

# Amazon

## Exam Questions AWS-Certified-DevOps-Engineer-Professional

Amazon AWS Certified DevOps Engineer Professional



### NEW QUESTION 1

A company is adopting AWS CodeDeploy to automate its application deployments for a Java-Apache Tomcat application with an Apache Webserver. The development team started with a proof of concept, created a deployment group for a developer environment, and performed functional tests within the application. After completion, the team will create additional deployment groups for staging and production.

The current log level is configured within the Apache settings, but the team wants to change this configuration dynamically when the deployment occurs, so that they can set different log level configurations depending on the deployment group without having a different application revision for each group.

How can these requirements be met with the LEAST management overhead and without requiring different script versions for each deployment group?

- A. Tag the Amazon EC2 instances depending on the deployment group
- B. Then place a script into the application revision that calls the metadata service and the EC2 API to identify which deployment group the instance is part of
- C. Use this information to configure the log level setting
- D. Reference the script as part of the AfterInstall lifecycle hook in the appspec.yml file.
- E. Create a script that uses the CodeDeploy environment variable DEPLOYMENT\_GROUP\_NAME to identify which deployment group the instance is part of
- F. Use this information to configure the log level setting
- G. Reference this script as part of the BeforeInstall lifecycle hook in the appspec.yml file.
- H. Create a CodeDeploy custom environment variable for each environment
- I. Then place a script into the application revision that checks this environment variable to identify which deployment group the instance is part of
- J. Use this information to configure the log level setting
- K. Reference this script as part of the ValidateService lifecycle hook in the appspec.yml file.
- L. Create a script that uses the CodeDeploy environment variable DEPLOYMENT\_GROUP\_ID to identify which deployment group the instance is part of to configure the log level setting
- M. Reference this script as part of the Install lifecycle hook in the appspec.yml file.

**Answer: B**

#### Explanation:

The following are the steps that the company can take to change the log level dynamically when the deployment occurs:

- ? Create a script that uses the CodeDeploy environment variable DEPLOYMENT\_GROUP\_NAME to identify which deployment group the instance is part of.
- ? Use this information to configure the log level settings.

? Reference this script as part of the BeforeInstall lifecycle hook in the appspec.yml file.

The DEPLOYMENT\_GROUP\_NAME environment variable is automatically set by CodeDeploy when the deployment is triggered. This means that the script does not need to call the metadata service or the EC2 API to identify the deployment group.

This solution is the least complex and requires the least management overhead. It also does not require different script versions for each deployment group.

The following are the reasons why the other options are not correct:

- ? Option A is incorrect because it would require tagging the Amazon EC2 instances, which would be a manual and time-consuming process.
- ? Option C is incorrect because it would require creating a custom environment variable for each environment. This would be a complex and error-prone process.
- ? Option D is incorrect because it would use

the DEPLOYMENT\_GROUP\_ID environment variable. However, this variable is not automatically set by CodeDeploy, so the script would need to call the metadata service or the EC2 API to get the deployment group ID. This would add complexity and overhead to the solution.

### NEW QUESTION 2

A company wants to use AWS development tools to replace its current bash deployment scripts. The company currently deploys a LAMP application to a group of Amazon EC2 instances behind an Application Load Balancer (ALB). During the deployments, the company unit tests the committed application, stops and starts services, unregisters and re-registers instances with the load balancer, and updates file permissions. The company wants to maintain the same deployment functionality through the shift to using AWS services.

Which solution will meet these requirements?

- A. Use AWS CodeBuild to test the application
- B. Use bash scripts invoked by AWS CodeDeploy's appspec.yml file to restart services, and deregister and register instances with the ALB
- C. Use the appspec.yml file to update file permissions without a custom script.
- D. Use AWS CodePipeline to move the application from the AWS CodeCommit repository to AWS CodeDeploy
- E. Use CodeDeploy's deployment group to test the application, unregister and re-register instances with the ALB and restart service
- F. and restart service
- G. Use the appspec.yml file to update file permissions without a custom script.
- H. Use AWS CodePipeline to move the application source code from the AWS CodeCommit repository to AWS CodeDeploy
- I. Use CodeDeploy to test the application
- J. Use CodeDeploy's appspec.yml file to restart services and update permissions without a custom script
- K. Use AWS CodeBuild to unregister and re-register instances with the ALB.
- L. Use AWS CodePipeline to trigger AWS CodeBuild to test the application
- M. Use bash scripts invoked by AWS CodeDeploy's appspec.yml file to restart service
- N. Unregister and re-register the instances in the AWS CodeDeploy deployment group with the ALB
- O. Update the appspec.yml file to update file permissions without a custom script.

**Answer: D**

#### Explanation:

<https://aws.amazon.com/blogs/devops/how-to-test-and-debug-aws-codedeploy-locally-before-you-ship-your-code/#:~:text=You%20can%20test%20application%20code,local%20server%20or%20EC2%20instance.>

### NEW QUESTION 3

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 Configure the EventBridge rule to publish a notification to the SNS topic.
- C. Configure AWS Config to send all evaluation results for the restricted-ssh rule to the SNS topic
- D. Configure a filter policy on the SNS topic to send only notifications that contain the text of NON\_COMPLIANT in the notification to subscribers.
- E. Create an Amazon EventBridge rule that matches an AWS Config evaluation result of NON\_COMPLIANT for the restricted-ssh rule 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
- F. Create an Amazon EventBridge rule that matches all AWS Config evaluation results of NON\_COMPLIANT Configure an input transformer for the restricted-ssh rule 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 4**

A company is examining its disaster recovery capability and wants the ability to switch over its daily operations to a secondary AWS Region. The company uses AWS CodeCommit as a source control tool in the primary Region.

A DevOps engineer must provide the capability for the company to develop code in the secondary Region. If the company needs to use the secondary Region, developers can add an additional remote URL to their local Git configuration.

Which solution will meet these requirements?

- A. Create a CodeCommit repository in the secondary Region
- B. Create an AWS CodeBuild project to perform a Git mirror operation of the primary Region's CodeCommit repository to the secondary Region's CodeCommit repository
- C. Create an AWS Lambda function that invokes the CodeBuild project
- D. Create an Amazon EventBridge rule that reacts to merge events in the primary Region's CodeCommit repository
- E. Configure the EventBridge rule to invoke the Lambda function.
- F. Create an Amazon S3 bucket in the secondary Region
- G. Create an AWS Fargate task to perform a Git mirror operation of the primary Region's CodeCommit repository and copy the result to the S3 bucket
- H. Create an AWS Lambda function that initiates the Fargate task
- I. Create an Amazon EventBridge rule that reacts to merge events in the CodeCommit repository
- J. Configure the EventBridge rule to invoke the Lambda function.
- K. Create an AWS CodeArtifact repository in the secondary Region
- L. Create an AWS CodePipeline pipeline that uses the primary Region's CodeCommit repository for the source action
- M. Create a Cross-Region stage in the pipeline that packages the CodeCommit repository contents and stores the contents in the CodeArtifact repository when a pull request is merged into the CodeCommit repository.
- N. Create an AWS Cloud9 environment and a CodeCommit repository in the secondary Region
- O. Configure the primary Region's CodeCommit repository as a remote repository in the AWS Cloud9 environment
- P. Connect the secondary Region's CodeCommit repository to the AWS Cloud9 environment.

**Answer:** A

**Explanation:**

The best solution to meet the disaster recovery capability and allow developers to switch over to a secondary AWS Region for code development is option A. This involves creating a CodeCommit repository in the secondary Region and setting up an AWS CodeBuild project to perform a Git mirror operation of the primary Region's CodeCommit repository to the secondary Region's repository. An AWS Lambda function is then created to invoke the CodeBuild project. Additionally, an Amazon EventBridge rule is configured to react to merge events in the primary Region's CodeCommit repository and invoke the Lambda function. This setup ensures that the secondary Region's repository is always up-to-date with the primary repository, allowing for a seamless transition in case of a disaster recovery event.

References:

? AWS CodeCommit User Guide on resilience and disaster recovery<sup>1</sup>.

? AWS Documentation on monitoring CodeCommit events in Amazon EventBridge and Amazon CloudWatch Events<sup>2</sup>.

**NEW QUESTION 5**

A company uses AWS Key Management Service (AWS KMS) keys and manual key rotation to meet regulatory compliance requirements. The security team wants to be notified when any keys have not been rotated after 90 days.

Which solution will accomplish this?

- A. Configure AWS KMS to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.
- B. Configure an Amazon EventBridge event to launch an AWS Lambda function to call the AWS Trusted Advisor API and publish to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Develop an AWS Config custom rule that publishes to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.
- D. Configure AWS Security Hub to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-determine-compliance-of-aws-kms-key-policies-to-your-specifications/>

**NEW QUESTION 6**

A company is migrating its on-premises Windows applications and Linux applications to AWS. The company will use automation to launch Amazon EC2 instances to mirror the on-premises configurations. The migrated applications require access to shared storage that uses SMB for Windows and NFS for Linux.

The company is also creating a pilot light disaster recovery (DR) environment in another AWS Region. The company will use automation to launch and configure the EC2 instances in the DR Region. The company needs to replicate the storage to the DR Region.

Which storage solution will meet these requirements?

- A. Use Amazon S3 for the application storag
- B. Create an S3 bucket in the primary Region and an S3 bucket in the DR Regio
- C. Configure S3 Cross-Region Replication (CRR) from the primary Region to the DR Region.
- D. Use Amazon Elastic Block Store (Amazon EBS) for the application storag
- E. Create a backup plan in AWS Backup that creates snapshots of the EBS volumes that are in the primary Region and replicates the snapshots to the DR Region.
- F. Use a Volume Gateway in AWS Storage Gateway for the application storag
- G. Configure Cross-Region Replication (CRR) of the Volume Gateway from the primary Region to the DR Region.
- H. Use Amazon FSx for NetApp ONTAP for the application storag
- I. Create an FSx for ONTAP instance in the DR Regio
- J. Configure NetApp SnapMirror replication from the primary Region to the DR Region.

**Answer: D**

**Explanation:**

To meet the requirements of migrating its on-premises Windows and Linux applications to AWS and creating a pilot light DR environment in another AWS Region, the company should use Amazon FSx for NetApp ONTAP for the application storage. Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage built on NetApp's popular ONTAP file system. FSx for ONTAP supports multiple protocols, including SMB for Windows and NFS for Linux, so the company can access the shared storage from both types of applications. FSx for ONTAP also supports NetApp SnapMirror replication, which enables the company to replicate the storage to the DR Region. NetApp SnapMirror replication is efficient, secure, and incremental, and it preserves the data deduplication and compression benefits of FSx for ONTAP. The company can use automation to launch and configure the EC2 instances in the DR Region and then use NetApp SnapMirror to restore the data from the primary Region.

The other options are not correct because they do not meet the requirements or follow best practices. Using Amazon S3 for the application storage is not a good option because S3 is an object storage service that does not support SMB or NFS protocols natively. The company would need to use additional services or software to mount S3 buckets as file systems, which would add complexity and cost. Using Amazon EBS for the application storage is also not a good option because EBS is a block storage service that does not support SMB or NFS protocols natively. The company would need to set up and manage file servers on EC2 instances to provide shared access to the EBS volumes, which would add overhead and maintenance. Using a Volume Gateway in AWS Storage Gateway for the application storage is not a valid option because Volume Gateway does not support SMB protocol. Volume Gateway only supports iSCSI protocol, which means that only Linux applications can access the shared storage.

References:

- ? 1: What is Amazon FSx for NetApp ONTAP? - FSx for ONTAP
- ? 2: Amazon FSx for NetApp ONTAP
- ? 3: Amazon FSx for NetApp ONTAP | NetApp
- ? 4: AWS Announces General Availability of Amazon FSx for NetApp ONTAP
- ? : Replicating Data with NetApp SnapMirror - FSx for ONTAP
- ? : What Is Amazon S3? - Amazon Simple Storage Service
- ? : What Is Amazon Elastic Block Store (Amazon EBS)? - Amazon Elastic Compute Cloud
- ? : What Is AWS Storage Gateway? - AWS Storage Gateway

**NEW QUESTION 7**

A development team manually builds an artifact locally and then places it in an Amazon S3 bucket. The application has a local cache that must be cleared when a deployment occurs. The team runs a command to do this downloads the artifact from Amazon S3 and unzips the artifact to complete the deployment.

A DevOps team wants to migrate to a CI/CD process and build in checks to stop and roll back the deployment when a failure occurs. This requires the team to track the progression of the deployment.

Which combination of actions will accomplish this? (Select THREE)

- A. Allow developers to check the code into a code repository Using Amazon EventBridge on every pull into the main branch invoke an AWS Lambda function to build the artifact and store it in Amazon S3.
- B. Create a custom script to clear the cache Specify the script in the BeforeInstall lifecycle hook in the AppSpec file.
- C. Create user data for each Amazon EC2 instance that contains the clear cache script Once deployed test the application If it is not successful deploy it again.
- D. Set up AWS CodePipeline to deploy the application Allow developers to check the code into a code repository as a source for the pipeline.
- E. Use AWS CodeBuild to build the artifact and place it in Amazon S3 Use AWS CodeDeploy to deploy the artifact to Amazon EC2 instances.
- F. Use AWS Systems Manager to fetch the artifact from Amazon S3 and deploy it to all the instances.

**Answer: BDE**

**NEW QUESTION 8**

A company has an AWS CodePipeline pipeline that is configured with an Amazon S3 bucket in the eu-west-1 Region. The pipeline deploys an AWS Lambda application to the same Region. The pipeline consists of an AWS CodeBuild project build action and an AWS CloudFormation deploy action.

The CodeBuild project uses the aws cloudformation package AWS CLI command to build an artifact that contains the Lambda function code's .zip file and the CloudFormation template. The CloudFormation deploy action references the CloudFormation template from the output artifact of the CodeBuild project's build action.

The company wants to also deploy the Lambda application to the us-east-1 Region by using the pipeline in eu-west-1. A DevOps engineer has already updated the CodeBuild project to use the aws cloudformation package command to produce an additional output artifact for us-east-1.

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

- A. Modify the CloudFormation template to include a parameter for the Lambda function code's zip file locatio
- B. Create a new CloudFormation deploy action for us-east-1 in the pipelin
- C. Configure the new deploy action to pass in the us-east-1 artifact location as a parameter override.
- D. Create a new CloudFormation deploy action for us-east-1 in the pipelin
- E. Configure the new deploy action to use the CloudFormation template from the us-east-1 output artifact.
- F. Create an S3 bucket in us-east-1. Configure the S3 bucket policy to allow CodePipeline to have read and write access.
- G. Create an S3 bucket in us-east-1. Configure S3 Cross-Region Replication (CRR) from the S3 bucket in eu-west-1 to the S3 bucket in us-east-1.
- H. Modify the pipeline to include the S3 bucket for us-east-1 as an artifact stor
- I. Create a new CloudFormation deploy action for us-east-1 in the pipelin
- J. Configure the new deploy action to use the CloudFormation template from the us-east-1 output artifact.

**Answer: AB**

**Explanation:**

A. The CloudFormation template should be modified to include a parameter that indicates the location of the .zip file containing the Lambda function's code. This allows the CloudFormation deploy action to use the correct artifact depending on the region. This is critical because Lambda functions need to reference their code

artifacts from the same region they are being deployed in. B. You would also need to create a new CloudFormation deploy action for the us-east-1 Region within the pipeline. This action should be configured to use the CloudFormation template from the artifact that was specifically created for us-east-1.

#### NEW QUESTION 9

A company has containerized all of its in-house quality control applications. The company is running Jenkins on Amazon EC2 instances, which require patching and upgrading. The compliance officer has requested a DevOps engineer begin encrypting build artifacts since they contain company intellectual property. What should the DevOps engineer do to accomplish this in the MOST maintainable manner?

- A. Automate patching and upgrading using AWS Systems Manager on EC2 instances and encrypt Amazon EBS volumes by default.
- B. Deploy Jenkins to an Amazon ECS cluster and copy build artifacts to an Amazon S3 bucket with default encryption enabled.
- C. Leverage AWS CodePipeline with a build action and encrypt the artifacts using AWS Secrets Manager.
- D. Use AWS CodeBuild with artifact encryption to replace the Jenkins instance running on EC2 instances.

**Answer: D**

#### Explanation:

The following are the steps involved in accomplishing this in the most maintainable manner:

- ? Use AWS CodeBuild with artifact encryption to replace the Jenkins instance running on EC2 instances.
- ? Configure CodeBuild to encrypt the build artifacts using AWS Secrets Manager.
- ? Deploy the containerized quality control applications to CodeBuild.

This approach is the most maintainable because it eliminates the need to manage Jenkins on EC2 instances. CodeBuild is a managed service, so the DevOps engineer does not need to worry about patching or upgrading the service. <https://docs.aws.amazon.com/codebuild/latest/userguide/security-encryption.html> Build artifact encryption - CodeBuild requires access to an AWS KMS CMK in order to encrypt its build output artifacts. By default, CodeBuild uses an AWS Key Management Service CMK for Amazon S3 in your AWS account. If you do not want to use this CMK, you must create and configure a customer-managed CMK. For more information Creating keys.

#### NEW QUESTION 10

A company requires that its internally facing web application be highly available. The architecture is made up of one Amazon EC2 web server instance and one NAT instance that provides outbound internet access for updates and accessing public data.

Which combination of architecture adjustments should the company implement to achieve high availability? (Choose two.)

- A. Add the NAT instance to an EC2 Auto Scaling group that spans multiple Availability Zone
- B. Update the route tables.
- C. Create additional EC2 instances spanning multiple Availability Zone
- D. Add an Application Load Balancer to split the load between them.
- E. Configure an Application Load Balancer in front of the EC2 instance
- F. Configure Amazon CloudWatch alarms to recover the EC2 instance upon host failure.
- G. Replace the NAT instance with a NAT gateway in each Availability Zone
- H. Update the route tables.
- I. Replace the NAT instance with a NAT gateway that spans multiple Availability Zone
- J. Update the route tables.

**Answer: BD**

#### Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

#### NEW QUESTION 10

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, 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. 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 15

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

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

**Answer:** BE

#### Explanation:

To meet the requirements of failover and disaster recovery, the company should use the following deployment strategies:

? Create an Amazon Aurora global database in two AWS Regions as the data store.

In the event of a failure, promote the secondary Region to the primary for the application. Update the application to use the Aurora cluster endpoint in the secondary Region. This strategy can provide a low RPO and RTO for the data, as Aurora global database replicates data with minimal latency across Regions and allows fast and easy failover<sup>12</sup>. The company can use the Amazon Aurora cluster endpoint to connect to the current primary DB cluster without needing to change any application code<sup>1</sup>.

? Set up the application in two AWS Regions. Configure AWS Global Accelerator to

point to Application Load Balancers (ALBs) in both Regions. Add both ALBs to a single endpoint group. Use health checks and Auto Scaling groups in each Region. This strategy can provide high availability and performance for the application, as AWS Global Accelerator uses the AWS global network to route traffic to the closest healthy endpoint<sup>3</sup>. The company can also use static IP addresses that are assigned by Global Accelerator as a fixed entry point for their application<sup>1</sup>. By using health checks and Auto Scaling groups, the company can ensure that their application can scale up or down based on demand and handle any instance failures<sup>4</sup>.

The other options are incorrect because:

? Creating an Amazon Aurora Single-AZ cluster in multiple AWS Regions as the data store would not provide a fast failover or disaster recovery solution, as the company would need to manually restore data from backups or snapshots in another Region in case of a failure.

? Creating an Amazon Aurora cluster in multiple AWS Regions as the data store and using a Network Load Balancer to balance the database traffic in different Regions would not work, as Network Load Balancers do not support cross-Region routing. Moreover, this strategy would not provide a consistent view of the data across Regions, as Aurora clusters do not replicate data automatically between Regions unless they are part of a global database.

? Setting up the application in two AWS Regions and using Amazon Route 53 failover routing that points to Application Load Balancers in both Regions would not provide a low RTO, as Route 53 failover routing relies on DNS resolution, which can take time to propagate changes across different DNS servers and clients. Moreover, this strategy would not provide deterministic routing, as Route 53 failover routing depends on DNS caching behavior, which can vary depending on different factors.

#### NEW QUESTION 19

A company uses AWS and has a VPC that contains critical compute infrastructure with predictable traffic patterns. The company has configured VPC flow logs that are published to a log group in Amazon CloudWatch Logs.

The company's DevOps team needs to configure a monitoring solution for the VPC flow logs to identify anomalies in network traffic to the VPC over time. If the monitoring solution detects an anomaly, the company needs the ability to initiate a response to the anomaly.

How should the DevOps team configure the monitoring solution to meet these requirements?

- A. Create an Amazon Kinesis data strea
- B. Subscribe the log group to the data strea
- C. Configure Amazon Kinesis Data Analytics to detect log anomalies in the data strea
- D. Create an AWS Lambda function to use as the output of the data strea
- E. Configure the Lambda function to write to the default Amazon EventBridge event bus in the event of an anomaly finding.
- F. Create an Amazon Kinesis Data Firehose delivery stream that delivers events to an Amazon S3 bucke
- G. Subscribe the log group to the delivery strea
- H. Configure Amazon Lookout for Metrics to monitor the data in the S3 bucket for anomalie
- I. Create an AWS Lambda function to run in response to Lookout for Metrics anomaly finding
- J. Configure the Lambda function to publish to the default Amazon EventBridge event bus.
- K. Create an AWS Lambda function to detect anomalie
- L. Configure the Lambda function to publish an event to the default Amazon EventBridge event bus if the Lambda function detects an anomal
- M. Subscribe the Lambda function to the log group.
- N. Create an Amazon Kinesis data strea
- O. Subscribe the log group to the data strea
- P. Create an AWS Lambda function to detect log anomalie
- Q. Configure the Lambda function to write to the default Amazon EventBridge event bus if the Lambda function detects an anomal
- R. Set the Lambda function as the processor for the data stream.

**Answer:** D

#### Explanation:

To meet the requirements, the DevOps team needs to configure a monitoring solution for the VPC flow logs that can detect anomalies in network traffic over time and initiate a response to the anomaly. The DevOps team can use Amazon Kinesis Data Streams to ingest and process streaming data from CloudWatch Logs. The DevOps team can subscribe the log group to a Kinesis data stream, which will deliver log events from CloudWatch Logs to Kinesis Data Streams in near real-time. The DevOps team can then create an AWS Lambda function to detect log anomalies using machine learning or statistical methods. The Lambda function can

be set as a processor for the data stream, which means that it will process each record from the stream before sending it to downstream applications or destinations. The Lambda function can also write to the default Amazon EventBridge event bus if it detects an anomaly, which will allow other AWS services or custom applications to respond to the anomaly event.

#### NEW QUESTION 20

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 21

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 22

An AWS CodePipeline pipeline has implemented a code release process. The pipeline is integrated with AWS CodeDeploy to deploy versions of an application to multiple Amazon EC2 instances for each CodePipeline stage.

During a recent deployment the pipeline failed due to a CodeDeploy issue. The DevOps team wants to improve monitoring and notifications during deployment to decrease resolution times.

What should the DevOps engineer do to create notifications. When issues are discovered?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 27**

A company's production environment uses an AWS CodeDeploy blue/green deployment to deploy an application. The deployment includes Amazon EC2 Auto Scaling groups that launch instances that run Amazon Linux 2.

A working appspec. yml file exists in the code repository and contains the following text.

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/application
```

A DevOps engineer needs to ensure that a script downloads and installs a license file onto the instances before the replacement instances start to handle request traffic. The DevOps engineer adds a hooks section to the appspec. yml file.

Which hook should the DevOps engineer use to run the script that downloads and installs the license file?

- A. AfterBlockTraffic
- B. BeforeBlockTraffic
- C. BeforeInstall
- D. Download Bundle

**Answer: C**

**Explanation:**

This hook runs before the new application version is installed on the replacement instances. This is the best place to run the script because it ensures that the license file is downloaded and installed before the replacement instances start to handle request traffic. If you use any other hook, you may encounter errors or inconsistencies in your application.

**NEW QUESTION 32**

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 35**

A company is using an AWS CodeBuild project to build and package an application. The packages are copied to a shared Amazon S3 bucket before being deployed across multiple AWS accounts.

The buildspec.yml file contains the following:

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 37**

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 42**

A company builds an application that uses an Application Load Balancer in front of Amazon EC2 instances that are in an Auto Scaling group. The application is stateless. The Auto Scaling group uses a custom AMI that is fully prebuilt. The EC2 instances do not have a custom bootstrapping process. The AMI that the Auto Scaling group uses was recently deleted. The Auto Scaling group's scaling activities show failures because the AMI ID does not exist. Which combination of steps should a DevOps engineer take to meet these requirements? (Select THREE.)

- A. Create a new launch template that uses the new AMI.
- B. Update the Auto Scaling group to use the new launch template.
- C. Reduce the Auto Scaling group's desired capacity to 0.
- D. Increase the Auto Scaling group's desired capacity by 1.
- E. Create a new AMI from a running EC2 instance in the Auto Scaling group.
- F. Create a new AMI by copying the most recent public AMI of the operating system that the EC2 instances use.

**Answer:** ABF

**Explanation:**

To restore the functionality of the Auto Scaling group after the AMI was deleted, the DevOps engineer needs to create a new AMI and update the Auto Scaling group to use it. The DevOps engineer can create a new AMI by copying the most recent public AMI of the operating system that the EC2 instances use. This will ensure that the new AMI has the same operating system as the custom AMI that was deleted. The DevOps engineer can then create a new launch template that uses the new AMI and update the Auto Scaling group to use the new launch template. This will allow the Auto Scaling group to launch new instances with the new AMI.

**NEW QUESTION 43**

A company is hosting a static website from an Amazon S3 bucket. The website is available to customers at example.com. The company uses an Amazon Route 53 weighted routing policy with a TTL of 1 day. The company has decided to replace the existing static website with a dynamic web application. The dynamic web application uses an Application Load Balancer (ALB) in front of a fleet of Amazon EC2 instances.

On the day of production launch to customers, the company creates an additional Route 53 weighted DNS record entry that points to the ALB with a weight of 255 and a TTL of 1 hour. Two days later, a DevOps engineer notices that the previous static website is displayed sometimes when customers navigate to example.com.

How can the DevOps engineer ensure that the company serves only dynamic content for example.com?

- A. Delete all objects, including previous versions, from the S3 bucket that contains the static website content.
- B. Update the weighted DNS record entry that points to the S3 bucket.
- C. Apply a weight of 0. Specify the domain reset option to propagate changes immediately.
- D. Configure webpage redirect requests on the S3 bucket with a hostname that redirects to the ALB.
- E. Remove the weighted DNS record entry that points to the S3 bucket from the example.com hosted zone.
- F. Wait for DNS propagation to become complete.

**Answer: D**

#### NEW QUESTION 47

A business has an application that consists of five independent AWS Lambda functions. The DevOps engineer has built a CI/CD pipeline using AWS CodePipeline and AWS CodeBuild that builds test packages and deploys each Lambda function in sequence. The pipeline uses an Amazon EventBridge rule to ensure the pipeline starts as quickly as possible after a change is made to the application source code.

After working with the pipeline for a few months the DevOps engineer has noticed the pipeline takes too long to complete.

What should the DevOps engineer implement to BEST improve the speed of the pipeline?

- A. Modify the CodeBuild projects within the pipeline to use a compute type with more available network throughput.
- B. Create a custom CodeBuild execution environment that includes a symmetric multiprocessing configuration to run the builds in parallel.
- C. Modify the CodePipeline configuration to run actions for each Lambda function in parallel by specifying the same runorder.
- D. Modify each CodeBuild project to run within a VPC and use dedicated instances to increase throughput.

**Answer: C**

#### Explanation:

<https://docs.aws.amazon.com/codepipeline/latest/userguide/reference-pipeline-structure.html>

AWS doc: "To specify parallel actions, use the same integer for each action you want to run in parallel. For example, if you want three actions to run in sequence in a stage, you would give the first action the runOrder value of 1, the second action the runOrder value of 2, and the third the runOrder value of 3. However, if you want the second and third actions to run in parallel, you would give the first action the runOrder value of 1 and both the second and third actions the runOrder value of 2."

#### NEW QUESTION 49

A company has an application that includes AWS Lambda functions. The Lambda functions run Python code that is stored in an AWS CodeCommit repository. The company has recently experienced failures in the production environment because of an error in the Python code. An engineer has written unit tests for the Lambda functions to help avoid releasing any future defects into the production environment.

The company's DevOps team needs to implement a solution to integrate the unit tests into an existing AWS CodePipeline pipeline. The solution must produce reports about the unit tests for the company to view.

Which solution will meet these requirements?

- A. Associate the CodeCommit repository with Amazon CodeGuru Reviewer
- B. Create a new AWS CodeBuild project
- C. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project
- D. Create a buildspec.yml file in the CodeCommit repository
- E. In the buildspec.yml file, define the actions to run a CodeGuru review.
- F. Create a new AWS CodeBuild project
- G. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project
- H. Create a CodeBuild report group
- I. Create a buildspec.yml file in the CodeCommit repository
- J. In the buildspec.yml file, define the actions to run the unit tests with an output of JUNITXML in the build phase section. Configure the test reports to be uploaded to the new CodeBuild report group.
- K. Create a new AWS CodeArtifact repository
- L. Create a new AWS CodeBuild project
- M. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project
- N. Create an appspec.yml file in the original CodeCommit repository
- O. In the appspec.yml file, define the actions to run the unit tests with an output of CUCUMBERJSON in the build phase section
- P. Configure the test reports to be sent to the new CodeArtifact repository.
- Q. Create a new AWS CodeBuild project
- R. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project
- S. Create a new Amazon S3 bucket
- T. Create a buildspec.yml file in the CodeCommit repository
- . In the buildspec.yml file, define the actions to run the unit tests with an output of HTML in the build phase section
- . In the reports section, upload the test reports to the S3 bucket.

**Answer: B**

#### Explanation:

The correct answer is B. Creating a new AWS CodeBuild project and configuring a test stage in the AWS CodePipeline pipeline that uses the new CodeBuild project is the best way to integrate the unit tests into the existing pipeline. Creating a CodeBuild report group and uploading the test reports to the new CodeBuild report group will produce reports about the unit tests for the company to view. Using JUNITXML as the output format for the unit tests is supported by CodeBuild and will generate a valid report. Option A is incorrect because Amazon CodeGuru Reviewer is a service that provides automated code reviews and recommendations for improving code quality and performance. It is not a tool for running unit tests or producing test reports. Therefore, option A will not meet the requirements.

Option C is incorrect because AWS CodeArtifact is a service that provides secure, scalable, and cost-effective artifact management for software development. It is not a tool for running unit tests or producing test reports. Moreover, option C uses CUCUMBERJSON as the output format for the unit tests, which is not supported by CodeBuild and will not generate a valid report.

Option D is incorrect because uploading the test reports to an Amazon S3 bucket is not the best way to produce reports about the unit tests for the company to view. CodeBuild has a built-in feature to create and manage test reports, which is more convenient and efficient than using S3. Furthermore, option D uses HTML as the output format for the unit tests, which is not supported by CodeBuild and will not generate a valid report.

#### NEW QUESTION 51

A company uses AWS Organizations to manage multiple accounts. Information security policies require that all unencrypted Amazon EBS volumes be marked as non-compliant. A DevOps engineer needs to automatically deploy the solution and ensure that this compliance check is always present. Which solution will accomplish this?

- A. Create an AWS CloudFormation template that defines an AWS Inspector rule to check whether EBS encryption is enable
- B. Save the template to an Amazon S3 bucket that has been shared with all accounts within the compan
- C. Update the account creation script pointing to the CloudFormation template in Amazon S3.
- D. Create an AWS Config organizational rule to check whether EBS encryption is enabled and deploy the rule using the AWS CL
- E. Create and apply an SCP to prohibit stopping and deleting AWS Config across the organization.
- F. Create an SCP in Organization
- G. Set the policy to prevent the launch of Amazon EC2 instances without encryption on the EBS volumes using a conditional expressio
- H. Apply the SCP to all AWS account
- I. Use Amazon Athena to analyze the AWS CloudTrail output, looking for events that deny an ec2: RunInstances action.
- J. Deploy an IAM role to all accounts from a single trusted accoun
- K. Build a pipeline withAWS CodePipeline with a stage in AWS Lambda to assume the IAM role, and list all EBS volumes in the accoun
- L. Publish a report to Amazon S3.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/config/latest/developerguide/ec2-ebs-encryption-by-default.html>

**NEW QUESTION 54**

A company updated the AWS Cloud Formation template for a critical business application. The stack update process failed due to an error in the updated template and AWS CloudFormation automatically began the stack rollback process Later a DevOps engineer discovered that the application was still unavailable and that the stack was in the UPDATE\_ROLLBACK\_FAILED state.

Which combination of actions should the DevOps engineer perform so that the stack rollback can complete successfully? (Select TWO.)

- A. Attach the AWSC loud Formation FullAccess IAM policy to the AWS CtoudFormation role.
- B. Automatically recover the stack resources by using AWS CloudFormation drift detection.
- C. Issue a ContinueUpdateRollback command from the AWS CloudFormation console or the AWS CLI.
- D. Manually adjust the resources to match the expectations of the stack.
- E. Update the existing AWS CloudFormation stack by using the original template.

**Answer: CD**

**Explanation:**

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/continue-update-rollback.html> For a specified stack that is in the UPDATE\_ROLLBACK\_FAILED state, continues rolling it back to the UPDATE\_ROLLBACK\_COMPLETE state. Depending on the cause of the failure, you can manually fix the error and continue the rollback. By continuing the rollback, you can return your stack to a working state (the UPDATE\_ROLLBACK\_COMPLETE state), and then try to update the stack again.

**NEW QUESTION 58**

A company uses AWS Secrets Manager to store a set of sensitive API keys that an AWS Lambda function uses. When the Lambda function is invoked, the Lambda function retrieves the API keys and makes an API call to an external service. The Secrets Manager secret is encrypted with the default AWS Key Management Service (AWS KMS) key.

A DevOps engineer needs to update the infrastructure to ensure that only the Lambda function's execution role can access the values in Secrets Manager. The solution must apply the principle of least privilege.

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

- A. Update the default KMS key for Secrets Manager to allow only the Lambda function's execution role to decrypt.
- B. Create a KMS customer managed key that trusts Secrets Manager and allows the Lambda function's execution role to decrypt
- C. Update Secrets Manager to use the new customer managed key.
- D. Create a KMS customer managed key that trusts Secrets Manager and allows the account's :root principal to decrypt
- E. Update Secrets Manager to use the new customer managed key.
- F. Ensure that the Lambda function's execution role has the KMS permissions scoped on the resource leve
- G. Configure the permissions so that the KMS key can encrypt the Secrets Manager secret.
- H. Remove all KMS permissions from the Lambda function's execution role.

**Answer: BD**

**Explanation:**

The requirement is to update the infrastructure to ensure that only the Lambda function's execution role can access the values in Secrets Manager. The solution must apply the principle of least privilege, which means granting the minimum permissions necessary to perform a task.

To do this, the DevOps engineer needs to use the following steps:

? Create a KMS customer managed key that trusts Secrets Manager and allows the Lambda function's execution role to decrypt. A customer managed key is a symmetric encryption key that is fully managed by the customer. The customer can define the key policy, which specifies who can use and manage the key. By creating a customer managed key, the DevOps engineer can restrict the decryption permission to only the Lambda function's execution role, and prevent other principals from accessing the secret values. The customer managed key also needs to trust Secrets Manager, which means allowing Secrets Manager to use the key to encrypt and decrypt secrets on behalf of the customer.

? Update Secrets Manager to use the new customer managed key. Secrets Manager allows customers to choose which KMS key to use for encrypting each secret. By default, Secrets Manager uses the default KMS key for Secrets Manager, which is a service-managed key that is shared by all customers in the same AWS Region. By updating Secrets Manager to use the new customer managed key, the DevOps engineer can ensure that only the Lambda function's execution role can decrypt the secret values using that key.

? Ensure that the Lambda function's execution role has the KMS permissions scoped on the resource level. The Lambda function's execution role is an IAM role that grants permissions to the Lambda function to access AWS services and resources. The role needs to have KMS permissions to use the customer managed key for decryption. However, to apply the principle of least privilege, the role should have the permissions scoped on the resource level, which means specifying the ARN of the customer managed key as a condition in the IAM policy statement. This way, the role can only use that specific key and not any other KMS keys in the account.

#### NEW QUESTION 61

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 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 62

A company wants to use a grid system for a proprietary enterprise in-memory data store on top of AWS. This system can run in multiple server nodes in any Linux-based distribution. The system must be able to reconfigure the entire cluster every time a node is added or removed. When adding or removing nodes an /etc./cluster/nodes config file must be updated listing the IP addresses of the current node members of that cluster.

The company wants to automate the task of adding new nodes to a cluster. What can a DevOps engineer do to meet these requirements?

- A. Use AWS OpsWorks Stacks to layer the server nodes of that cluster
- B. Create a Chef recipe that populates the content of the /etc./cluster/nodes config file and restarts the service by using the current members of the layer
- C. Assign that recipe to the Configure lifecycle event.
- D. Put the file nodes config in version control
- E. Create an AWS CodeDeploy deployment configuration and deployment group based on an Amazon EC2 tag value for the cluster node
- F. When adding a new node to the cluster update the file with all tagged instances and make a commit in version control
- G. Deploy the new file and restart the services.
- H. Create an Amazon S3 bucket and upload a version of the /etc./cluster/nodes config file Create a crontab script that will poll for that S3 file and download it frequently
- I. Use a process manager such as Monit or systemd, to restart the cluster services when it detects that the new file was modified
- J. When adding a node to the cluster edit the file's most recent members Upload the new file to the S3 bucket.
- K. Create a user data script that lists all members of the current security group of the cluster and automatically updates the /etc/cluster/. nodes config
- L. Trigger whenever a new instance is added to the cluster.

**Answer: A**

#### Explanation:

You can run custom recipes manually, but the best approach is usually to have AWS OpsWorks Stacks run them automatically. Every layer has a set of built-in recipes assigned each of five lifecycle events—Setup, Configure, Deploy, Undeploy, and Shutdown. Each time an event occurs for an instance, AWS OpsWorks Stacks runs the associated recipes for each of the instance's layers, which handle the corresponding tasks. For example, when an instance finishes booting, AWS OpsWorks Stacks triggers a Setup event. This event runs the associated layer's Setup recipes, which typically handle tasks such as installing and configuring packages

#### NEW QUESTION 65

An ecommerce company has chosen AWS to host its new platform. The company's DevOps team has started building an AWS Control Tower landing zone. The DevOps team has set the identity store within AWS IAM Identity Center (AWS Single Sign-On) to external identity provider (IdP) and has configured SAML 2.0. The DevOps team wants a robust permission model that applies the principle of least privilege. The model must allow the team to build and manage only the team's own resources.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create IAM policies that include the required permission
- B. Include the aws:PrincipalTag condition key.
- C. Create permission set
- D. Attach an inline policy that includes the required permissions and uses the aws:PrincipalTag condition key to scope the permissions.
- E. Create a group in the IdP
- F. Place users in the group
- G. Assign the group to accounts and the permission sets in IAM Identity Center.
- H. Create a group in the IdP
- I. Place users in the group
- J. Assign the group to OUs and IAM policies.
- K. Enable attributes for access control in IAM Identity Center
- L. Apply tags to user
- M. Map the tags as key-value pairs.
- N. Enable attributes for access control in IAM Identity Center
- O. Map attributes from the IdP as key-value pairs.

**Answer: BCF**

**Explanation:**

Using the principalTag in the Permission Set inline policy a logged in user belonging to a specific AD group in the IDP can be permitted access to perform operations on certain resources if their group matches the group used in the PrincipleTag. Basically you are narrowing the scope of privileges assigned via Permission policies conditionally based on whether the logged in user belongs to a specific AD Group in IDP. The mapping of the AD group to the request attributes can be done using SSO attributes where we can pass other attributes like the SAML token as well.

<https://docs.aws.amazon.com/singlesignon/latest/userguide/abac.html>

**NEW QUESTION 68**

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 69**

A DevOps engineer is building a continuous deployment pipeline for a serverless application that uses AWS Lambda functions. The company wants to reduce the customer impact of an unsuccessful deployment. The company also wants to monitor for issues.

Which deploy stage configuration will meet these requirements?

- A. Use an AWS Serverless Application Model (AWS SAM) template to define the serverless applicatio
- B. Use AWS CodeDeploy to deploy the Lambda functions with the Canary10Percent15Minutes Deployment Preference Typ
- C. Use Amazon CloudWatch alarms to monitor the health of the functions.
- D. Use AWS CloudFormation to publish a new stack update, and include Amazon CloudWatch alarms on all resource
- E. Set up an AWS CodePipeline approval action for a developer to verify and approve the AWS CloudFormation change set.
- F. Use AWS CloudFormation to publish a new version on every stack update, and include Amazon CloudWatch alarms on all resource
- G. Use the RoutingConfig property of the AWS::Lambda::Alias resource to update the traffic routing during the stack update.
- H. Use AWS CodeBuild to add sample event payloads for testing to the Lambda function
- I. Publish a new version of the functions, and include Amazon CloudWatch alarm
- J. Update the production alias to point to the new versio
- K. Configure rollbacks to occur when an alarm is in the ALARM state.

**Answer:** D

**Explanation:**

Use routing configuration on an alias to send a portion of traffic to a second function version. For example, you can reduce the risk of deploying a new version by configuring the alias to send most of the traffic to the existing version, and only a small percentage of traffic to the new version.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html>

The following are the steps involved in the deploy stage configuration that will meet the requirements:

? Use AWS CodeBuild to add sample event payloads for testing to the Lambda functions.

? Publish a new version of the functions, and include Amazon CloudWatch alarms.

? Update the production alias to point to the new version.

? Configure rollbacks to occur when an alarm is in the ALARM state.

This configuration will help to reduce the customer impact of an unsuccessful deployment

by deploying the new version of the functions to a staging environment first. This will allow the DevOps engineer to test the new version of the functions before deploying it to production.

The configuration will also help to monitor for issues by including Amazon CloudWatch alarms. These alarms will alert the DevOps engineer if there are any problems with the new version of the functions.

**NEW QUESTION 73**

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 polic
- D. Set the interval period for unattached EBS volumes to 14 days and set the retention rule to delet

- 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 78**

To run an application, a DevOps engineer launches an Amazon EC2 instance with public IP addresses in a public subnet. A user data script obtains the application artifacts and installs them on the instances upon launch. A change to the security classification of the application now requires the instances to run with no access to the internet. While the instances launch successfully and show as healthy, the application does not seem to be installed. Which of the following should successfully install the application while complying with the new rule?

- A. Launch the instances in a public subnet with Elastic IP addresses attached.
- B. Once the application is installed and running, run a script to disassociate the Elastic IP addresses afterwards.
- C. Set up a NAT gateway.
- D. Deploy the EC2 instances to a private subnet.
- E. Update the private subnet's route table to use the NAT gateway as the default route.
- F. Publish the application artifacts to an Amazon S3 bucket and create a VPC endpoint for S3. Assign an IAM instance profile to the EC2 instances so they can read the application artifacts from the S3 bucket.
- G. Create a security group for the application instances and allow only outbound traffic to the artifact repository.
- H. Remove the security group rule once the install is complete.

**Answer: C**

**Explanation:**

EC2 instances running in private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets 1-  
<https://aws.amazon.com/pt/blogs/aws/new-vpc-endpoint-for-amazon-s3/>

**NEW QUESTION 82**

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 84

A company deploys updates to its Amazon API Gateway API several times a week by using an AWS CodePipeline pipeline. As part of the update process the company exports the JavaScript SDK for the API from the API Gateway console and uploads the SDK to an Amazon S3 bucket. The company has configured an Amazon CloudFront distribution that uses the S3 bucket as an origin. Web clients then download the SDK by using the CloudFront distribution's endpoint. A DevOps engineer needs to implement a solution to make the new SDK available automatically during new API deployments. Which solution will meet these requirements?

- A. Create a CodePipeline action immediately after the deployment stage of the API
- B. Configure the action to invoke an AWS Lambda function
- C. Configure the Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and create a CloudFront invalidation for the SDK path.
- D. Create a CodePipeline action immediately after the deployment stage of the API. Configure the action to use the CodePipeline integration with API Gateway to export the SDK to Amazon S3. Create another action that uses the CodePipeline integration with Amazon S3 to invalidate the cache for the SDK path.
- E. Create an Amazon EventBridge rule that reacts to UpdateStage events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.
- F. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.
- G. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.
- H. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.
- I. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.
- J. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket and call the CloudFront API to create an invalidation for the SDK path.

**Answer:** A

#### Explanation:

This solution would allow the company to automate the process of updating the SDK and making it available to web clients. By adding a CodePipeline action immediately after the deployment stage of the API, the Lambda function will be invoked automatically each time the API is updated. The Lambda function should be able to download the new SDK from API Gateway, upload it to the S3 bucket and also create a CloudFront invalidation for the SDK path so that the latest version of the SDK is available for the web clients. This is the most straightforward solution and it will meet the requirements.

#### NEW QUESTION 88

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 93

A company's security policies require the use of security hardened AMIs in production environments. A DevOps engineer has used EC2 Image Builder to create a pipeline that builds the AMIs on a recurring schedule. The DevOps engineer needs to update the launch templates of the company's Auto Scaling groups. The Auto Scaling groups must use the newest AMIs during the launch of Amazon EC2 instances. Which solution will meet these requirements with the MOST operational efficiency?

- A. Configure an Amazon EventBridge rule to receive new AMI events from Image Builder
- B. Target an AWS Systems Manager Run Command document that updates the launch templates of the Auto Scaling groups with the newest AMI ID.
- C. Configure an Amazon EventBridge rule to receive new AMI events from Image Builder
- D. Target an AWS Lambda function that updates the launch templates of the Auto Scaling groups with the newest AMI ID.
- E. Configure the launch template to use a value from AWS Systems Manager Parameter Store for the AMI ID.
- F. Configure the Image Builder pipeline to update the Parameter Store value with the newest AMI ID.
- G. Configure the Image Builder distribution settings to update the launch templates with the newest AMI ID.
- H. Configure the Auto Scaling groups to use the newest version of the launch template.

**Answer:** C

#### Explanation:

? The most operationally efficient solution is to use AWS Systems Manager Parameter Store<sup>1</sup> to store the AMI ID and reference it in the launch template<sup>2</sup>. This way, the launch template does not need to be updated every time a new AMI is created by Image Builder. Instead, the Image Builder pipeline can update the Parameter Store value with the newest AMI ID<sup>3</sup>, and the Auto Scaling group can launch instances using the latest value from Parameter Store.  
 ? The other solutions require updating the launch template or creating a new version of it every time a new AMI is created, which adds complexity and overhead. Additionally, using EventBridge rules and Lambda functions or Run Command documents introduces additional dependencies and potential points of failure.  
 References: 1: AWS Systems Manager Parameter Store 2: Using AWS Systems Manager parameters instead of AMI IDs in launch templates 3: Update an SSM parameter with Image Builder

**NEW QUESTION 97**

A company provides an application to customers. The application has an Amazon API Gateway REST API that invokes an AWS Lambda function. On initialization, the Lambda function loads a large amount of data from an Amazon DynamoDB table. The data load process results in long cold-start times of 8-10 seconds. The DynamoDB table has DynamoDB Accelerator (DAX) configured.

Customers report that the application intermittently takes a long time to respond to requests. The application receives thousands of requests throughout the day. In the middle of the day, the application experiences 10 times more requests than at any other time of the day. Near the end of the day, the application's request volume decreases to 10% of its normal total.

A DevOps engineer needs to reduce the latency of the Lambda function at all times of the day.

Which solution will meet these requirements?

- A. Configure provisioned concurrency on the Lambda function with a concurrency value of 1. Delete the DAX cluster for the DynamoDB table.
- B. Configure reserved concurrency on the Lambda function with a concurrency value of 0.
- C. Configure provisioned concurrency on the Lambda function.
- D. Configure AWS Application Auto Scaling on the Lambda function with provisioned concurrency values set to a minimum of 1 and a maximum of 100.
- E. Configure reserved concurrency on the Lambda function.
- F. Configure AWS Application Auto Scaling on the API Gateway API with a reserved concurrency maximum value of 100.

**Answer: C**

**Explanation:**

The following are the steps that the DevOps engineer should take to reduce the latency of the Lambda function at all times of the day:

? Configure provisioned concurrency on the Lambda function.

? Configure AWS Application Auto Scaling on the Lambda function with provisioned concurrency values set to a minimum of 1 and a maximum of 100.

The provisioned concurrency setting ensures that there is always a minimum number of Lambda function instances available to handle requests. The Application Auto Scaling setting will automatically scale the number of Lambda function instances up or down based on the demand for the application.

This solution will ensure that the Lambda function is able to handle the increased load during the middle of the day, while also keeping the cold-start latency low.

The following are the reasons why the other options are not correct:

? Option A is incorrect because it will not reduce the cold-start latency of the Lambda function.

? Option B is incorrect because it will not scale the number of Lambda function instances up or down based on demand.

? Option D is incorrect because it will only configure reserved concurrency on the API Gateway API, which will not affect the Lambda function.

**NEW QUESTION 98**

A company has multiple AWS accounts. The company uses AWS IAM Identity Center (AWS Single Sign-On) that is integrated with AWS Toolkit for Microsoft Azure DevOps. The attributes for access control feature is enabled in IAM Identity Center.

The attribute mapping list contains two entries. The department key is mapped to

`${path:enterprise.department}`. The costCenter key is mapped to

`${path:enterprise.costCenter}`.

All existing Amazon EC2 instances have a department tag that corresponds to three company departments (d1, d2, d3). A DevOps engineer must create policies based on the matching attributes. The policies must minimize administrative effort and must grant each Azure AD user access to only the EC2 instances that are tagged with the user's respective department name.

Which condition key should the DevOps engineer include in the custom permissions policies to meet these requirements?

A.

```
"Condition": {
  "ForAllValues:StringEquals": {
    "aws:TagKeys": ["department"]
  }
}
```

B.

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalTag/department": "${aws:ResourceTag/department}"
  }
}
```

C.

```
"Condition": {
  "StringEquals": {
    "ec2:ResourceTag/department": "${aws:PrincipalTag/department}"
  }
}
```

D.

```
"Condition": {
  "ForAllValues:StringEquals": {
    "ec2:ResourceTag/department": ["d1", "d2", "d3"]
  }
}
```

A.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/singlesignon/latest/userguide/configure-abac.html>

#### NEW QUESTION 100

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 102

A DevOps engineer needs to back up sensitive Amazon S3 objects that are stored within an S3 bucket with a private bucket policy using S3 cross-Region replication functionality. The objects need to be copied to a target bucket in a different AWS Region and account.

Which combination of actions should be performed to enable this replication? (Choose three.)

- A. Create a replication IAM role in the source account
- B. Create a replication IAM role in the target account.
- C. Add statements to the source bucket policy allowing the replication IAM role to replicate objects.
- D. Add statements to the target bucket policy allowing the replication IAM role to replicate objects.
- E. Create a replication rule in the source bucket to enable the replication.
- F. Create a replication rule in the target bucket to enable the replication.

**Answer:** ADE

**Explanation:**

S3 cross-Region replication (CRR) automatically replicates data between buckets across different AWS Regions. To enable CRR, you need to add a replication configuration to your source bucket that specifies the destination bucket, the IAM role, and the encryption type (optional). You also need to grant permissions to the IAM role to perform replication actions on both the source and destination buckets. Additionally, you can choose the destination storage class and enable additional replication options such as S3 Replication Time Control (S3 RTC) or S3 Batch Replication. <https://medium.com/cloud-techies/s3-same-region-replication-srr-and-cross-region-replication-crr-34d446806bab> <https://aws.amazon.com/getting-started/hands-on/replicate-data-using-amazon-s3-replication/> <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>

#### NEW QUESTION 107

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 deployment
- 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 112**

A company manages AWS accounts for application teams in AWS Control Tower. Individual application teams are responsible for securing their respective AWS accounts.

A DevOps engineer needs to enable Amazon GuardDuty for all AWS accounts in which the application teams have not already enabled GuardDuty. The DevOps engineer is using AWS CloudFormation StackSets from the AWS Control Tower management account.

How should the DevOps engineer configure the CloudFormation template to prevent failure during the StackSets deployment?

- A. Create a CloudFormation custom resource that invokes an AWS Lambda function
- B. Configure the Lambda function to conditionally enable GuardDuty if GuardDuty is not already enabled in the accounts.
- C. Use the Conditions section of the CloudFormation template to enable GuardDuty in accounts where GuardDuty is not already enabled.
- D. Use the CloudFormation Fn::GetAtt intrinsic function to check whether GuardDuty is already enabled. If GuardDuty is not already enabled use the Resources section of the CloudFormation template to enable GuardDuty.
- E. Use the Fn::GetAtt intrinsic function to check whether GuardDuty is already enabled. If GuardDuty is not already enabled use the Resources section of the CloudFormation template to enable GuardDuty.
- F. Manually discover the list of AWS account IDs where GuardDuty is not enabled. Use the CloudFormation Fn::ImportValue intrinsic function to import the list of account IDs into the CloudFormation template to skip deployment for the listed AWS accounts.

**Answer: A**

**Explanation:**

This solution will meet the requirements because it will use a CloudFormation custom resource to execute custom logic during the stack set operation. A custom resource is a resource that you define in your template and that is associated with an AWS Lambda function. The Lambda function runs whenever the custom resource is created, updated, or deleted, and can perform any actions that are supported by the AWS SDK. In this case, the Lambda function can use the GuardDuty API to check whether GuardDuty is already enabled in each target account, and if not, enable it. This way, the DevOps engineer can avoid deploying the stack set to accounts that already have GuardDuty enabled, and prevent failure during the deployment.

**NEW QUESTION 115**

A company has multiple accounts in an organization in AWS Organizations. The company's SecOps team needs to receive an Amazon Simple Notification Service (Amazon SNS) notification if any account in the organization turns off the Block Public Access feature on an Amazon S3 bucket. A DevOps engineer must implement this change without affecting the operation of any AWS accounts. The implementation must ensure that individual member accounts in the organization cannot turn off the notification.

Which solution will meet these requirements?

- A. Designate an account to be the delegated Amazon GuardDuty administrator account
- B. Turn on GuardDuty for all accounts across the organization
- C. In the GuardDuty administrator account, create an SNS topic
- D. Subscribe the SecOps team's email address to the SNS topic
- E. In the same account, create an Amazon EventBridge rule that uses an event pattern for GuardDuty findings and a target of the SNS topic.
- F. Create an AWS CloudFormation template that creates an SNS topic and subscribes the SecOps team's email address to the SNS topic
- G. In the template, include an Amazon EventBridge rule that uses an event pattern of CloudTrail activity for s3:PutBucketPublicAccessBlock and a target of the SNS topic
- H. Deploy the stack to every account in the organization by using CloudFormation StackSets.
- I. Turn on AWS Config across the organization
- J. In the delegated administrator account, create an SNS topic
- K. Subscribe the SecOps team's email address to the SNS topic
- L. Deploy a conformance pack that uses the s3-bucket-level-public-access-prohibited AWS Config managed rule in each account and uses an AWS Systems Manager document to publish an event to the SNS topic to notify the SecOps team.
- M. Turn on Amazon Inspector across the organization
- N. In the Amazon Inspector delegated administrator account, create an SNS topic
- O. Subscribe the SecOps team's email address to the SNS topic
- P. In the same account, create an Amazon EventBridge rule that uses an event pattern for public network exposure of the S3 bucket and publishes an event to the SNS topic to notify the SecOps team.

**Answer: C**

**Explanation:**

Amazon GuardDuty is primarily on threat detection and response, not configuration monitoring. A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.  
<https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html> <https://docs.aws.amazon.com/config/latest/developerguide/s3-account-level-public-access-blocks.html>

**NEW QUESTION 116**

A company sells products through an ecommerce web application. The company wants a dashboard that shows a pie chart of product transaction details. The company wants to integrate the dashboard with the company's existing Amazon CloudWatch dashboards.

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

- A. Update the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction
- B. Use CloudWatch Logs Insights to query the log group and to visualize the results in a pie chart format. Attach the results to the desired CloudWatch dashboard.

- C. Update the ecommerce application to emit a JSON object to an Amazon S3 bucket for each processed transaction
- D. Use Amazon Athena to query the S3 bucket and to visualize the results in a Pie chart format
- E. Export the results from Athena Attach the results to the desired CloudWatch dashboard
- F. Update the ecommerce application to use AWS X-Ray for instrumentation
- G. Create a new X-Ray subsegment Add an annotation for each processed transaction
- H. Use X-Ray traces to query the data and to visualize the results in a pie chart format Attach the results to the desired CloudWatch dashboard
- I. Update the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction\_ Create an AWS Lambda function to aggregate and write the results to Amazon DynamoDB
- J. Create a Lambda subscription filter for the log file
- K. Attach the results to the desired CloudWatch dashboard.

**Answer: A**

**Explanation:**

The correct answer is A.

A comprehensive and detailed explanation is:

? Option A is correct because it meets the requirements with the most operational efficiency. Updating the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction is a simple and cost-effective way to collect the data needed for the dashboard. Using CloudWatch Logs Insights to query the log group and to visualize the results in a pie chart format is also a convenient and integrated solution that leverages the existing CloudWatch dashboards. Attaching the results to the desired CloudWatch dashboard is straightforward and does not require any additional steps or services.

? Option B is incorrect because it introduces unnecessary complexity and cost.

Updating the ecommerce application to emit a JSON object to an Amazon S3 bucket for each processed transaction is a valid way to store the data, but it requires creating and managing an S3 bucket and its permissions. Using Amazon Athena to query the S3 bucket and to visualize the results in a pie chart format is also a valid way to analyze the data, but it incurs charges based on the amount of data scanned by each query. Exporting the results from Athena and attaching them to the desired CloudWatch dashboard is also an extra step that adds more overhead and latency.

? Option C is incorrect because it uses AWS X-Ray for an inappropriate purpose.

Updating the ecommerce application to use AWS X-Ray for instrumentation is a good practice for monitoring and tracing distributed applications, but it is not designed for aggregating product transaction details. Creating a new X-Ray subsegment and adding an annotation for each processed transaction is possible, but it would clutter the X-Ray service map and make it harder to debug performance issues. Using X-Ray traces to query the data and to visualize the results in a pie chart format is also possible, but it would require custom code and logic that are not supported by X-Ray natively. Attaching the results to the desired CloudWatch dashboard is also not supported by X-Ray directly, and would require additional steps or services.

? Option D is incorrect because it introduces unnecessary complexity and cost.

Updating the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction is a simple and cost-effective way to collect the data needed for the dashboard, as in option A. However, creating an AWS Lambda function to aggregate and write the results to Amazon DynamoDB is redundant, as CloudWatch Logs Insights can already perform aggregation queries on log data. Creating a Lambda subscription filter for the log file is also redundant, as CloudWatch Logs Insights can already access log data directly. Attaching the results to the desired CloudWatch dashboard would also require additional steps or services, as DynamoDB does not support native integration with CloudWatch dashboards.

References:

- ? CloudWatch Logs Insights
- ? Amazon Athena
- ? AWS X-Ray
- ? AWS Lambda
- ? Amazon DynamoDB

**NEW QUESTION 118**

A company runs a workload on Amazon EC2 instances. The company needs a control that requires the use of Instance Metadata Service Version 2 (IMDSv2) on all EC2 instances in the AWS account. If an EC2 instance does not prevent the use of Instance Metadata Service Version 1 (IMDSv1), the EC2 instance must be terminated.

Which solution will meet these requirements?

- A. Set up AWS Config in the account
- B. Use a managed rule to check EC2 instance
- C. Configure the rule to remediate the findings by using AWS Systems Manager Automation to terminate the instance.
- D. Create a permissions boundary that prevents the ec2:RunInstance action if the ec2:MetadataHttpTokens condition key is not set to a value of required
- E. Attach the permissions boundary to the IAM role that was used to launch the instance.
- F. Set up Amazon Inspector in the account
- G. Configure Amazon Inspector to activate deep inspection for EC2 instance
- H. Create an Amazon EventBridge rule for an Inspector2 finding
- I. Set an AWS Lambda function as the target to terminate the instance.
- J. Create an Amazon EventBridge rule for the EC2 instance launch successful event
- K. Send the event to an AWS Lambda function to inspect the EC2 metadata and to terminate the instance.

**Answer: B**

**Explanation:**

To implement a control that requires the use of IMDSv2 on all EC2 instances in the account, the DevOps engineer can use a permissions boundary. A permissions boundary is a policy that defines the maximum permissions that an IAM entity can have. The DevOps engineer can create a permissions boundary that prevents the ec2:RunInstance action if the ec2:MetadataHttpTokens condition key is not set to a value of required. This condition key enforces the use of IMDSv2 on EC2 instances. The DevOps engineer can attach the permissions boundary to the IAM role that was used to launch the instance. This way, any attempt to launch an EC2 instance without using IMDSv2 will be denied by the permissions boundary.

**NEW QUESTION 122**

A healthcare services company is concerned about the growing costs of software licensing for an application for monitoring patient wellness. The company wants to create an audit process to ensure that the application is running exclusively on Amazon EC2 Dedicated Hosts. A DevOps engineer must create a workflow to audit the application to ensure compliance.

What steps should the engineer take to meet this requirement with the LEAST administrative overhead?

- A. Use AWS Systems Manager Configuration Compliance
- B. Use calls to the put-compliance-items API action to scan and build a database of noncompliant EC2 instances based on their host placement configuration
- C. Use an Amazon DynamoDB table to store these instance IDs for fast access

- D. Generate a report through Systems Manager by calling the list-compliance-summaries API action.
- E. Use custom Java code running on an EC2 instance
- F. Set up EC2 Auto Scaling for the instance depending on the number of instances to be checked
- G. Send the list of noncompliant EC2 instance IDs to an Amazon SQS queue
- H. Set up another worker instance to process instance IDs from the SQS queue and write them to Amazon DynamoDB
- I. Use an AWS Lambda function to terminate noncompliant instance IDs obtained from the queue, and send them to an Amazon SNS email topic for distribution.
- J. Use AWS Config
- K. Identify all EC2 instances to be audited by enabling Config Recording on all Amazon EC2 resources for the region
- L. Create a custom AWS Config rule that triggers an AWS Lambda function by using the "config-rule-change-triggered" blueprint. Modify the Lambda evaluateCompliance () function to verify host placement to return a NON\_COMPLIANT result if the instance is not running on an EC2 Dedicated Host
- M. Use the AWS Config report to address noncompliant instances.
- N. Use AWS CloudTrail
- O. Identify all EC2 instances to be audited by analyzing all calls to the EC2 RunCommand API action
- P. Invoke a AWS Lambda function that analyzes the host placement of the instances
- Q. Store the EC2 instance ID of noncompliant resources in an Amazon RDS for MySQL DB instance
- R. Generate a report by querying the RDS instance and exporting the query results to a CSV text file.

**Answer: C**

**Explanation:**

The correct answer is C. Using AWS Config to identify and audit all EC2 instances based on their host placement configuration is the most efficient and scalable solution to ensure compliance with the software licensing requirement. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. By creating a custom AWS Config rule that triggers a Lambda function to verify host placement, the DevOps engineer can automate the process of checking whether the instances are running on EC2 Dedicated Hosts or not. The Lambda function can return a NON\_COMPLIANT result if the instance is not running on an EC2 Dedicated Host, and the AWS Config report can provide a summary of the compliance status of the instances. This solution requires the least administrative overhead compared to the other options.

Option A is incorrect because using AWS Systems Manager Configuration Compliance to scan and build a database of noncompliant EC2 instances based on their host placement configuration is a more complex and costly solution than using AWS Config. AWS Systems Manager Configuration Compliance is a feature of AWS Systems Manager that enables you to scan your managed instances for patch compliance and configuration inconsistencies. To use this feature, the DevOps engineer would need to install the Systems Manager Agent on each EC2 instance, create a State Manager association to run the put-compliance-items API action periodically, and use a DynamoDB table to store the instance IDs of noncompliant resources. This solution would also require more API calls and storage costs than using AWS Config.

Option B is incorrect because using custom Java code running on an EC2 instance to check and terminate noncompliant EC2 instances is a more cumbersome and error-prone solution than using AWS Config. This solution would require the DevOps engineer to write and maintain the Java code, set up EC2 Auto Scaling for the instance, use an SQS queue and another worker instance to process the instance IDs, use a Lambda function and an SNS topic to terminate and notify the noncompliant instances, and handle any potential failures or exceptions in the workflow. This solution would also incur more compute, storage, and messaging costs than using AWS Config.

Option D is incorrect because using AWS CloudTrail to identify and audit EC2 instances by analyzing the EC2 RunCommand API action is a less reliable and accurate solution than using AWS Config. AWS CloudTrail is a service that enables you to monitor and log the API activity in your AWS account. The EC2 RunCommand API action is used to execute commands on one or more EC2 instances. However, this API action does not necessarily indicate the host placement of the instance, and it may not capture all the instances that are running on EC2 Dedicated Hosts or not. Therefore, option D would not provide a comprehensive and consistent audit of the EC2 instances.

**NEW QUESTION 126**

A large enterprise is deploying a web application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application stores data in an Amazon RDS for Oracle DB instance and Amazon DynamoDB. There are separate environments for development testing and production. What is the MOST secure and flexible way to obtain password credentials during deployment?

- A. Retrieve an access key from an AWS Systems Manager securestring parameter to access AWS service
- B. Retrieve the database credentials from a Systems Manager SecureString parameter.
- C. Launch the EC2 instances with an EC2 IAM role to access AWS services Retrieve the database credentials from AWS Secrets Manager.
- D. Retrieve an access key from an AWS Systems Manager plaintext parameter to access AWS service
- E. Retrieve the database credentials from a Systems Manager SecureString parameter.
- F. Launch the EC2 instances with an EC2 IAM role to access AWS services Store the database passwords in an encrypted config file with the application artifacts.

**Answer: B**

**Explanation:**

AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources. This service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Using Secrets Manager, you can secure and manage secrets used to access resources in the AWS Cloud, on third-party services, and on-premises. SSM parameter store and AWS Secret manager are both a secure option. However, Secrets manager is more flexible and has more options like password generation. Reference: <https://www.1strategy.com/blog/2019/02/28/aws-parameter-store-vs-aws-secrets-manager/>

**NEW QUESTION 130**

A company has an application and a CI/CD pipeline. The CI/CD pipeline consists of an AWS CodePipeline pipeline and an AWS CodeBuild project. The CodeBuild project runs tests against the application as part of the build process and outputs a test report. The company must keep the test reports for 90 days. Which solution will meet these requirements?

- A. Add a new stage in the CodePipeline pipeline after the stage that contains the CodeBuild project
- B. Create an Amazon S3 bucket to store the report
- C. Configure an S3 deploy action type in the new CodePipeline stage with the appropriate path and format for the reports.
- D. Add a report group in the CodeBuild project buildspec file with the appropriate path and format for the report
- E. Create an Amazon S3 bucket to store the report
- F. Configure an Amazon EventBridge rule that invokes an AWS Lambda function to copy the reports to the S3 bucket when a build is complete
- G. Create an S3 Lifecycle rule to expire the objects after 90 days.
- H. Add a new stage in the CodePipeline pipeline
- I. Configure a test action type with the appropriate path and format for the report
- J. Configure the report expiration time to be 90 days in the CodeBuild project buildspec file.
- K. Add a report group in the CodeBuild project buildspec file with the appropriate path and format for the report

- L. Create an Amazon S3 bucket to store the report
- M. Configure the report group as an artifact in the CodeBuild project buildspec file
- N. Configure the S3 bucket as the artifact destination
- O. Set the object expiration to 90 days.

**Answer: B**

**Explanation:**

The correct solution is to add a report group in the AWS CodeBuild project buildspec file with the appropriate path and format for the reports. Then, create an Amazon S3 bucket to store the reports. You should configure an Amazon EventBridge rule that invokes an AWS Lambda function to copy the reports to the S3 bucket when a build is completed. Finally, create an S3 Lifecycle rule to expire the objects after 90 days. This approach allows for the automated transfer of reports to long-term storage and ensures they are retained for the required duration without manual intervention<sup>1</sup>. References:  
 ? AWS CodeBuild User Guide on test reporting<sup>1</sup>.  
 ? AWS CodeBuild User Guide on working with report groups<sup>2</sup>.  
 ? AWS Documentation on using AWS CodePipeline with AWS CodeBuild<sup>3</sup>.

**NEW QUESTION 132**

A production account has a requirement that any Amazon EC2 instance that has been logged in to manually must be terminated within 24 hours. All applications in the production account are using Auto Scaling groups with the Amazon CloudWatch Logs agent configured. How can this process be automated?

- A. Create a CloudWatch Logs subscription to an AWS Step Functions application
- B. Configure an AWS Lambda function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned
- C. Create an Amazon EventBridge rule to invoke a second Lambda function once a day that will terminate all instances with this tag.
- D. Create an Amazon CloudWatch alarm that will be invoked by the login event
- E. Send the notification to an Amazon Simple Notification Service (Amazon SNS) topic that the operations team is subscribed to, and have them terminate the EC2 instance within 24 hours.
- F. Create an Amazon CloudWatch alarm that will be invoked by the login event
- G. Configure the alarm to send to an Amazon Simple Queue Service (Amazon SQS) queue
- H. Use a group of worker instances to process messages from the queue, which then schedules an Amazon EventBridge rule to be invoked.
- I. Create a CloudWatch Logs subscription to an AWS Lambda function
- J. Configure the function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned
- K. Create an Amazon EventBridge rule to invoke a daily Lambda function that terminates all instances with this tag.

**Answer: D**

**Explanation:**

"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or AWS Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format." See <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

**NEW QUESTION 133**

A growing company manages more than 50 accounts in an organization in AWS Organizations. The company has configured its applications to send logs to Amazon CloudWatch Logs. A DevOps engineer needs to aggregate logs so that the company can quickly search the logs to respond to future security incidents. The DevOps engineer has created a new AWS account for centralized monitoring. Which combination of steps should the DevOps engineer take to make the application logs searchable from the monitoring account? (Select THREE.)

- A. In the monitoring account, download an AWS CloudFormation template from CloudWatch to use in Organization
- B. Use CloudFormation StackSets in the organization's management account to deploy the CloudFormation template to the entire organization.
- C. Create an AWS CloudFormation template that defines an IAM role
- D. Configure the role to allow logs.amazonaws.com to perform the logs:Link action if the aws:ResourceAccount property is equal to the monitoring account ID
- E. Use CloudFormation StackSets in the organization's management account to deploy the CloudFormation template to the entire organization.
- F. Create an IAM role in the monitoring account
- G. Attach a trust policy that allows logs.amazonaws.com to perform the iam:CreateSink action if the aws:PrincipalOrgId property is equal to the organization ID.
- H. In the organization's management account, enable the logging policies for the organization.
- I. Use CloudWatch Observability Access Manager in the monitoring account to create a sink
- J. Allow logs to be shared with the monitoring account
- K. Configure the monitoring account data selection to view the Observability data from the organization ID.
- L. In the monitoring account, attach the CloudWatchLogsReadOnlyAccess AWS managed policy to an IAM role that can be assumed to search the logs.

**Answer: BCF**

**Explanation:**

? To aggregate logs from multiple accounts in an organization, the DevOps engineer needs to create a cross-account subscription<sup>1</sup> that allows the monitoring account to receive log events from the sharing accounts.  
 ? To enable cross-account subscription, the DevOps engineer needs to create an IAM role in each sharing account that grants permission to CloudWatch Logs to link the log groups to the destination in the monitoring account<sup>2</sup>. This can be done using a CloudFormation template and StackSets<sup>3</sup> to deploy the role to all accounts in the organization.  
 ? The DevOps engineer also needs to create an IAM role in the monitoring account that allows CloudWatch Logs to create a sink for receiving log events from other accounts<sup>4</sup>. The role must have a trust policy that specifies the organization ID as a condition.  
 ? Finally, the DevOps engineer needs to attach the CloudWatchLogsReadOnlyAccess policy<sup>5</sup> to an IAM role in the monitoring account that can be used to search the logs from the cross-account subscription.  
 References: 1: Cross-account log data sharing with subscriptions 2: Create an IAM role for CloudWatch Logs in each sharing account 3: AWS CloudFormation StackSets 4: Create an IAM role for CloudWatch Logs in your monitoring account 5: CloudWatchLogsReadOnlyAccess policy

**NEW QUESTION 136**

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 137**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **AWS-Certified-DevOps-Engineer-Professional Practice Exam Features:**

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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The AWS-Certified-DevOps-Engineer-Professional Practice Test Here](#)**