFailed metric
- B. Use the recover action to stop and start the instance
- C. Use an S3 event notification to push the metadata to the instance when the instance is back up and running.
- D. Configure AWS OpsWorks, and use the auto healing feature to stop and start the instance
- E. Use a lifecycle event in OpsWorks to pull the metadata from Amazon S3 and update it on the instance.
- F. Use EC2 Auto Recovery to automatically stop and start the instance in case of a failure
- G. Use an S3 event notification to push the metadata to the instance when the instance is back up and running.
- H. Use AWS CloudFormation to create an EC2 instance that includes the UserData property for the EC2 resource
- I. Add a command in UserData to retrieve the application metadata from Amazon S3.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/blogs/mt/how-to-set-up-aws-opsworks-stacks-auto-healing-notifications-in-amazon-cloudwatch-events/>

#### NEW QUESTION 5

A company has an application that runs on AWS Lambda and sends logs to Amazon CloudWatch Logs. An Amazon Kinesis data stream is subscribed to the log groups in CloudWatch Logs. A single consumer Lambda function processes the logs from the data stream and stores the logs in an Amazon S3 bucket. The company's DevOps team has noticed high latency during the processing and ingestion of some logs.

Which combination of steps will reduce the latency? (Select THREE.)

- A. Create a data stream consumer with enhanced fan-out
- B. Set the Lambda function that processes the logs as the consumer.
- C. Increase the ParallelizationFactor setting in the Lambda event source mapping.
- D. Configure reserved concurrency for the Lambda function that processes the logs.
- E. Increase the batch size in the Kinesis data stream.
- F. Turn off the ReportBatchItemFailures setting in the Lambda event source mapping.
- G. Increase the number of shards in the Kinesis data stream.

**Answer:** ABC

**Explanation:**

The latency in processing and ingesting logs can be caused by several factors, such as the throughput of the Kinesis data stream, the concurrency of the Lambda function, and the configuration of the event source mapping. To reduce the latency, the following steps can be taken:

? Create a data stream consumer with enhanced fan-out. Set the Lambda function that processes the logs as the consumer. This will allow the Lambda function to receive records from the data stream with dedicated throughput of up to 2 MB per second per shard, independent of other consumers<sup>1</sup>. This will reduce the contention and delay in accessing the data stream.

? Increase the ParallelizationFactor setting in the Lambda event source mapping. This will allow the Lambda service to invoke more instances of the function concurrently to process the records from the data stream<sup>2</sup>. This will increase the processing capacity and reduce the backlog of records in the data stream.

? Configure reserved concurrency for the Lambda function that processes the logs. This will ensure that the function has enough concurrency available to handle the increased load from the data stream<sup>3</sup>. This will prevent the function from being throttled by the account-level concurrency limit.

The other options are not effective or may have negative impacts on the latency. Option D is not suitable because increasing the batch size in the Kinesis data stream will increase the amount of data that the Lambda function has to process in each invocation, which may increase the execution time and latency<sup>4</sup>. Option E is not advisable because turning off the ReportBatchItemFailures setting in the Lambda event source mapping will prevent the Lambda service from retrying the failed records, which may result in data loss. Option F is not necessary because increasing the number of shards in the Kinesis data stream will increase the throughput of the data stream, but it will not affect the processing speed of the Lambda function, which is the bottleneck in this scenario.

References:

? 1: Using AWS Lambda with Amazon Kinesis Data Streams - AWS Lambda

? 2: AWS Lambda event source mappings - AWS Lambda

? 3: Managing concurrency for a Lambda function - AWS Lambda

? 4: AWS Lambda function scaling - AWS Lambda

? : AWS Lambda event source mappings - AWS Lambda

? : Scaling Amazon Kinesis Data Streams with AWS CloudFormation - Amazon Kinesis Data Streams

#### NEW QUESTION 6

A company wants to set up a continuous delivery pipeline. The company stores application code in a private GitHub repository. The company needs to deploy the application components to Amazon Elastic Container Service (Amazon ECS), Amazon EC2, and AWS Lambda. The pipeline must support manual approval actions.

Which solution will meet these requirements?

- A. Use AWS CodePipeline with Amazon EC
- B. Amazon EC2, and Lambda as deploy providers.
- C. Use AWS CodePipeline with AWS CodeDeploy as the deploy provider.
- D. Use AWS CodePipeline with AWS Elastic Beanstalk as the deploy provider.
- E. Use AWS CodeDeploy with GitHub integration to deploy the application.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-steps.html>

#### NEW QUESTION 7

A company is implementing a well-architected design for its globally accessible API stack. The design needs to ensure both high reliability and fast response times for users located in North America and Europe.

The API stack contains the following three tiers: Amazon API Gateway

AWS Lambda Amazon DynamoDB

Which solution will meet the requirements?

- A. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using health check
- B. Configure the APIs to forward requests to a Lambda function in that Region
- C. Configure the Lambda functions to retrieve and update the data in a DynamoDB table in the same Region as the Lambda function.
- D. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using latency-based routing and health check
- E. Configure the APIs to forward requests to a Lambda function in that Region
- F. Configure the Lambda functions to retrieve and update the data in a DynamoDB global table.
- G. Configure Amazon Route 53 to point to API Gateway in North America, create a disaster recovery API in Europe, and configure both APIs to forward requests to the Lambda functions in that Region
- H. Retrieve the data from a DynamoDB global table
- I. Deploy a Lambda function to check the North America API health every 5 minute
- J. In the event of a failure, update Route 53 to point to the disaster recovery API.
- K. Configure Amazon Route 53 to point to API Gateway API in North America using latency-based routing

- L. Configure the API to forward requests to the Lambda function in the Region nearest to the use
- M. Configure the Lambda function to retrieve and update the data in a DynamoDB table.

**Answer:** B

#### NEW QUESTION 8

A company hosts its staging website using an Amazon EC2 instance backed with Amazon EBS storage. The company wants to recover quickly with minimal data losses in the event of network connectivity issues or power failures on the EC2 instance. Which solution will meet these requirements?

- A. Add the instance to an EC2 Auto Scaling group with the minimum, maximum, and desired capacity set to 1.
- B. Add the instance to an EC2 Auto Scaling group with a lifecycle hook to detach the EBS volume when the EC2 instance shuts down or terminates.
- C. Create an Amazon CloudWatch alarm for the StatusCheckFailed System metric and select the EC2 action to recover the instance.
- D. Create an Amazon CloudWatch alarm for the StatusCheckFailed Instance metric and select the EC2 action to reboot the instance.

**Answer:** C

#### Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html>

#### NEW QUESTION 9

A company has a mobile application that makes HTTP API calls to an Application Load Balancer (ALB). The ALB routes requests to an AWS Lambda function. Many different versions of the application are in use at any given time, including versions that are in testing by a subset of users. The version of the application is defined in the user-agent header that is sent with all requests to the API.

After a series of recent changes to the API, the company has observed issues with the application. The company needs to gather a metric for each API operation by response code for each version of the application that is in use. A DevOps engineer has modified the Lambda function to extract the API operation name, version information from the user-agent header and response code.

Which additional set of actions should the DevOps engineer take to gather the required metrics?

- A. Modify the Lambda function to write the API operation name, response code, and version number as a log line to an Amazon CloudWatch Logs log group
- B. Configure a CloudWatch Logs metric filter that increments a metric for each API operation name
- C. Specify response code and application version as dimensions for the metric.
- D. Modify the Lambda function to write the API operation name, response code, and version number as a log line to an Amazon CloudWatch Logs log group
- E. Configure a CloudWatch Logs Insights query to populate CloudWatch metrics from the log line
- F. Specify response code and application version as dimensions for the metric.
- G. Configure the ALB access logs to write to an Amazon CloudWatch Logs log group
- H. Modify the Lambda function to respond to the ALB with the API operation name, response code, and version number as response metadata
- I. Configure a CloudWatch Logs metric filter that increments a metric for each API operation name
- J. Specify response code and application version as dimensions for the metric.
- K. Configure AWS X-Ray integration on the Lambda function
- L. Modify the Lambda function to create an X-Ray subsegment with the API operation name, response code, and version number
- M. Configure X-Ray insights to extract an aggregated metric for each API operation name and to publish the metric to Amazon CloudWatch
- N. Specify response code and application version as dimensions for the metric.

**Answer:** A

#### Explanation:

"Note that the metric filter is different from a log insights query, where the experience is interactive and provides immediate search results for the user to investigate.

No automatic action can be invoked from an insights query. Metric filters, on the other hand, will generate metric data in the form of a time series. This lets you create alarms that integrate into your ITSM processes, execute AWS Lambda functions, or even create anomaly detection models."

<https://aws.amazon.com/blogs/mt/quantify-custom-application-metrics-with-amazon-cloudwatch-logs-and-metric-filters/>

#### NEW QUESTION 10

A company has chosen AWS to host a new application. The company needs to implement a multi-account strategy. A DevOps engineer creates a new AWS account and an organization in AWS Organizations. The DevOps engineer also creates the OU structure for the organization and sets up a landing zone by using AWS Control Tower.

The DevOps engineer must implement a solution that automatically deploys resources for new accounts that users create through AWS Control Tower Account Factory. When a user creates a new account, the solution must apply AWS CloudFormation templates and SCPs that are customized for the OU or the account to automatically deploy all the resources that are attached to the account. All the OUs are enrolled in AWS Control Tower.

Which solution will meet these requirements in the MOST automated way?

- A. Use AWS Service Catalog with AWS Control Tower
- B. Create portfolios and products in AWS Service Catalog
- C. Grant granular permissions to provision these resources
- D. Deploy SCPs by using the AWS CLI and JSON documents.
- E. Deploy CloudFormation stack sets by using the required template
- F. Enable automatic deployments
- G. Deploy stack instances to the required account
- H. Deploy a CloudFormation stack set to the organization's management account to deploy SCPs.
- I. Create an Amazon EventBridge rule to detect the CreateManagedAccount event
- J. Configure AWS Service Catalog as the target to deploy resources to any new account
- K. Deploy SCPs by using the AWS CLI and JSON documents.
- L. Deploy the Customizations for AWS Control Tower (CfCT) solution
- M. Use an AWS CodeCommit repository as the source
- N. In the repository, create a custom package that includes the CloudFormation templates and the SCP JSON documents.

**Answer:** D

#### Explanation:



The CfCT solution is designed for the exact purpose stated in the question. It extends the capabilities of AWS Control Tower by providing you with a way to automate resource provisioning and apply custom configurations across all AWS accounts created in the Control Tower environment. This enables the company to implement additional account customizations when new accounts are provisioned via the Control Tower Account Factory. The CloudFormation templates and SCPs can be added to a CodeCommit repository and will be automatically deployed to new accounts when they are created. This provides a highly automated solution that does not require manual intervention to deploy resources and SCPs to new accounts.

#### NEW QUESTION 10

A DevOps engineer is creating an AWS CloudFormation template to deploy a web service. The web service will run on Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). The DevOps engineer must ensure that the service can accept requests from clients that have IPv6 addresses. What should the DevOps engineer do with the CloudFormation template so that IPv6 clients can access the web service?

- A. Add an IPv6 CIDR block to the VPC and the private subnet for the EC2 instance
- B. Create route table entries for the IPv6 network, use EC2 instance types that support IPv6, and assign IPv6 addresses to each EC2 instance.
- C. Assign each EC2 instance an IPv6 Elastic IP address
- D. Create a target group, and add the EC2 instances as target
- E. Create a listener on port 443 of the ALB, and associate the target group with the ALB.
- F. Replace the ALB with a Network Load Balancer (NLB). Add an IPv6 CIDR block to the VPC and subnets for the NLB, and assign the NLB an IPv6 Elastic IP address.
- G. Add an IPv6 CIDR block to the VPC and subnets for the AL
- H. Create a listener on port 443. and specify the dualstack IP address type on the AL
- I. Create a target group, and add the EC2 instances as target
- J. Associate the target group with the ALB.

**Answer:** D

#### Explanation:

it involves adding an IPv6 CIDR block to the VPC and subnets for the ALB and specifying the dualstack IP address type on the ALB listener. This allows the ALB to listen on both IPv4 and IPv6 addresses, and forward requests to the EC2 instances that are added as targets to the target group associated with the ALB.

#### NEW QUESTION 13

A company deploys its corporate infrastructure on AWS across multiple AWS Regions and Availability Zones. The infrastructure is deployed on Amazon EC2 instances and connects with AWS IoT Greengrass devices. The company deploys additional resources on on- premises servers that are located in the corporate headquarters.

The company wants to reduce the overhead involved in maintaining and updating its resources. The company's DevOps team plans to use AWS Systems Manager to implement automated management and application of patches. The DevOps team confirms that Systems Manager is available in the Regions that the resources are deployed m Systems Manager also is available in a Region near the corporate headquarters.

Which combination of steps must the DevOps team take to implement automated patch and configuration management across the company's EC2 instances IoT devices and on- premises infrastructure? (Select THREE.)

- A. Apply tags lo all the EC2 instance
- B. AWS IoT Greengrass devices, and on-premises server
- C. Use Systems Manager Session Manager to push patches to all the tagged devices.
- D. Use Systems Manager Run Command to schedule patching for the EC2 instances AWS IoT Greengrass devices and on-premises servers.
- E. Use Systems Manager Patch Manager to schedule patching IoT the EC2 instances AWS IoT Greengrass devices and on-premises servers as a Systems Manager maintenance window task.
- F. Configure Amazon EventBridge to monitor Systems Manager Patch Manager for updates to patch baseline
- G. Associate Systems Manager Run Command with the event lo initiate a patch action for all EC2 instances AWS IoT Greengrass devices and on-premises servers.
- H. Create an IAM instance profile for Systems Manager Attach the instance profile to all the EC2 instances in the AWS accoun
- I. For the AWS IoT Greengrass devices and on-premises servers create an IAM service role for Systems Manager.
- J. Generate a managed-instance activation Use the Activation Code and Activation ID to install Systems Manager Agent (SSM Agent) on each server in the on-premises environment Update the AWS IoT Greengrass IAM token exchange role Use the role to deploy SSM Agent on all the IoT devices.

**Answer:** CEF

#### Explanation:

[https://aws.amazon.com/blogs/mt/how-to-centrally-manage-aws-iot-greengrass-devices-using-aws-systems-manager/?force\\_isolation=true](https://aws.amazon.com/blogs/mt/how-to-centrally-manage-aws-iot-greengrass-devices-using-aws-systems-manager/?force_isolation=true)

#### NEW QUESTION 18

A DevOps team manages an API running on-premises that serves as a backend for an Amazon API Gateway endpoint. Customers have been complaining about high response latencies, which the development team has verified using the API Gateway latency metrics in Amazon CloudWatch. To identify the cause, the team needs to collect relevant data without introducing additional latency.

Which actions should be taken to accomplish this? (Choose two.)

- A. Install the CloudWatch agent server side and configure the agent to upload relevant logs to CloudWatch.
- B. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and upload those segments to X-Ray during each request.
- C. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and use the X-Ray daemon to upload segments to X-Ray.
- D. Modify the on-premises application to send log information back to API Gateway with each request.
- E. Modify the on-premises application to calculate and upload statistical data relevant to the API service requests to CloudWatch metrics.

**Answer:** AC

#### Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html>  
<https://docs.aws.amazon.com/xray/latest/devguide/xray-api-sendingdata.html>

#### NEW QUESTION 21

An Amazon EC2 instance is running in a VPC and needs to download an object from a restricted Amazon S3 bucket. When the DevOps engineer tries to download the object, an AccessDenied error is received,

What are the possible causes for this error? (Select TWO,)

- A. The S3 bucket default encryption is enabled.
- B. There is an error in the S3 bucket policy.
- C. The object has been moved to S3 Glacier.
- D. There is an error in the IAM role configuration.
- E. S3 Versioning is enabled.

**Answer:** BD

**Explanation:**

These are the possible causes for the AccessDenied error because they affect the permissions to access the S3 object from the EC2 instance. An S3 bucket policy is a resource-based policy that defines who can access the bucket and its objects, and what actions they can perform. An IAM role is an identity that can be assumed by an EC2 instance to grant it permissions to access AWS services and resources. If there is an error in the S3 bucket policy or the IAM role configuration, such as a missing or incorrect statement, condition, or principal, then the EC2 instance may not have the necessary permissions to download the object from the S3 bucket. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html>  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

**NEW QUESTION 25**

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 CodeDeploy 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 LambdaCanary10Percent10Minute.
- C. 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.
- E. Create an Amazon Simple Notification Service (Amazon SNS) topic to send notifications every time a deployment fails.
- F. Configure the SNS topic to invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment.
- G. Set the deployment configuration in CodeDeploy to LambdaCanary10Percent10Minutes. 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 error.
- H. Configure the metric filter to invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment.

**Answer:** B

**Explanation:**

? 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

**NEW QUESTION 27**

A company requires its internal business teams to launch resources through pre-approved AWS CloudFormation templates only. The security team requires automated monitoring when resources drift from their expected state. Which strategy should be used to meet these requirements?

- A. Allow users to deploy CloudFormation stacks using a CloudFormation service role only.
- B. Use CloudFormation drift detection to detect when resources have drifted from their expected state.
- C. Allow users to deploy CloudFormation stacks using a CloudFormation service role only.
- D. Use AWS Config rules to detect when resources have drifted from their expected state.
- E. Allow users to deploy CloudFormation stacks using AWS Service Catalog only.
- F. Enforce the use of a launch constraint.
- G. Use AWS Config rules to detect when resources have drifted from their expected state.
- H. Allow users to deploy CloudFormation stacks using AWS Service Catalog only.
- I. Enforce the use of a template constraint.
- J. Use Amazon EventBridge notifications to detect when resources have drifted from their expected state.

**Answer:** C

**Explanation:**

The correct answer is C. Allowing users to deploy CloudFormation stacks using AWS Service Catalog only and enforcing the use of a launch constraint is the best

way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only. AWS Service Catalog is a service that enables organizations to create and manage catalogs of IT services that are approved for use on AWS. A launch constraint is a rule that specifies the role that AWS Service Catalog assumes when launching a product.

By using a launch constraint, the DevOps engineer can control the permissions that the users have when launching a product. Using AWS Config rules to detect when resources have drifted from their expected state is the best way to automate the monitoring of the resources. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config rules are custom or managed rules that AWS Config uses to evaluate whether your AWS resources comply with your desired configurations. By using AWS Config rules, the DevOps engineer can track the changes in the resources and identify any non-compliant resources.

Option A is incorrect because allowing users to deploy CloudFormation stacks using a CloudFormation service role only is not the best way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only. A CloudFormation service role is an IAM role that CloudFormation assumes to create, update, or delete the stack resources. By using a CloudFormation service role, the DevOps engineer can control the permissions that CloudFormation has when acting on the resources, but not the permissions that the users have when launching a stack. Therefore, option A does not prevent the users from launching resources that are not approved by the company. Using CloudFormation drift detection to detect when resources have drifted from their expected state is a valid way to monitor the resources, but it is not as automated and scalable as using AWS Config rules. CloudFormation drift detection is a feature that enables you to detect whether a stack's actual configuration differs, or has drifted, from its expected configuration. To use this feature, the DevOps engineer would need to manually initiate a drift detection operation on the stack or the stack resources, and then view the drift status and details in the CloudFormation console or API.

Option B is incorrect because allowing users to deploy CloudFormation stacks using a CloudFormation service role only is not the best way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only, as explained in option A. Using AWS Config rules to detect when resources have drifted from their expected state is a valid way to monitor the resources, as explained in option C. Option D is incorrect because enforcing the use of a template constraint is not the best way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only. A template constraint is a rule that defines the values or properties that users can specify when launching a product. By using a template constraint, the DevOps engineer can control the parameters that the users can provide when launching a product, but not the permissions that the users have when launching a product. Therefore, option D does not prevent the users from launching resources that are not approved by the company. Using Amazon EventBridge notifications to detect when resources have drifted from their expected state is a less reliable and consistent solution than using AWS Config rules. Amazon EventBridge is a service that enables you to connect your applications with data from a variety of sources. Amazon EventBridge can deliver a stream of real-time data from event sources, such as AWS services, and route

that data to targets, such as AWS Lambda functions. However, to use this solution, the DevOps engineer would need to configure the event source, the event bus, the event rule, and the event target for each resource type that needs to be monitored, which is more complex and error-prone than using AWS Config rules.

#### NEW QUESTION 29

A company has multiple development groups working in a single shared AWS account. The Senior Manager of the groups wants to be alerted via a third-party API call when the creation of resources approaches the service limits for the account.

Which solution will accomplish this with the LEAST amount of development effort?

- A. Create an Amazon CloudWatch Event rule that runs periodically and targets an AWS Lambda function
- B. Within the Lambda function, evaluate the current state of the AWS environment and compare deployed resource values to resource limits on the account
- C. Notify the Senior Manager if the account is approaching a service limit.
- D. Deploy an AWS Lambda function that refreshes AWS Trusted Advisor checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically
- E. Create another CloudWatch Events rule with an event pattern matching Trusted Advisor events and a target Lambda function
- F. In the target Lambda function, notify the Senior Manager.
- G. Deploy an AWS Lambda function that refreshes AWS Personal Health Dashboard checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically
- H. Create another CloudWatch Events rule with an event pattern matching Personal Health Dashboard events and a target Lambda function
- I. In the target Lambda function, notify the Senior Manager.
- J. Add an AWS Config custom rule that runs periodically, checks the AWS service limit status, and streams notifications to an Amazon SNS topic
- K. Deploy an AWS Lambda function that notifies the Senior Manager, and subscribe the Lambda function to the SNS topic.

**Answer: B**

#### Explanation:

To meet the requirements, the company needs to create a solution that alerts the Senior Manager when the creation of resources approaches the service limits for the account with the least amount of development effort. The company can use AWS Trusted Advisor, which is a service that provides best practice recommendations for cost optimization, performance, security, and service limits. The company can deploy an AWS Lambda function that refreshes Trusted Advisor checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically. This will ensure that Trusted Advisor checks are up to date and reflect the current state of the account. The company can then create another CloudWatch Events rule with an event pattern matching Trusted Advisor events and a target Lambda function. The event pattern can filter for events related to service limit checks and their status. The target Lambda function can notify the Senior Manager via a third-party API call if the event indicates that the account is approaching or exceeding a service limit.

#### NEW QUESTION 30

A company's DevOps engineer is creating an AWS Lambda function to process notifications from an Amazon Simple Notification Service (Amazon SNS) topic. The Lambda function will process the notification messages and will write the contents of the notification messages to an Amazon RDS Multi-AZ DB instance.

During testing a database administrator accidentally shut down the DB instance. While the database was down the company lost several of the SNS notification messages that were delivered during that time.

The DevOps engineer needs to prevent the loss of notification messages in the future. Which solutions will meet this requirement? (Select TWO.)

- A. Replace the RDS Multi-AZ DB instance with an Amazon DynamoDB table.
- B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination of the Lambda function.
- C. Configure an Amazon Simple Queue Service (Amazon SQS) dead-letter queue for the SNS topic.
- D. Subscribe an Amazon Simple Queue Service (Amazon SQS) queue to the SNS topic. Configure the Lambda function to process messages from the SQS queue.
- E. Replace the SNS topic with an Amazon EventBridge event bus. Configure an EventBridge rule on the new event bus to invoke the Lambda function for each event.

**Answer: CD**

#### Explanation:

These solutions will meet the requirement because they will prevent the loss of notification messages in the future. An Amazon SQS queue is a service that provides a reliable, scalable, and secure message queue for asynchronous communication between distributed components. You can use an SQS queue to buffer messages from an SNS topic and ensure that they are delivered and processed by a Lambda function, even if the function or the database is temporarily



unavailable.

Option C will configure an SQS dead-letter queue for the SNS topic. A dead-letter queue is a queue that receives messages that could not be delivered to any subscriber after a specified number of retries. You can use a dead-letter queue to store and analyze failed messages, or to reprocess them later. This way, you can avoid losing messages that could not be delivered to the Lambda function due to network errors, throttling, or other issues. Option D will subscribe an SQS queue to the SNS topic and configure the Lambda function to process messages from the SQS queue. This will decouple the SNS topic from the Lambda function and provide more flexibility and control over the message delivery and processing. You can use an SQS queue to store messages from the SNS topic until they are ready to be processed by the Lambda function, and also to retry processing in case of failures. This way, you can avoid losing messages that could not be processed by the Lambda function due to database errors, timeouts, or other issues.

### NEW QUESTION 31

A company's application teams use AWS CodeCommit repositories for their applications.

The application teams have repositories in multiple AWS accounts. All accounts are in an organization in AWS Organizations.

Each application team uses AWS IAM Identity Center (AWS Single Sign-On) configured with an external IdP to assume a developer IAM role. The developer role allows the application teams to use Git to work with the code in the repositories.

A security audit reveals that the application teams can modify the main branch in any repository. A DevOps engineer must implement a solution that allows the application teams to modify the main branch of only the repositories that they manage.

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

- A. Update the SAML assertion to pass the user's team name
- B. Update the IAM role's trust policy to add an access-team session tag that has the team name.
- C. Create an approval rule template for each team in the Organizations management account
- D. Associate the template with all the repositories
- E. Add the developer role ARN as an approver.
- F. Create an approval rule template for each account
- G. Associate the template with all repositories
- H. Add the "aws:ResourceTag/access-team": "\$ ;{aws:PrincipalTag/access-team}" condition to the approval rule template.
- I. For each CodeCommit repository, add an access-team tag that has the value set to the name of the associated team.
- J. Attach an SCP to the account
- K. Include the following statement:

```
{
  "Effect": "Deny",
  "Action": [
    "codecommit:GitPush",
    "codecommit:PutFile",
    "codecommit:Merge*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEqualsIfExists": {
      "codecommit:References": ["refs/heads/main"]
    },
    "StringNotEquals": {
      "aws:ResourceTag/access-team": "$ ;{aws:PrincipalTag/access-team}"
    },
    "Null": {
      "codecommit:References": "false"
    }
  }
}
```

- L. Create an IAM permissions boundary in each account

- M. Include the following statement:

```
{
  "Effect": "Allow",
  "Action": [
    "codecommit:GitPush",
    "codecommit:PutFile",
    "codecommit:Merge*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEqualsIfExists": {
      "codecommit:References": ["refs/heads/main"]
    },
    "StringNotEquals": {
      "aws:ResourceTag/access-team": "$ ;{aws:PrincipalTag/access-team}"
    },
    "Null": {
      "codecommit:References": "false"
    }
  }
}
```

Answer: ADF



**Explanation:**

Short Explanation: To meet the requirements, the DevOps engineer should update the SAML assertion to pass the user's team name, update the IAM role's trust policy to add an access-team session tag that has the team name, create an IAM permissions boundary in each account, and for each CodeCommit repository, add an access-team tag that has the value set to the name of the associated team.

References:

? Updating the SAML assertion to pass the user's team name allows the DevOps engineer to use IAM tags to identify which team a user belongs to. This can help enforce fine-grained access control based on the user's team membership<sup>1</sup>.

? Updating the IAM role's trust policy to add an access-team session tag that has the team name allows the DevOps engineer to use IAM condition keys to restrict access based on the session tag value<sup>2</sup>. For example, the DevOps engineer can use the `aws:PrincipalTag` condition key to match the access-team tag of the user with the access-team tag of the repository<sup>3</sup>.

? Creating an IAM permissions boundary in each account allows the DevOps engineer to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries<sup>4</sup>. For example, the DevOps engineer can use a permissions boundary policy to limit the actions that a user can perform on CodeCommit repositories based on their access-team tag<sup>5</sup>.

? For each CodeCommit repository, adding an access-team tag that has the value set to the name of the associated team allows the DevOps engineer to use resource tags to identify which team manages a repository. This can help enforce fine-grained access control based on the resource tag value<sup>6</sup>.

? The other options are incorrect because:

**NEW QUESTION 35**

A company is running an application on Amazon EC2 instances in an Auto Scaling group. Recently an issue occurred that prevented EC2 instances from launching successfully and it took several hours for the support team to discover the issue. The support team wants to be notified by email whenever an EC2 instance does not start successfully.

Which action will accomplish this?

- A. Add a health check to the Auto Scaling group to invoke an AWS Lambda function whenever an instance status is impaired.
- B. Configure the Auto Scaling group to send a notification to an Amazon SNS topic whenever a failed instance launch occurs.
- C. Create an Amazon CloudWatch alarm that invokes an AWS Lambda function when a failed `AttachInstances` Auto Scaling API call is made.
- D. Create a status check alarm on Amazon EC2 to send a notification to an Amazon SNS topic whenever a status check fail occurs.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ASGettingNotifications.html#auto-scaling-sns-notifications>

**NEW QUESTION 37**

A security review has identified that an AWS CodeBuild project is downloading a database population script from an Amazon S3 bucket using an unauthenticated request. The security team does not allow unauthenticated requests to S3 buckets for this project.

How can this issue be corrected in the MOST secure manner?

- A. Add the bucket name to the `AllowedBuckets` section of the CodeBuild project setting
- B. Update the build spec to use the AWS CLI to download the database population script.
- C. Modify the S3 bucket settings to enable HTTPS basic authentication and specify a token
- D. Update the build spec to use `cURL` to pass the token and download the database population script.
- E. Remove unauthenticated access from the S3 bucket with a bucket policy
- F. Modify the service role for the CodeBuild project to include Amazon S3 access
- G. Use the AWS CLI to download the database population script.
- H. Remove unauthenticated access from the S3 bucket with a bucket policy
- I. Use the AWS CLI to download the database population script using an IAM access key and a secret access key.

**Answer: C**

**Explanation:**

A bucket policy is a resource-based policy that defines who can access a specific S3 bucket and what actions they can perform on it. By removing unauthenticated access from the bucket policy, you can prevent anyone without valid credentials from accessing the bucket. A service role is an IAM role that allows an AWS service, such as CodeBuild, to perform actions on your behalf. By modifying the service role for the CodeBuild project to include Amazon S3 access, you can grant the project permission to read and write objects in the S3 bucket. The AWS CLI is a command-line tool that allows you to interact with AWS services, such as S3, using commands in your terminal. By using the AWS CLI to download the database population script, you can leverage the service role credentials and encryption to secure the data transfer.

For more information, you can refer to these web pages:

? [Using bucket policies and user policies - Amazon Simple Storage Service]

? [Create a service role for CodeBuild - AWS CodeBuild]

? [AWS Command Line Interface]

**NEW QUESTION 38**

A company hosts applications in its AWS account. Each application logs to an individual Amazon CloudWatch log group. The company's CloudWatch costs for ingestion are increasing.

A DevOps engineer needs to identify which applications are the source of the increased logging costs.

Which solution will meet these requirements?

- A. Use CloudWatch metrics to create a custom expression that identifies the CloudWatch log groups that have the most data being written to them.
- B. Use CloudWatch Logs Insights to create a set of queries for the application log groups to identify the number of logs written for a period of time.
- C. Use AWS Cost Explorer to generate a cost report that details the cost for CloudWatch usage.
- D. Use AWS CloudTrail to filter for `CreateLogStream` events for each application.

**Answer: C**

**Explanation:**

The correct answer is C.

A comprehensive and detailed explanation is:

? Option A is incorrect because using CloudWatch metrics to create a custom expression that identifies the CloudWatch log groups that have the most data being

written to them is not a valid solution. CloudWatch metrics do not provide information about the size or volume of data being ingested by CloudWatch logs. CloudWatch metrics only provide information about the number of events, bytes, and errors that occur within a log group or stream. Moreover, creating a custom expression with CloudWatch metrics would require using the `search_web` tool, which is not necessary for this use case.

? Option B is incorrect because using CloudWatch Logs Insights to create a set of queries for the application log groups to identify the number of logs written for a period of time is not a valid solution. CloudWatch Logs Insights can help analyze and filter log events based on patterns and expressions, but it does not provide information about the cost or billing of CloudWatch logs. CloudWatch Logs Insights also charges based on the amount of data scanned by each query, which could increase the logging costs further.

? Option C is correct because using AWS Cost Explorer to generate a cost report that details the cost for CloudWatch usage is a valid solution. AWS Cost Explorer is a tool that helps visualize, understand, and manage AWS costs and usage over time. AWS Cost Explorer can generate custom reports that show the breakdown of costs by service, region, account, tag, or any other dimension. AWS Cost Explorer can also filter and group costs by usage type, which can help identify the specific CloudWatch log groups that are the source of the increased logging costs.

? Option D is incorrect because using AWS CloudTrail to filter for `CreateLogStream` events for each application is not a valid solution. AWS CloudTrail is a service that records API calls and account activity for AWS services, including CloudWatch logs. However, AWS CloudTrail does not provide information about the cost or billing of CloudWatch logs. Filtering for `CreateLogStream` events would only show when a new log stream was created within a log group, but not how much data was ingested or stored by that log stream.

References:

- ? CloudWatch Metrics
- ? CloudWatch Logs Insights
- ? AWS Cost Explorer
- ? AWS CloudTrail

#### NEW QUESTION 43

A company that runs many workloads on AWS has an Amazon EBS spend that has increased over time. The DevOps team notices there are many unattached EBS volumes. Although there are workloads where volumes are detached, volumes over 14 days old are stale and no longer needed. A DevOps engineer has been tasked with creating automation that deletes unattached EBS volumes that have been unattached for 14 days. Which solution will accomplish this?

- A. Configure the AWS Config `ec2-volume-inuse-check` managed rule with a configuration changes trigger type and an Amazon EC2 volume resource target
- B. Create a new Amazon CloudWatch Events rule scheduled to execute an AWS Lambda function in 14 days to delete the specified EBS volume.
- C. Use Amazon EC2 and Amazon Data Lifecycle Manager to configure a volume lifecycle policy
- D. Set the interval period for unattached EBS volumes to 14 days and set the retention rule to delete
- E. Set the policy target volumes as `*`.
- F. Create an Amazon CloudWatch Events rule to execute an AWS Lambda function daily
- G. The Lambda function should find unattached EBS volumes and tag them with the current date, and delete unattached volumes that have tags with dates that are more than 14 days old.
- H. Use AWS Trusted Advisor to detect EBS volumes that have been detached for more than 14 days
- I. Execute an AWS Lambda function that creates a snapshot and then deletes the EBS volume.

**Answer: C**

#### Explanation:

The requirement is to create automation that deletes unattached EBS volumes that have been unattached for 14 days. To do this, the DevOps engineer needs to use the following steps:

? Create an Amazon CloudWatch Events rule to execute an AWS Lambda function daily. CloudWatch Events is a service that enables event-driven architectures by delivering events from various sources to targets. Lambda is a service that lets you run code without provisioning or managing servers. By creating a CloudWatch Events rule that executes a Lambda function daily, the DevOps engineer can schedule a recurring task to check and delete unattached EBS volumes.

? The Lambda function should find unattached EBS volumes and tag them with the current date, and delete unattached volumes that have tags with dates that are more than 14 days old. The Lambda function can use the EC2 API to list and filter unattached EBS volumes based on their state and tags. The function can then tag each unattached volume with the current date using the `create-tags` command. The function can also compare the tag value with the current date and delete any unattached volume that has been tagged more than 14 days ago using the `delete-volume` command.

#### NEW QUESTION 44

A company has a guideline that every Amazon EC2 instance must be launched from an AMI that the company's security team produces. Every month the security team sends an email message with the latest approved AMIs to all the development teams. The development teams use AWS CloudFormation to deploy their applications. When developers launch a new service they have to search their email for the latest AMIs that the security department sent. A DevOps engineer wants to automate the process that the security team uses to provide the AMI IDs to the development teams. What is the MOST scalable solution that meets these requirements?

- A. Direct the security team to use CloudFormation to create new versions of the AMIs and to list the AMI ARNs in an encrypted Amazon S3 object as part of the stack's Outputs Section. Instruct the developers to use a cross-stack reference to load the encrypted S3 object and obtain the most recent AMI ARNs.
- B. Direct the security team to use a CloudFormation stack to create an AWS CodePipeline pipeline that builds new AMIs and places the latest AMI ARNs in an encrypted Amazon S3 object as part of the pipeline output. Instruct the developers to use a cross-stack reference within their own CloudFormation template to obtain the S3 object location and the most recent AMI ARNs.
- C. Direct the security team to use Amazon EC2 Image Builder to create new AMIs and to place the AMI ARNs as parameters in AWS Systems Manager Parameter Store. Instruct the developers to specify a parameter of type SSM in their CloudFormation stack to obtain the most recent AMI ARNs from Parameter Store.
- D. Direct the security team to use Amazon EC2 Image Builder to create new AMIs and to create an Amazon Simple Notification Service (Amazon SNS) topic so that every development team can receive notification.
- E. When the development teams receive a notification, instruct them to write an AWS Lambda function that will update their CloudFormation stack with the most recent AMI ARNs.

**Answer: C**

#### Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/dynamic-references.html>

#### NEW QUESTION 49

A rapidly growing company wants to scale for developer demand for AWS development environments. Development environments are created manually in the AWS Management Console. The networking team uses AWS CloudFormation to manage the networking infrastructure, exporting stack output values for the Amazon VPC and all subnets. The development environments have common standards, such as Application Load Balancers, Amazon EC2 Auto Scaling groups, security groups, and Amazon DynamoDB tables.

To keep up with demand, the DevOps engineer wants to automate the creation of development environments. Because the infrastructure required to support the application is expected to grow, there must be a way to easily update the deployed infrastructure. CloudFormation will be used to create a template for the development environments.

Which approach will meet these requirements and quickly provide consistent AWS environments for developers?

- A. Use Fn::ImportValue intrinsic functions in the Resources section of the template to retrieve Virtual Private Cloud (VPC) and subnet value
- B. Use CloudFormation StackSets for the development environments, using the Count input parameter to indicate the number of environments needed
- C. Use the UpdateStackSet command to update existing development environments.
- D. Use nested stacks to define common infrastructure component
- E. To access the exported values, use TemplateURL to reference the networking team's template
- F. To retrieve Virtual Private Cloud (VPC) and subnet values, use Fn::ImportValue intrinsic functions in the Parameters section of the root template
- G. Use the CreateChangeSet and ExecuteChangeSet commands to update existing development environments.
- H. Use nested stacks to define common infrastructure component
- I. Use Fn::ImportValue intrinsic functions with the resources of the nested stack to retrieve Virtual Private Cloud (VPC) and subnet value
- J. Use the CreateChangeSet and ExecuteChangeSet commands to update existing development environments.
- K. Use Fn::ImportValue intrinsic functions in the Parameters section of the root template to retrieve Virtual Private Cloud (VPC) and subnet value
- L. Define the development resources in the order they need to be created in the CloudFormation nested stack
- M. Use the CreateChangeSet
- N. and ExecuteChangeSet commands to update existing development environments.

**Answer:** C

#### Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-importvalue.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-importvalue.html> CF of network exports the VPC, subnet or needed information CF of application imports the above information to its stack and UpdateChangeSet/ ExecuteChangeSet

#### NEW QUESTION 50

A company uses an organization in AWS Organizations that has all features enabled. The company uses AWS Backup in a primary account and uses an AWS Key Management Service (AWS KMS) key to encrypt the backups.

The company needs to automate a cross-account backup of the resources that AWS Backup backs up in the primary account. The company configures cross-account backup in the Organizations management account. The company creates a new AWS account in the organization and configures an AWS Backup backup vault in the new account. The company creates a KMS key in the new account to encrypt the backups. Finally, the company configures a new backup plan in the primary account. The destination for the new backup plan is the backup vault in the new account.

When the AWS Backup job in the primary account is invoked, the job creates backups in the primary account. However, the backups are not copied to the new account's backup vault.

Which combination of steps must the company take so that backups can be copied to the new account's backup vault? (Select TWO.)

- A. Edit the backup vault access policy in the new account to allow access to the primary account.
- B. Edit the backup vault access policy in the primary account to allow access to the new account.
- C. Edit the backup vault access policy in the primary account to allow access to the KMS key in the new account.
- D. Edit the key policy of the KMS key in the primary account to share the key with the new account.
- E. Edit the key policy of the KMS key in the new account to share the key with the primary account.

**Answer:** AE

#### Explanation:

To enable cross-account backup, the company needs to grant permissions to both the backup vault and the KMS key in the destination account. The backup vault access policy in the destination account must allow the primary account to copy backups into the vault. The key policy of the KMS key in the destination account must allow the primary account to use the key to encrypt and decrypt the backups. These steps are described in the AWS documentation<sup>12</sup>. Therefore, the correct answer is A and E.

References:

? 1: Creating backup copies across AWS accounts - AWS Backup

? 2: Using AWS Backup with AWS Organizations - AWS Backup

#### NEW QUESTION 53

A company manages multiple AWS accounts in AWS Organizations. The company's security policy states that AWS account root user credentials for member accounts must not be used. The company monitors access to the root user credentials.

A recent alert shows that the root user in a member account launched an Amazon EC2 instance. A DevOps engineer must create an SCP at the organization's root level that will prevent the root user in member accounts from making any AWS service API calls.

Which SCP will meet these requirements?

A)



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
      }
    }
  ]
}
```

B)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Principal": { "AWS": "arn:aws:iam::*:root" }
    }
  ]
}
```

C)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
      }
    }
  ]
}
```

D)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Principal": "root"
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

**NEW QUESTION 58**

An application running on a set of Amazon EC2 instances in an Auto Scaling group requires a configuration file to operate. The instances are created and maintained with AWS CloudFormation. A DevOps engineer wants the instances to have the latest configuration file when launched and wants changes to the configuration file to be reflected on all the instances with a minimal delay when the CloudFormation template is updated. Company policy requires that application configuration files be maintained along with AWS infrastructure configuration files in source control. Which solution will accomplish this?

- A. In the CloudFormation template add an AWS Config rule
- B. Place the configuration file content in the rule's InputParameters property and set the Scope property to the EC2 Auto Scaling group
- C. Add an AWS Systems Manager Resource Data Sync resource to the template to poll for updates to the configuration.
- D. In the CloudFormation template add an EC2 launch template resource
- E. Place the configuration file content in the launch template
- F. Configure the cfn-init script to run when the instance is launched and configure the cfn-hup script to poll for updates to the configuration.
- G. In the CloudFormation template add an EC2 launch template resource
- H. Place the configuration file content in the launch template
- I. Add an AWS Systems Manager Resource Data Sync resource to the template to poll for updates to the configuration.
- J. In the CloudFormation template add CloudFormation intrinsic metadata
- K. Place the configuration file content in the metadata
- L. Configure the cfn-init script to run when the instance is launched and configure the cfn-hup script to poll for updates to the configuration.

**Answer: D**

**Explanation:**

Use the AWS::CloudFormation::Init type to include metadata on an Amazon EC2 instance for the cfn-init helper script. If your template calls the cfn-init script, the script looks for resource metadata rooted in the AWS::CloudFormation::Init metadata key. Reference: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-init.html>

**NEW QUESTION 60**

A development team wants to use AWS CloudFormation stacks to deploy an application. However, the developer IAM role does not have the required permissions to provision the resources that are specified in the AWS CloudFormation template. A DevOps engineer needs to implement a solution that allows the developers to deploy the stacks. The solution must follow the principle of least privilege. Which solution will meet these requirements?

- A. Create an IAM policy that allows the developers to provision the required resource
- B. Attach the policy to the developer IAM role.
- C. Create an IAM policy that allows full access to AWS CloudFormation
- D. Attach the policy to the developer IAM role.
- E. Create an AWS CloudFormation service role that has the required permission
- F. Grant the developer IAM role a cloudformation:\* action
- G. Use the new service role during stack deployments.
- H. Create an AWS CloudFormation service role that has the required permission
- I. Grant the developer IAM role the iam:PassRole permission
- J. Use the new service role during stack deployments.

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-service-role.html>

**NEW QUESTION 62**

An online retail company based in the United States plans to expand its operations to Europe and Asia in the next six months. Its product currently runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. All data is stored in an Amazon Aurora database instance.

When the product is deployed in multiple regions, the company wants a single product catalog across all regions, but for compliance purposes, its customer information and purchases must be kept in each region.

How should the company meet these requirements with the LEAST amount of application changes?

- A. Use Amazon Redshift for the product catalog and Amazon DynamoDB tables for the customer information and purchases.
- B. Use Amazon DynamoDB global tables for the product catalog and regional tables for the customer information and purchases.
- C. Use Aurora with read replicas for the product catalog and additional local Aurora instances in each region for the customer information and purchases.
- D. Use Aurora for the product catalog and Amazon DynamoDB global tables for the customer information and purchases.

**Answer: C**

**NEW QUESTION 67**

A company must encrypt all AMIs that the company shares across accounts. A DevOps engineer has access to a source account where an unencrypted custom AMI has been built. The DevOps engineer also has access to a target account where an Amazon EC2 Auto Scaling group will launch EC2 instances from the AMI. The DevOps engineer must share the AMI with the target account.

The company has created an AWS Key Management Service (AWS KMS) key in the source account.

Which additional steps should the DevOps engineer perform to meet the requirements? (Choose three.)

- A. In the source account, copy the unencrypted AMI to an encrypted AMI
- B. Specify the KMS key in the copy action.
- C. In the source account, copy the unencrypted AMI to an encrypted AMI
- D. Specify the default Amazon Elastic Block Store (Amazon EBS) encryption key in the copy action.
- E. In the source account, create a KMS grant that delegates permissions to the Auto Scaling group service-linked role in the target account.
- F. In the source account, modify the key policy to give the target account permissions to create a grant
- G. In the target account, create a KMS grant that delegates permissions to the Auto Scaling group service-linked role.
- H. In the source account, share the unencrypted AMI with the target account.
- I. In the source account, share the encrypted AMI with the target account.

**Answer:** ADF

**Explanation:**

The Auto Scaling group service-linked role must have a specific grant in the source account in order to decrypt the encrypted AMI. This is because the service-linked role does not have permissions to assume the default IAM role in the source account. The following steps are required to meet the requirements:

? In the source account, copy the unencrypted AMI to an encrypted AMI. Specify the KMS key in the copy action.

? In the source account, create a KMS grant that delegates permissions to the Auto Scaling group service-linked role in the target account.

? In the source account, share the encrypted AMI with the target account.

? In the target account, attach the KMS grant to the Auto Scaling group service-linked role.

The first three steps are the same as the steps that I described earlier. The fourth step is required to grant the Auto Scaling group service-linked role permissions to decrypt the AMI

in the target account.

**NEW QUESTION 71**

A developer is maintaining a fleet of 50 Amazon EC2 Linux servers. The servers are part of an Amazon EC2 Auto Scaling group, and also use Elastic Load Balancing for load balancing.

Occasionally, some application servers are being terminated after failing ELB HTTP health checks. The developer would like to perform a root cause analysis on the issue, but before being able to access application logs, the server is terminated.

How can log collection be automated?

A. Use Auto Scaling lifecycle hooks to put instances in a Pending:Wait stat

B. Create an Amazon CloudWatch alarm for EC2 Instance Terminate Successful and trigger an AWS Lambda function that invokes an SSM Run Command script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

C. Use Auto Scaling lifecycle hooks to put instances in a Terminating:Wait stat

D. Create an AWS Config rule for EC2 Instance-terminate Lifecycle Action and trigger a step function that invokes a script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

E. Use Auto Scaling lifecycle hooks to put instances in a Terminating:Wait stat

F. Create an Amazon CloudWatch subscription filter for EC2 Instance Terminate Successful and trigger a CloudWatch agent that invokes a script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

G. Use Auto Scaling lifecycle hooks to put instances in a Terminating:Wait stat

H. Create an Amazon EventBridge rule for EC2 Instance-terminate Lifecycle Action and trigger an AWS Lambda function that invokes an SSM Run Command script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

**Answer:** D

**Explanation:**

<https://blog.fourninecloud.com/auto-scaling-lifecycle-hooks-to-export-server-logs-when-instance-terminating-58e06d7c0d6a>

**NEW QUESTION 75**

A global company manages multiple AWS accounts by using AWS Control Tower. The company hosts internal applications and public applications.

Each application team in the company has its own AWS account for application hosting. The accounts are consolidated in an organization in AWS Organizations.

One of the AWS Control Tower member accounts serves as a centralized DevOps account with CI/CD pipelines that application teams use to deploy applications to their respective target AWS accounts. An IAM role for deployment exists in the centralized DevOps account.

An application team is attempting to deploy its application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in an application AWS account. An IAM role for deployment exists in the application AWS account. The deployment is through an AWS CodeBuild project that is set up in the centralized DevOps account. The CodeBuild project uses an IAM service role for CodeBuild. The deployment is failing with an Unauthorized error during attempts to connect to the cross-account EKS cluster from CodeBuild.

Which solution will resolve this error?

A. Configure the application account's deployment IAM role to have a trust relationship with the centralized DevOps account

B. Configure the trust relationship to allow the sts:AssumeRole action

C. Configure the application account's deployment IAM role to have the required access to the EKS cluster

D. Configure the EKS cluster aws-auth ConfigMap to map the role to the appropriate system permissions.

E. Configure the centralized DevOps account's deployment IAM role to have a trust relationship with the application account

F. Configure the trust relationship to allow the sts:AssumeRole action

G. Configure the centralized DevOps account's deployment IAM role to allow the required access to CodeBuild.

H. Configure the centralized DevOps account's deployment IAM role to have a trust relationship with the application account

I. Configure the trust relationship to allow the sts:AssumeRoleWithSAML action

J. Configure the centralized DevOps account's deployment IAM role to allow the required access to CodeBuild.

K. Configure the application account's deployment IAM role to have a trust relationship with the AWS Control Tower management account

L. Configure the trust relationship to allow the sts:AssumeRole action

M. Configure the application account's deployment IAM role to have the required access to the EKS cluster

N. Configure the EKS cluster aws-auth ConfigMap to map the role to the appropriate system permissions.

**Answer:** A

**Explanation:**

In the source AWS account, the IAM role used by the CI/CD pipeline should have permissions to access the source code repository, build artifacts, and any other resources required for the build process. In the destination AWS accounts, the IAM role used for deployment should have permissions to access the AWS resources required for deploying the application, such as EC2 instances, RDS databases, S3 buckets, etc. The exact permissions required will depend on the specific resources being used by the application. The IAM role used for deployment in the destination accounts should also have permissions to assume the IAM role for deployment in the centralized DevOps account. This is typically done using an IAM role trust policy that allows the destination account to assume the DevOps account role.

**NEW QUESTION 80**

A DevOps engineer manages a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group across multiple Availability Zones. The engineer needs to implement a deployment strategy that:

Launches a second fleet of instances with the same capacity as the original fleet. Maintains the original fleet unchanged while the second fleet is launched.

Transitions traffic to the second fleet when the second fleet is fully deployed. Terminates the original fleet automatically 1 hour after transition.

Which solution will satisfy these requirements?



- A. Use an AWS CloudFormation template with a retention policy for the ALB set to 1 hour
- B. Update the Amazon Route 53 record to reflect the new ALB.
- C. Use two AWS Elastic Beanstalk environments to perform a blue/green deployment from the original environment to the new one
- D. Create an application version lifecycle policy to terminate the original environment in 1 hour.
- E. Use AWS CodeDeploy with a deployment group configured with a blue/green deployment configuration. Select the option Terminate the original instances in the deployment group with a waiting period of 1 hour.
- F. Use AWS Elastic Beanstalk with the configuration set to Immutable
- G. Create an extension using the Resources key that sets the deletion policy of the ALB to 1 hour, and deploy the application.

**Answer: C**

**Explanation:**

[https://docs.aws.amazon.com/codedeploy/latest/APIReference/API\\_BlueInstanceTerminationOption.html](https://docs.aws.amazon.com/codedeploy/latest/APIReference/API_BlueInstanceTerminationOption.html)  
The original revision termination settings are configured to wait 1 hour after traffic has been rerouted before terminating the blue task set.  
<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/deployment-type-bluegreen.html>

**NEW QUESTION 84**

A company wants to use AWS CloudFormation for infrastructure deployment. The company has strict tagging and resource requirements and wants to limit the deployment to two Regions. Developers will need to deploy multiple versions of the same application. Which solution ensures resources are deployed in accordance with company policy?

- A. Create AWS Trusted Advisor checks to find and remediate unapproved CloudFormation StackSets.
- B. Create a CloudFormation drift detection operation to find and remediate unapproved CloudFormation StackSets.
- C. Create CloudFormation StackSets with approved CloudFormation templates.
- D. Create AWS Service Catalog products with approved CloudFormation templates.

**Answer: D**

**Explanation:**

Service Catalog uses stacksets and can enforce tag and restrict resources. AWS Customer case with tag enforcement  
<https://aws.amazon.com/ko/blogs/apn/enforce-centralized-tag-compliance-using-aws-service-catalog-amazon-dynamodb-aws-lambda-and-amazon-cloudwatch-events/> And Youtube video showing how to restrict resources per user with portfolio <https://www.youtube.com/watch?v=LzvhTcqyog>

**NEW QUESTION 88**

The security team depends on AWS CloudTrail to detect sensitive security issues in the company's AWS account. The DevOps engineer needs a solution to automatically remediate CloudTrail being turned off in an AWS account. What solution ensures the LEAST amount of downtime for the CloudTrail log deliveries?

- A. Create an Amazon EventBridge rule for the CloudTrail StopLogging event
- B. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on the ARN of the resource in which StopLogging was called
- C. Add the Lambda function ARN as a target to the EventBridge rule.
- D. Deploy the AWS-managed CloudTrail-enabled AWS Config rule set with a periodic interval to 1 hour
- E. Create an Amazon EventBridge rule for AWS Config rules compliance change
- F. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on the ARN of the resource in which StopLogging was called
- G. Add the Lambda function ARN as a target to the EventBridge rule.
- H. Create an Amazon EventBridge rule for a scheduled event every 5 minutes
- I. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on a CloudTrail trail in the AWS account
- J. Add the Lambda function ARN as a target to the EventBridge rule.
- K. Launch a t2.nano instance with a script running every 5 minutes that uses the AWS SDK to query CloudTrail in the current account
- L. If the CloudTrail trail is disabled, have the script re-enable the trail.

**Answer: A**

**Explanation:**

<https://aws.amazon.com/blogs/mt/monitor-changes-and-auto-enable-logging-in-aws-cloudtrail/>

**NEW QUESTION 89**

A DevOps engineer is building a multistage pipeline with AWS CodePipeline to build, verify, stage, test, and deploy an application. A manual approval stage is required between the test stage and the deploy stage. The development team uses a custom chat tool with webhook support that requires near-real-time notifications.

How should the DevOps engineer configure status updates for pipeline activity and approval requests to post to the chat tool?

- A. Create an Amazon CloudWatch Logs subscription that filters on CodePipeline Pipeline Execution State Change
- B. Publish subscription events to an Amazon Simple Notification Service (Amazon SNS) topic
- C. Subscribe the chat webhook URL to the SNS topic, and complete the subscription validation.
- D. Create an AWS Lambda function that is invoked by AWS CloudTrail event
- E. When a CodePipeline Pipeline Execution State Change event is detected, send the event details to the chat webhook URL.
- F. Create an Amazon EventBridge rule that filters on CodePipeline Pipeline Execution State Change
- G. Publish the events to an Amazon Simple Notification Service (Amazon SNS) topic
- H. Create an AWS Lambda function that sends event details to the chat webhook URL
- I. Subscribe the function to the SNS topic.
- J. Modify the pipeline code to send the event details to the chat webhook URL at the end of each stage
- K. Parameterize the URL so that each pipeline can send to a different URL based on the pipeline environment.

**Answer: C**

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/sns-lambda-webhooks-chime-slack-teams/>

#### NEW QUESTION 94

A company uses AWS Storage Gateway in file gateway mode in front of an Amazon S3 bucket that is used by multiple resources. In the morning when business begins, users do not see the objects processed by a third party the previous evening. When a DevOps engineer looks directly at the S3 bucket, the data is there, but it is missing in Storage Gateway.

Which solution ensures that all the updated third-party files are available in the morning?

- A. Configure a nightly Amazon EventBridge event to invoke an AWS Lambda function to run the RefreshCache command for Storage Gateway.
- B. Instruct the third party to put data into the S3 bucket using AWS Transfer for SFTP.
- C. Modify Storage Gateway to run in volume gateway mode.
- D. Use S3 Same-Region Replication to replicate any changes made directly in the S3 bucket to Storage Gateway.

**Answer:** A

#### Explanation:

[https://docs.aws.amazon.com/storagegateway/latest/APIReference/API\\_RefreshCache.html](https://docs.aws.amazon.com/storagegateway/latest/APIReference/API_RefreshCache.html) " It only updates the cached inventory to reflect changes in the inventory of the objects in the S3 bucket. This operation is only supported in the S3 File Gateway types."

#### NEW QUESTION 97

A company uses AWS Directory Service for Microsoft Active Directory as its identity provider (IdP). The company requires all infrastructure to be defined and deployed by AWS CloudFormation.

A DevOps engineer needs to create a fleet of Windows-based Amazon EC2 instances to host an application. The DevOps engineer has created a CloudFormation template that contains an EC2 launch template, IAM role, EC2 security group, and EC2 Auto Scaling group. The DevOps engineer must implement a solution that joins all EC2 instances to the domain of the AWS Managed Microsoft AD directory.

Which solution will meet these requirements with the MOST operational efficiency?

- A. In the CloudFormation template, create an AWS::SSM::Document resource that joins the EC2 instance to the AWS Managed Microsoft AD domain by using the parameters for the existing director
- B. Update the launch template to include the SSMAssociation property to use the new SSM document
- C. Attach the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess AWS managed policies to the IAM role that the EC2 instances use.
- D. In the CloudFormation template, update the launch template to include specific tags that propagate on launch
- E. Create an AWS::SSM::Association resource to associate the AWS- JoinDirectoryServiceDomain Automation runbook with the EC2 instances that have the specified tag
- F. Define the required parameters to join the AWS Managed Microsoft AD director
- G. Attach the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess AWS managed policies to the IAM role that the EC2 instances use.
- H. Store the existing AWS Managed Microsoft AD domain connection details in AWS Secrets Manager
- I. In the CloudFormation template, create an AWS::SSM::Association resource to associate the AWS-CreateManagedWindowsInstanceWithApproval Automation runbook with the EC2 Auto Scaling group
- J. Pass the ARNs for the parameters from Secrets Manager to join the domain
- K. Attach the AmazonSSMDirectoryServiceAccess and SecretsManagerReadWrite AWS managed policies to the IAM role that the EC2 instances use.
- L. Store the existing AWS Managed Microsoft AD domain administrator credentials in AWS Secrets Manager
- M. In the CloudFormation template, update the EC2 launch template to include user data
- N. Configure the user data to pull the administrator credentials from Secrets Manager and to join the AWS Managed Microsoft AD domain
- O. Attach the AmazonSSMManagedInstanceCore and SecretsManagerReadWrite AWS managed policies to the IAM role that the EC2 instances use.

**Answer:** B

#### Explanation:

To meet the requirements, the DevOps engineer needs to create a solution that joins all EC2 instances to the domain of the AWS Managed Microsoft AD directory with the most operational efficiency. The DevOps engineer can use AWS Systems Manager Automation to automate the domain join process using an existing runbook called AWS- JoinDirectoryServiceDomain. This runbook can join Windows instances to an AWS Managed Microsoft AD or Simple AD directory by using PowerShell commands. The DevOps engineer can create an AWS::SSM::Association resource in the CloudFormation template to associate the runbook with the EC2 instances that have specific tags. The tags can be defined in the launch template and propagated on launch to the EC2 instances. The DevOps engineer can also define the required parameters for the runbook, such as the directory ID, directory name, and organizational unit. The DevOps engineer can attach the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess AWS managed policies to the IAM role that the EC2 instances use. These policies grant the necessary permissions for Systems Manager and Directory Service operations.

#### NEW QUESTION 100

A company's security team requires that all external Application Load Balancers (ALBs) and Amazon API Gateway APIs are associated with AWS WAF web ACLs. The company

has hundreds of AWS accounts, all of which are included in a single organization in AWS Organizations. The company has configured AWS Config for the organization. During an audit, the company finds some externally facing ALBs that are not associated with AWS WAF web ACLs.

Which combination of steps should a DevOps engineer take to prevent future violations? (Choose two.)

- A. Delegate AWS Firewall Manager to a security account.
- B. Delegate Amazon GuardDuty to a security account.
- C. Create an AWS Firewall Manager policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
- D. Create an Amazon GuardDuty policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
- E. Configure an AWS Config managed rule to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.

**Answer:** AC

#### Explanation:

If instead you want to automatically apply the policy to existing in-scope resources, choose Auto remediate any noncompliant resources. This option creates a web ACL in each applicable account within the AWS organization and associates the web ACL with the resources in the accounts. When you choose Auto remediate any noncompliant resources, you can also choose to remove existing web ACL associations from in-scope resources, for the web ACLs that aren't managed by another active Firewall Manager policy. If you choose this option, Firewall Manager first associates the policy's web ACL with the resources, and then removes the prior associations. If a resource has an association with another web ACL that's managed by a different active Firewall Manager policy, this choice doesn't affect that association.

#### NEW QUESTION 105

A company is using AWS to run digital workloads. Each application team in the company has its own AWS account for application hosting. The accounts are consolidated in an organization in AWS Organizations. The company wants to enforce security standards across the entire organization. To avoid noncompliance because of security misconfiguration, the company has enforced the use of AWS CloudFormation. A production support team can modify resources in the production environment by using the AWS Management Console to troubleshoot and resolve application-related issues. A DevOps engineer must implement a solution to identify in near real time any AWS service misconfiguration that results in noncompliance. The solution must automatically remediate the issue within 15 minutes of identification. The solution also must track noncompliant resources and events in a centralized dashboard with accurate timestamps. Which solution will meet these requirements with the LEAST development overhead?

- A. Use CloudFormation drift detection to identify noncompliant resource
- B. Use drift detection events from CloudFormation to invoke an AWS Lambda function for remediation
- C. Configure the Lambda function to publish logs to an Amazon CloudWatch Logs log group
- D. Configure an Amazon CloudWatch dashboard to use the log group for tracking.
- E. Turn on AWS CloudTrail in the AWS account
- F. Analyze CloudTrail logs by using Amazon Athena to identify noncompliant resource
- G. Use AWS Step Functions to track query results on Athena for drift detection and to invoke an AWS Lambda function for remediation
- H. For tracking, set up an Amazon QuickSight dashboard that uses Athena as the data source.
- I. Turn on the configuration recorder in AWS Config in all the AWS accounts to identify noncompliant resource
- J. Enable AWS Security Hub with the `~no-enable-default-standards` option in all the AWS account
- K. Set up AWS Config managed rules and custom rule
- L. Set up automatic remediation by using AWS Config conformance pack
- M. For tracking, set up a dashboard on Security Hub in a designated Security Hub administrator account.
- N. Turn on AWS CloudTrail in the AWS account
- O. Analyze CloudTrail logs by using Amazon CloudWatch Logs to identify noncompliant resource
- P. Use CloudWatch Logs filters for drift detection
- Q. Use Amazon EventBridge to invoke the Lambda function for remediation
- R. Stream filtered CloudWatch logs to Amazon OpenSearch Service
- S. Set up a dashboard on OpenSearch Service for tracking.

**Answer: C**

**Explanation:**

The best solution is to use AWS Config and AWS Security Hub to identify and remediate noncompliant resources across multiple AWS accounts. AWS Config enables continuous monitoring of the configuration of AWS resources and evaluates them against desired configurations. AWS Config can also automatically remediate noncompliant resources by using conformance packs, which are a collection of AWS Config rules and remediation actions that can be deployed as a single entity. AWS Security Hub provides a comprehensive view of the security posture of AWS accounts and resources. AWS Security Hub can aggregate and normalize the findings from AWS Config and other AWS services, as well as from partner solutions. AWS Security Hub can also be used to create a dashboard for tracking noncompliant resources and events in a centralized location.

The other options are not optimal because they either require more development overhead, do not provide near real time detection and remediation, or do not provide a centralized dashboard for tracking.

Option A is not optimal because CloudFormation drift detection is not a near real time solution. Drift detection has to be manually initiated on each stack or resource, or scheduled using a cron expression. Drift detection also does not provide remediation

actions, so a custom Lambda function has to be developed and invoked. CloudWatch Logs and dashboard can be used for tracking, but they do not provide a comprehensive view of the security posture of the AWS accounts and resources.

Option B is not optimal because CloudTrail logs analysis using Athena is not a near real time solution. Athena queries have to be manually run or scheduled using a cron expression. Athena also does not provide remediation actions, so a custom Lambda function has to be developed and invoked. Step Functions can be used to orchestrate the query and remediation workflow, but it adds more complexity and cost. QuickSight dashboard can be used for tracking, but it does not provide a comprehensive view of the security posture of the AWS accounts and resources.

Option D is not optimal because CloudTrail logs analysis using CloudWatch Logs is not a near real time solution. CloudWatch Logs filters have to be manually created or updated for each resource type and configuration change. CloudWatch Logs also does not provide remediation actions, so a custom Lambda function has to be developed and invoked. EventBridge can be used to trigger the Lambda function, but it adds more complexity and cost. OpenSearch Service dashboard can be used for tracking, but it does not provide a comprehensive view of the security posture of the AWS accounts and resources. References:

? AWS Config conformance packs

? Introducing AWS Config conformance packs

? Managing conformance packs across all accounts in your organization

**NEW QUESTION 109**

A company plans to use Amazon CloudWatch to monitor its Amazon EC2 instances. The company needs to stop EC2 instances when the average of the NetworkPacketsIn metric is less than 5 for at least 3 hours in a 12-hour time window. The company must evaluate the metric every hour. The EC2 instances must continue to run if there is missing data for the NetworkPacketsIn metric during the evaluation period.

A DevOps engineer creates a CloudWatch alarm for the NetworkPacketsIn metric. The DevOps engineer configures a threshold value of 5 and an evaluation period of 1 hour.

Which set of additional actions should the DevOps engineer take to meet these requirements?

- A. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as breaching the threshold
- B. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.
- C. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as not breaching the threshold
- D. Add an EC2 action to stop the instance when the alarm enters the ALARM state.
- E. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as breaching the threshold
- F. Add an EC2 action to stop the instance when the alarm enters the ALARM state.
- G. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as not breaching the threshold
- H. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.

**Answer: B**

**Explanation:**

To meet the requirements, the DevOps engineer needs to configure the CloudWatch alarm to stop the EC2 instances when the average of the NetworkPacketsIn metric is less than 5 for at least 3 hours in a 12-hour time window. This means that the alarm should trigger when 3 out of 12 datapoints are below the threshold of 5. The alarm should also treat missing data as not breaching the threshold, so that the EC2 instances continue to run if there is no data for the metric during the evaluation period. The DevOps engineer can add an EC2 action to stop the instance when the alarm enters the ALARM state, which is a built-in action type for CloudWatch alarms.



#### NEW QUESTION 114

A DevOps engineer is setting up a container-based architecture. The engineer has decided to use AWS CloudFormation to automatically provision an Amazon ECS cluster and an Amazon EC2 Auto Scaling group to launch the EC2 container instances. After successfully creating the CloudFormation stack, the engineer noticed that, even though the ECS cluster and the EC2 instances were created successfully and the stack finished the creation, the EC2 instances were associating with a different cluster.

How should the DevOps engineer update the CloudFormation template to resolve this issue?

- A. Reference the EC2 instances in the AWS: ECS: Cluster resource and reference the ECS cluster in the AWS: ECS: Service resource.
- B. Reference the ECS cluster in the AWS: AutoScaling: LaunchConfiguration resource of the UserData property.
- C. Reference the ECS cluster in the AWS:EC2: Instance resource of the UserData property.
- D. Reference the ECS cluster in the AWS: CloudFormation: CustomResource resource to trigger an AWS Lambda function that registers the EC2 instances with the appropriate ECS cluster.

**Answer: B**

#### Explanation:

The UserData property of the AWS: AutoScaling: LaunchConfiguration resource can be used to specify a script that runs when the EC2 instances are launched. This script can include the ECS cluster name as an environment variable for the ECS agent running on the EC2 instances. This way, the EC2 instances will register with the correct ECS cluster. Option A is incorrect because the AWS: ECS: Cluster resource does not have a property to reference the EC2 instances. Option C is incorrect because the EC2 instances are launched by the Auto Scaling group, not by the AWS: EC2: Instance resource. Option D is incorrect because using a custom resource and a Lambda function is unnecessary and overly complex for this scenario. References: AWS::AutoScaling::LaunchConfiguration, Amazon ECS Container Agent Configuration

#### NEW QUESTION 118

A company has an on-premises application that is written in Go. A DevOps engineer must move the application to AWS. The company's development team wants to enable blue/green deployments and perform A/B testing.

Which solution will meet these requirements?

- A. Deploy the application on an Amazon EC2 instance, and create an AMI of the instance
- B. Use the AMI to create an automatic scaling launch configuration that is used in an Auto Scaling group
- C. Use Elastic Load Balancing to distribute traffic
- D. When changes are made to the application, a new AMI will be created, which will initiate an EC2 instance refresh.
- E. Use Amazon Lightsail to deploy the application
- F. Store the application in a zipped format in an Amazon S3 bucket
- G. Use this zipped version to deploy new versions of the application to Lightsail
- H. Use Lightsail deployment options to manage the deployment.
- I. Use AWS CodeArtifact to store the application code
- J. Use AWS CodeDeploy to deploy the application to a fleet of Amazon EC2 instances
- K. Use Elastic Load Balancing to distribute the traffic to the EC2 instance
- L. When making changes to the application, upload a new version to CodeArtifact and create a new CodeDeploy deployment.
- M. Use AWS Elastic Beanstalk to host the application
- N. Store a zipped version of the application in Amazon S3. Use that location to deploy new versions of the application
- O. Use Elastic Beanstalk to manage the deployment options.

**Answer: D**

#### Explanation:

<https://aws.amazon.com/quickstart/architecture/blue-green-deployment/>

#### NEW QUESTION 120

A Company uses AWS CodeCommit for source code control. Developers apply their changes to various feature branches and create pull requests to move those changes to the main branch when the changes are ready for production.

The developers should not be able to push changes directly to the main branch. The company applied the AWSCodeCommitPowerUser managed policy to the developers' IAM role, and now these developers can push changes to the main branch directly on every repository in the AWS account.

What should the company do to restrict the developers' ability to push changes to the main branch directly?

- A. Create an additional policy to include a Deny rule for the GitPush and PutFile action
- B. Include a restriction for the specific repositories in the policy statement with a condition that references the main branch.
- C. Remove the IAM policy, and add an AWSCodeCommitReadOnly managed policy
- D. Add an Allow rule for the GitPush and PutFile actions for the specific repositories in the policy statement with a condition that references the main branch.
- E. Modify the IAM policy Include a Deny rule for the GitPush and PutFile actions for the specific repositories in the policy statement with a condition that references the main branch.
- F. Create an additional policy to include an Allow rule for the GitPush and PutFile action
- G. Include a restriction for the specific repositories in the policy statement with a condition that references the feature branches.

**Answer: A**

#### Explanation:

By default, the AWSCodeCommitPowerUser managed policy allows users to push changes to any branch in any repository in the AWS account. To restrict the developers' ability to push changes to the main branch directly, an additional policy is needed that explicitly denies these actions for the main branch. The Deny rule should be included in a policy statement that targets the specific repositories and includes a condition that references the main branch. The policy statement should look something like this:

```
{
  "Effect": "Deny", "Action": [ "codecommit:GitPush", "codecommit:PutFile"
],
  "Resource": "arn:aws:codecommit:<region>:<account-id>:<repository-name>", "Condition": {
    "StringEqualsIfExists": { "codecommit:References": [ "refs/heads/main"
]
}
```

```
}  
}  
}
```

**NEW QUESTION 123**

A company has developed a serverless web application that is hosted on AWS. The application consists of Amazon S3, Amazon API Gateway, several AWS Lambda functions, and an Amazon RDS for MySQL database. The company is using AWS CodeCommit to store the source code. The source code is a combination of AWS Serverless Application Model (AWS SAM) templates and Python code.

A security audit and penetration test reveal that user names and passwords for authentication to the database are hardcoded within CodeCommit repositories. A DevOps engineer must implement a solution to automatically detect and prevent hardcoded secrets.

What is the MOST secure solution that meets these requirements?

- A. Enable Amazon CodeGuru Profile
- B. Decorate the handler function with `@with_lambda_profiler()`. Manually review the recommendation report
- C. Write the secret to AWS Systems Manager Parameter Store as a secure string
- D. Update the SAM templates and the Python code to pull the secret from Parameter Store.
- E. Associate the CodeCommit repository with Amazon CodeGuru Reviewer
- F. Manually check the code review for any recommendation
- G. Choose the option to protect the secret
- H. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.
- I. Enable Amazon CodeGuru Profile
- J. Decorate the handler function with `@with_lambda_profiler()`. Manually review the recommendation report
- K. Choose the option to protect the secret
- L. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.
- M. Associate the CodeCommit repository with Amazon CodeGuru Reviewer
- N. Manually check the code review for any recommendation
- O. Write the secret to AWS Systems Manager Parameter Store as a string
- P. Update the SAM templates and the Python code to pull the secret from Parameter Store.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-amazon-codeguru-reviewer.html>

**NEW QUESTION 127**

A space exploration company receives telemetry data from multiple satellites. Small packets of data are received through Amazon API Gateway and are placed directly into an Amazon Simple Queue Service (Amazon SQS) standard queue. A custom application is subscribed to the queue and transforms the data into a standard format.

Because of inconsistencies in the data that the satellites produce, the application is occasionally unable to transform the data. In these cases, the messages remain in the SQS queue. A DevOps engineer must develop a solution that retains the failed messages and makes them available to scientists for review and future processing.

Which solution will meet these requirements?

- A. Configure AWS Lambda to poll the SQS queue and invoke a Lambda function to check whether the queue messages are valid
- B. If validation fails, send a copy of the data that is not valid to an Amazon S3 bucket so that the scientists can review and correct the data
- C. When the data is corrected, amend the message in the SQS queue by using a replay Lambda function with the corrected data.
- D. Convert the SQS standard queue to an SQS FIFO queue
- E. Configure AWS Lambda to poll the SQS queue every 10 minutes by using an Amazon EventBridge schedule
- F. Invoke the Lambda function to identify any messages with a `SentTimestamp` value that is older than 5 minutes, push the data to the same location as the application's output location, and remove the messages from the queue.
- G. Create an SQS dead-letter queue
- H. Modify the existing queue by including a redrive policy that sets the `MaximumReceives` setting to 1 and sets the dead-letter queue ARN to the ARN of the newly created queue
- I. Instruct the scientists to use the dead-letter queue to review the data that is not valid
- J. Reprocess this data at a later time.
- K. Configure API Gateway to send messages to different SQS virtual queues that are named for each of the satellites
- L. Update the application to use a new virtual queue for any data that it cannot transform, and send the message to the new virtual queue
- M. Instruct the scientists to use the virtual queue to review the data that is not valid
- N. Reprocess this data at a later time.

**Answer: C**

**Explanation:**

Create an SQS dead-letter queue. Modify the existing queue by including a redrive policy that sets the `MaximumReceives` setting to 1 and sets the dead-letter queue ARN to the ARN of the newly created queue. Instruct the scientists to use the dead-letter queue to review the data that is not valid. Reprocess this data at a later time.

**NEW QUESTION 129**

A company runs an application on Amazon EC2 instances. The company uses a series of AWS CloudFormation stacks to define the application resources. A developer performs updates by building and testing the application on a laptop and then uploading the build output and CloudFormation stack templates to Amazon S3. The developer's peers review the changes before the developer performs the CloudFormation stack update and installs a new version of the application onto the EC2 instances.

The deployment process is prone to errors and is time-consuming when the developer updates each EC2 instance with the new application. The company wants to automate as much of the application deployment process as possible while retaining a final manual approval step before the modification of the application or resources.

The company already has moved the source code for the application and the CloudFormation templates to AWS CodeCommit. The company also has created an AWS CodeBuild project to build and test the application.

Which combination of steps will meet the company's requirements? (Choose two.)

- A. Create an application group and a deployment group in AWS CodeDeploy
- B. Install the CodeDeploy agent on the EC2 instances.

- C. Create an application revision and a deployment group in AWS CodeDeploy
- D. Create an environment in CodeDeploy
- E. Register the EC2 instances to the CodeDeploy environment.
- F. Use AWS CodePipeline to invoke the CodeBuild job, run the CloudFormation update, and pause for a manual approval step
- G. After approval, start the AWS CodeDeploy deployment.
- H. Use AWS CodePipeline to invoke the CodeBuild job, create CloudFormation change sets for each of the application stacks, and pause for a manual approval step
- I. After approval, run the CloudFormation change sets and start the AWS CodeDeploy deployment.
- J. Use AWS CodePipeline to invoke the CodeBuild job, create CloudFormation change sets for each of the application stacks, and pause for a manual approval step
- K. After approval, start the AWS CodeDeploy deployment.

**Answer:** AD

**Explanation:**

A- <https://docs.aws.amazon.com/codedeploy/latest/userguide/codedeploy-agent.html> D - This option correctly utilizes AWS CodePipeline to invoke the CodeBuild job and create CloudFormation change sets. It adds a manual approval step before executing the change sets and starting the AWS CodeDeploy deployment. This ensures that the deployment process is automated while retaining the final manual approval step.

**NEW QUESTION 133**

A DevOps engineer is planning to deploy a Ruby-based application to production. The application needs to interact with an Amazon RDS for MySQL database and should have automatic scaling and high availability. The stored data in the database is critical and should persist regardless of the state of the application stack. The DevOps engineer needs to set up an automated deployment strategy for the application with automatic rollbacks. The solution also must alert the application team when a deployment fails.

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

- A. Deploy the application on AWS Elastic Beanstalk
- B. Deploy an Amazon RDS for MySQL DB instance as part of the Elastic Beanstalk configuration.
- C. Deploy the application on AWS Elastic Beanstalk
- D. Deploy a separate Amazon RDS for MySQL DB instance outside of Elastic Beanstalk.
- E. Configure a notification email address that alerts the application team in the AWS Elastic Beanstalk configuration.
- F. Configure an Amazon EventBridge rule to monitor AWS Health event
- G. Use an Amazon Simple Notification Service (Amazon SNS) topic as a target to alert the application team.
- H. Use the immutable deployment method to deploy new application versions.
- I. Use the rolling deployment method to deploy new application versions.

**Answer:** BDE

**Explanation:**

For deploying a Ruby-based application with requirements for interaction with an Amazon RDS for MySQL database, automatic scaling, high availability, and data persistence, the following steps will meet the requirements:

? B. Deploy the application on AWS Elastic Beanstalk. Deploy a separate Amazon RDS for MySQL DB instance outside of Elastic Beanstalk. This approach ensures that the database persists independently of the Elastic Beanstalk environment, which can be torn down and recreated without affecting the database<sup>123</sup>.

? E. Use the immutable deployment method to deploy new application versions. Immutable deployments provide a zero-downtime deployment method that ensures that if any part of the deployment process fails, the environment is rolled back to the original state automatically<sup>4</sup>.

? D. Configure an Amazon EventBridge rule to monitor AWS Health events. Use an Amazon Simple Notification Service (Amazon SNS) topic as a target to alert the application team. This setup allows for automated monitoring and alerting of the application team in case of deployment failures or other health events<sup>56</sup>.

References:

? AWS Elastic Beanstalk documentation on deploying Ruby applications<sup>1</sup>.

? AWS documentation on application auto-scaling<sup>7</sup>.

? AWS documentation on automated deployment strategies with automatic rollbacks and alerts<sup>456</sup>.

**NEW QUESTION 135**

A company is launching an application that stores raw data in an Amazon S3 bucket. Three applications need to access the data to generate reports. The data must be redacted differently for each application before the applications can access the data.

Which solution will meet these requirements?

- A. Create an S3 bucket for each application
- B. Configure S3 Same-Region Replication (SRR) from the raw data's S3 bucket to each application's S3 bucket
- C. Configure each application to consume data from its own S3 bucket.
- D. Create an Amazon Kinesis data stream
- E. Create an AWS Lambda function that is invoked by object creation events in the raw data's S3 bucket
- F. Program the Lambda function to redact data for each application
- G. Publish the data on the Kinesis data stream
- H. Configure each application to consume data from the Kinesis data stream.
- I. For each application, create an S3 access point that uses the raw data's S3 bucket as the destination
- J. Create an AWS Lambda function that is invoked by object creation events in the raw data's S3 bucket
- K. Program the Lambda function to redact data for each application
- L. Store the data in each application's S3 access point
- M. Configure each application to consume data from its own S3 access point.
- N. Create an S3 access point that uses the raw data's S3 bucket as the destination
- O. For each application, create an S3 Object Lambda access point that uses the S3 access point
- P. Configure the AWS Lambda function for each S3 Object Lambda access point to redact data when objects are retrieved
- Q. Configure each application to consume data from its own S3 Object Lambda access point.

**Answer:** D



**Explanation:**

? The best solution is to use S3 Object Lambda<sup>1</sup>, which allows you to add your own code to S3 GET, LIST, and HEAD requests to modify and process data as it is returned to an application<sup>2</sup>. This way, you can redact the data differently for each application without creating and storing multiple copies of the data or running proxies.

? The other solutions are less efficient or scalable because they require replicating the data to multiple buckets, streaming the data through Kinesis, or storing the data in S3 access points.

References: 1: Amazon S3 Features | Object Lambda | AWS 2: Transforming objects with S3 Object Lambda - Amazon Simple Storage Service

**NEW QUESTION 136**

A company's DevOps engineer is working in a multi-account environment. The company uses AWS Transit Gateway to route all outbound traffic through a network operations account. In the network operations account all account traffic passes through a firewall appliance for inspection before the traffic goes to an internet gateway.

The firewall appliance sends logs to Amazon CloudWatch Logs and includes event

severities of CRITICAL, HIGH, MEDIUM, LOW, and INFO. The security team wants to receive an alert if any CRITICAL events occur.

What should the DevOps engineer do to meet these requirements?

- A. Create an Amazon CloudWatch Synthetics canary to monitor the firewall stat
- B. If the firewall reaches a CRITICAL state or logs a CRITICAL event use a CloudWatch alarm to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe the security team's email address to the topic.
- C. Create an Amazon CloudWatch metric filter by using a search for CRITICAL events Publish a custom metric for the findin
- D. Use a CloudWatch alarm based on the custom metric to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic
- E. Subscribe the security team's email address to the topic.
- F. Enable Amazon GuardDuty in the network operations account
- G. Configure GuardDuty to monitor flow logs Create an Amazon EventBridge event rule that is invoked by GuardDuty events that are CRITICAL Define an Amazon Simple Notification Service (Amazon SNS) topic as a target Subscribe the security team's email address to the topic.
- H. Use AWS Firewall Manager to apply consistent policies across all account
- I. Create an Amazon
- J. EventBridge event rule that is invoked by Firewall Manager events that are CRITICAL Define an Amazon Simple Notification Service (Amazon SNS) topic as a target Subscribe the security team's email address to the topic.

**Answer: B**

**Explanation:**

"The firewall appliance sends logs to Amazon CloudWatch Logs and includes event severities of CRITICAL, HIGH, MEDIUM, LOW, and INFO"

**NEW QUESTION 139**

A company is using an Amazon Aurora cluster as the data store for its application. The Aurora cluster is configured with a single DB instance. The application performs read and write operations on the database by using the cluster's instance endpoint.

The company has scheduled an update to be applied to the cluster during an upcoming maintenance window. The cluster must remain available with the least possible interruption during the maintenance window.

What should a DevOps engineer do to meet these requirements?

- A. Add a reader instance to the Aurora cluster
- B. Update the application to use the Aurora cluster endpoint for write operation
- C. Update the Aurora cluster's reader endpoint for reads.
- D. Add a reader instance to the Aurora cluster
- E. Create a custom ANY endpoint for the cluster
- F. Update the application to use the Aurora cluster's custom ANY endpoint for read and write operations.
- G. Turn on the Multi-AZ option on the Aurora cluster
- H. Update the application to use the Aurora cluster endpoint for write operation
- I. Update the Aurora cluster's reader endpoint for reads.
- J. Turn on the Multi-AZ option on the Aurora cluster
- K. Create a custom ANY endpoint for the cluster
- L. Update the application to use the Aurora cluster's custom ANY endpoint for read and write operations.

**Answer: C**

**Explanation:**

To meet the requirements, the DevOps engineer should do the following:

? Turn on the Multi-AZ option on the Aurora cluster.

? Update the application to use the Aurora cluster endpoint for write operations.

? Update the Aurora cluster's reader endpoint for reads.

Turning on the Multi-AZ option will create a replica of the database in a different Availability Zone. This will ensure that the database remains available even if one of the Availability Zones is unavailable.

Updating the application to use the Aurora cluster endpoint for write operations will ensure that all writes are sent to both the primary and replica databases. This will ensure that the data is always consistent.

Updating the Aurora cluster's reader endpoint for reads will allow the application to read data from the replica database. This will improve the performance of the application during the maintenance window.

**NEW QUESTION 143**

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. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instance
- B. Configure the SNS topic to invoke the runbook.

- C. Create an AWS Lambda function that restarts the application on the instance
- D. Configure the Lambda function as an event destination of the SNS topic.
- E. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instance
- F. Create an AWS Lambda function to invoke the runboo
- G. Configure the Lambda function as an event destination of the SNS topic.
- H. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instance
- I. Configure an Amazon EventBridge rule that reacts when the CloudWatch alarm enters ALARM stat
- J. Specify the runbook as a target of the rule.

**Answer:** D

**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 147**

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 AWS CloudFormation template for the applicatio
- B. Define each Lambda function in the template by using the AWS::Lambda::Function resource typ
- C. In the template, include a version for the Lambda function by using the AWS::Lambda::Version resource typ
- D. Declare the CodeSha256 propert
- E. Configure an AWS::Lambda::Alias resource that references the latest version of the Lambda function.
- F. Create an AWS Serverless Application Model (AWS SAM) template for the applicatio
- G. Define each Lambda function in the template by using the AWS::Serverless::Function resource typ
- H. For each function, include configurations for the AutoPublishAlias property and the DeploymentPreference propert
- I. Configure the deployment configuration type to LambdaCanary10Percent10Minutes.
- J. Create an AWS CodeCommit repositor
- K. Create an AWS CodePipeline pipelin
- L. Use the CodeCommit repository in a new source stage that starts the pipelin
- M. Create an AWS CodeBuild project to deploy the AWS Serverless Application Model (AWS SAM) templat
- N. Upload the template and source code to the CodeCommit repositor
- O. In the CodeCommit repository, create a buildspec.yml file that includes the commands to build and deploy the SAM application.
- P. Create an AWS CodeCommit repositor
- Q. Create an AWS CodePipeline pipelin
- R. Use the CodeCommit repository in a new source stage that starts the pipelin
- S. Create an AWS CodeDeploy deployment group that is configured for canary deployments with a DeploymentPreference type of Canary10Percent10Minute
- T. Upload the AWS CloudFormation template and source code to the CodeCommit repositor
- . In the CodeCommit repository, create an appspec.yml file that includes the commands to deploy the CloudFormation template.
- . Create an Amazon CloudWatch composite alarm for all the Lambda function
- . Configure an evaluation period and dimensions for Lambd
- . Configure the alarm to enter the ALARMstate if any errors are detected or if there is insufficient data.
- . Create an Amazon CloudWatch alarm for each Lambda functio
- . Configure the alarms to enter the ALARM state if any errors are detecte
- . Configure an evaluation period, dimensions for each Lambda function and version, and the namespace as AWS/Lambda on the Errors metric.

**Answer:** BCF

**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 148**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual DOP-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the DOP-C02 Product From:

<https://www.2passeasy.com/dumps/DOP-C02/>

## Money Back Guarantee

### DOP-C02 Practice Exam Features:

- \* DOP-C02 Questions and Answers Updated Frequently
- \* DOP-C02 Practice Questions Verified by Expert Senior Certified Staff
- \* DOP-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* DOP-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year