

[Home](https://www.whizlabs.com/learn) (<https://www.whizlabs.com/learn>) > [My Courses](https://www.whizlabs.com/learn/my-courses) (<https://www.whizlabs.com/learn/my-courses>)

- > [AWS Certified DevOps Engineer Professional](https://www.whizlabs.com/learn/course/aws-devops-professional-practice-test#section-1) (<https://www.whizlabs.com/learn/course/aws-devops-professional-practice-test#section-1>)
- > [CD and Process Automation](https://www.whizlabs.com/learn/course/aws-devops-professional-practice-test/quiz/14878) (<https://www.whizlabs.com/learn/course/aws-devops-professional-practice-test/quiz/14878>)
- > **Report**

## CD AND PROCESS AUTOMATION

**Attempt** 1

**Marks Obtained** 0 / 25

**Your score is** 0.0%

**Completed on** Tuesday , 29 January 2019 , 02:41 PM

**Time Taken** 00 H 00 M 04 S

**Result** Fail

### Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Continuous Delivery and Process Automation	25	0	1	24

<b>25</b> Questions	<b>0</b> Correct	<b>1</b> Incorrect	<b>24</b> Unattempted
------------------------	---------------------	-----------------------	--------------------------

Show Answers

All	▼
-----	---

A startup company has a new feature which is used to track the customers' feedback on its main website. On the website, there are product introductions and also customers are able to purchase the products and get them delivered. The development team has utilized Elastic Beanstalk to deploy the new feedback system. One developer just made a big change to the survey format and deployed the feature to a totally new Elastic Beanstalk Environment. Then he used the "Swap URL" function to switch to the new one. After monitoring the site for a day, by tracing the logs, the developer found that there were still few cases that old survey format was used even after about 12 hours. Which below explanation is correct?

- ☒ A. The Elastic Beanstalk Environment has the wrong feature branch deployed. Track the Elastic Beanstalk logs to identify if the wrong code was committed. Roll back to the old environment and delete this new one. ✕
- ☐ B. When the "Swap URL" has been triggered, Route 53 is involved to change the DNS settings. In this case a wrong CNAME may be utilized, which has resulted in the the wrong cases. The Route 53 configurations should be checked and modified.
- ☐ C. When the "Swap URL" has been utilized, Route 53 is involved to adjust the DNS Alias settings. However Route53 may have a wrong TTL settings which is too big. As a result, the DNS clients did not expire until a long timer.
- ☐ D. The "Swap URL" has used Route 53 to change the DNS settings. It may bring in some TTL issue as DNS clients may exist at various levels and not all of them obey TTL rules. ✓

Explanation :

Option D is Correct:

After Elastic Beanstalk completes the swap operation, users should verify that the new environment responds when they try to connect to the old environment URL. However, do not terminate your old environment until the DNS changes have been propagated.

Besides, DNS clients exist at various levels, and not all of them obey TTL rules. If users are dealing with mobile, particularly internationally, this is even worse. Using DNS for blue/green deployments means the switch over will not be clean, and both sets will need to be live for a much longer period of time than they should be, costing you money. Details please refer to

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

(<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>)

<https://minops.com/blog/2015/02/the-dos-and-donts-of-bluegreen-deployment/>

(<https://minops.com/blog/2015/02/the-dos-and-donts-of-bluegreen-deployment/>)

Option A is incorrect: DNS TTL issue should be suspected in this case for Swap URL and if wrong code branch was deployed, there should not be just few cases that were using wrong survey formats.

Option B is incorrect: if wrong CNAME was used, all cases should be wrong however there are only few cases that were wrong.

Option C is incorrect: TTL setting may be an issue however it should affect all users.

Besides, Swap URL has modified CNAME rather than Alias record.

Ask our Experts



QUESTION 2

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A development team is using Java/Tomcat to build up a new feature for an IOT project. They decided to create a new autoscaling group using a launch configuration that contained the latest AMI. And then they attached the new autoscaling group to the existing Classic ELB with a HTTP health check. After ELB passed the health check, they removed the old autoscaling group. Using this way, they were trying to implement

the Blue/Green deployment. However, they found that the new autoscaling did not service properly and there were lots of Tomcat errors. Which below action should be done to reduce Tomcat errors?

- ☐ A. The health check is not accurate. The classic ELB HTTP health check should point to a file that only exists after the new instances are ready to service. ✓
- ☐ B. The health check is not configured properly. The classic ELB should be replaced using an application load balancer and the HTTPs health check is required.
- ☐ C. The classic ELB or network ELB cannot meet the need. The application load balancer should be used as it is able to check the application status. In this case, the application is not ready yet when the ELB health check passed.
- ☐ D. After the new autoscaling group is created, wait for a longer time firstly so that the instances are ready to service the traffic. Then attach the autoscaling group to the ELB.

#### Explanation :

Option A is Correct:

We should use ELB health check to know when we should start sending traffic to a new set of instances. For Java apps running on Tomcat, even when the EC2 instance has finished its boot sequence, there is so much that can happen at the application level before the app is ready for traffic - initializing data structures, reading configuration, configuring logging, warming a cache. The user should create an endpoint/page in the application and let it tell you when it is ready to receive traffic. The classic HTTP health check is able to ping this new page and understand when the new instances are truly ready to service traffic.

Option B is incorrect: because classic HTTP ELB health check is able to meet the need. HTTPS is also not necessary.

Option C is incorrect: because classic HTTP ELB health check is able to meet the need.

Option D is incorrect because ELB health check should be used to avoid any manual check on the instance status.



QUESTION 3

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

The DevOps team of a big company is considering to use AWS CodeCommit rather than Github. The company has very strict security policies and it needs to consider whether or not CodeCommit is secure. They need to make sure that all new tools are able to pass their annual security audit which comes from an external organization. One key part of the audit is to check if the important data is encrypted. What should the DevOps team do to make sure that the CodeCommit pass the security audit?

- ☐ A. AWS CodeCommit repositories are already encrypted at rest however the team should configure the CodeCommit to encrypt the data in transit such as during “git push”.
- ☐ B. The team should create a key in KMS for ?CodeCommit?and ensure that ?CodeCommit?use that new created key to encrypt all data in transit and at rest.
- ☐ C. Nothing as data in AWS CodeCommit repositories is already encrypted in transit and at rest. ✓
- ☐ D. During the creation of new CodeCommit repo ensure that the setting of Encryption is enabled. Therefore both data in transit and at rest are encrypted and the audit is able to pass.

**Explanation :**

Option C is Correct:

For AWS CodeCommit repositories, the data is encrypted in transit and at rest. When data is pushed into an AWS CodeCommit repository (for example, by calling git push), AWS CodeCommit encrypts the received data as it is stored in the repository. When data is pulled from an AWS CodeCommit repository (for example, by calling git pull), AWS CodeCommit decrypts the data and then sends it to the caller.

Also CodeCommit creates an AWS-managed key in that same region in AWS Key Management Service (AWS KMS) that is used only by AWS CodeCommit (the aws/codecommit key). This key is created and stored in your AWS account. User does not need to create a new key manually for CodeCommit.

Option A is incorrect: because the data at transit is also encrypted by CodeCommit as well.

Option B is incorrect: because CodeCommit creates new key by itself. No manual work is needed.

Option D is incorrect: because there is no such settings for encryption. All data is encrypted automatically.

Ask our Experts



QUESTION 4

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A team of about 30 developers is working on a photo sharing project. Most of developers are using Github. One developer (Jeffery) has just used CodeCommit for a feature and found that it is very convenient to use. Moreover, the whole project is almost fully developed and integrated under AWS environment. Jeffery just demoed his experience to the team and they agreed to migrate all their existing developments into CodeCommit as well. Some other developers need to work on Jeffery's CodeCommit code repository too. How should the team migrate to ensure CodeCommit is used properly? Select 2.

- ☐ A. Create new CodeCommit Repo when required. Git Clone the Repo in local PCs and the use git push to the new CodeCommit Repo url such as "http://git?-codecommit.us-east-2.amazonaws.com/v1/repos/MyRepository (http://git-codecommit.us-east-2.amazonaws.com/v1/repos/MyRepository)".? After that, view files in AWS CodeCommit to see if the git push is successful.
- ☐ B. Set up new CodeCommit Repo using AWS CLI. Find the repo url which may be a HTTPS or SSH one. Use git push to upload the repo from local to CodeCommit server. After that, inspect if the files show properly in CodeCommit. ✓
- ☐ C. In order to work on existing CodeCommit Repo for other developers, create an IAM group with a suitable CodeCommit policy. Add users to that group. Then all developers are able to git clone the CodeCommit Repo and start working on their own branches. ✓
- ☐ D. To work on existing CodeCommit Repo, create an IAM user for each developer, add a CodeCommit Read policy to each user. After that, all developers are able to git clone the CodeCommit Repo and start working on their branches.
- ☐ E. Make sure that all users have full admin access so that they do not need to worry about the access of CodeCommit. Then they are able to git clone or push any new or existing CodeCommit Repo.

### Explanation :

Option B & C are Correct:

You can migrate an existing Git repository to an AWS CodeCommit repository. This process includes:

- Complete the initial setup required for AWS CodeCommit.
- Create an AWS CodeCommit repository.
- Clone the repository and push it to AWS CodeCommit.
- View files in the AWS CodeCommit repository.
- Share the AWS CodeCommit repository with your team. Refer to the below link for details:  
<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existin>

(<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existing.html#how-to-migrate-existing-share>) g.html#how-to-migrate-existing-share (<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existing.html#how-to-migrate-existing-share>)

Option A is incorrect because the CodeCommit Repo url should be a HTTPS or SSH. HTTP is incorrect.

Option D is incorrect: because the team contains 30 users so it is not proper to assign an IAM policy for each IAM user. Option C is better than Option D. This is also stated in <https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existing.html#how-to-migrate-existing-share> g.html#how-to-migrate-existing-share

(<https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-migrate-repository-existing.html#how-to-migrate-existing-share>)

Option E is incorrect because full admin access is improper as they only need the CodeCommit relevant access. This option is insecure and not a best practice.

Ask our Experts



QUESTION 5

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

The Development Lead wants to know the status of CodeDeploy in time such as DeploymentStart, DeploymentSuccess or DeploymentFailure for the deployment of an autoscaling group. One DevOps engineer is in charge of this task. He needs to make sure that most of the major CodeDeploy activities are monitored and the Development Lead is notified in a suitable manner. What below method should the DevOps engineer use to meet the Development Lead's need in a straightforward way?



- A. AWS Config should be used as it is able to show the status of every CodeDeploy activity. One SNS topic can be used to subscribe to the CodeDeploy activities in AWS Config to get the development lead notified.
- B. CodeDeploy is able to pass all its status to Cloudwatch metrics including CodeDeploy start, stop or pause. Create an alarm in the CodeDeploy metrics such as when a CodeDeploy failure happens. And then subscribe this alarm to an existing SNS topic. The SNS topic is responsible for notifying the development lead by email or SMS.
- C. Create a new Cloudtrail and use it to record all the CodeDeploy API calls. When a CodeDeploy activity happens, the development lead will be able to see the details for the CodeDeploy status. He can then filter the CodeDeploy specific events in the Cloudtrail console/CLI and understand the running status.
- D. The DevOps engineer should create a trigger in AWS CodeDeploy that publishes an Amazon Simple Notification Service (Amazon SNS) topic for the relevant AWS CodeDeploy deployment event. Then, when that event occurs, all subscribers to the associated topic will receive notifications through the endpoint specified in the topic, such as an SMS message or email message to the development lead. ✓

### Explanation :

Option D is Correct:

The requirement is that the Development Lead should be notified in time so the most straightforward way is SNS. Option C is eliminated as it can not notify the Development Lead. Option A is also incorrect because although AWS Config can record the configuration

changes, it does not report the CodeDeploy activity status. The best way is to configure SNS

directly in the AWS CodeDeploy by a trigger. This could be done via console or CLI.

The details can be found in

<https://docs.aws.amazon.com/codedeploy/latest/userguide/monitoring-sns-event-notification> (<https://docs.aws.amazon.com/codedeploy/latest/userguide/monitoring-sns-event-notifications.html>)s.html

(<https://docs.aws.amazon.com/codedeploy/latest/userguide/monitoring-sns-event-notifications.html>).

Option B is incorrect: because CodeDeploy is not a service that Cloudwatch

Metrics supports. Please refer to <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html> (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html) for the list of services that Cloudwatch Metrics supports. Please notice that Cloudwatch Logs of CodeDeploy can be used to set up SNS to provide notifications. However it is still not the easiest way if compared with Option D.

Ask our Experts



QUESTION 6

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

CodeDeploy is being used by a small company for its project. This project aims to analyze the customers' behaviors on how to choose new cars. The team decides to use a load balancer and autoscaling for its EC2 instances as the project needs a highly available and elastic environment. And at least 4 instances are supposed to work at the same time and the number may reach at 8 during the peak hour when there are some sales activities such as at Black Friday. The company's AWS engineer wants to use the in-place deployment. What below items should the AWS engineer do before creating the CodeDeploy Deployment Group in AWS console? Select 3.

- ☐ **A.** Make sure that you have a service role that trusts AWS CodeDeploy with correct permissions. This should be done before creating the Deployment Group in CodeDeploy. IAM should be involved for that by creating a new role and the role type is AWS Service. ✓
- ☐ **B.** Prepare an autoscaling group with Min 4 and Max 8 instances. Make sure that the autoscaling group has the correct autoscaling launch configurations attached. You can use the prebaked AMI to install some configuration packages for the instances. ✓

- ☐ C. Make sure the correct SNS topic is created because when CodeDeploy Deployment Group is being created, one SNS topic is required to subscribe to the CodeDeploy application, which is a mandatory step
- ☐ D. Make sure that the Elastic Load Balancer is already setup no matter it is a Classic Load Balancer, Application Load Balancer, or Network Load Balancer as the ELB will be used in the CodeDeploy Deployment Group. ✓
- ☐ E. Ensure that all instances under the autoscaling group have proper tags such as env/dev because when CodeDeploy Deployment Group is being created, EC2 tags are needed for CodeDeploy to understand the targets to deploy to.

### Explanation :

Correct Answer – A, B, D

Option A,B,D are Correct: The steps on how to use the AWS CodeDeploy console to create a deployment group for an in-place deployment is at

<https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-groups-create-in-place.html>,

(<https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-groups-create-in-place.html>),

however, Do not follow these steps if:

- You have not prepared your instances to be used in the first AWS CodeDeploy deployment of an application. To set up your instances, follow the instructions in Working with Instances for AWS CodeDeploy, and then follow the steps in this topic.
- You want to create a deployment group that uses a custom deployment configuration, but you have not yet created the deployment configuration. Follow the instructions in Create a Deployment configuration, and then follow the steps in this topic.
- You do not have a service role that trusts AWS CodeDeploy with, at minimum, the trust and permissions described in Step 3: Create a Service Role for AWS CodeDeploy. To create and configure a service role, follow the instructions in Step 3: Create a Service Role for AWS CodeDeploy, and then follow the steps in this topic.
- You want to select a Classic Load Balancer, Application Load Balancer, or Network Load Balancer in Elastic Load Balancing for the in-place deployment, but have not yet created it.

According to this, options A, B and D are correct as proper service role, autoscaling group and ELB are required for this case.

Option C is incorrect: because SNS is not a mandatory step. You could add a trigger to setup the SNS notification for the CodeDeploy environment. However it is optional.

▼ Advanced - optional

## Triggers

Delete trigger

Create trigger

Name

Events

Type

No triggers have been created for this deployment group.

Option E is incorrect: because tags are not required if the deployment target is autoscaling group. You could select the autoscaling group name as the target. Please notice that if the target is EC2 instances, tags are needed in order for CodeDeploy to understand which instances to deploy to.

☐ Amazon EC2 Auto Scaling groups

☒ Amazon EC2 instances

You can add up to three groups of tags for EC2 instances to this deployment group.

**One tag group:** Any instance identified by the tag group will be deployed to.

**Multiple tag groups:** Only instances identified by all the tag groups will be deployed to.

Tag group 1

Key	Value - optional	
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove tag"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove tag"/>
<input type="button" value="Add tag"/>		
<input type="button" value="+ Add tag group"/>		

Ask our Experts



QUESTION 7

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

The operation team in the company has recently initiated an audit to ensure that all major AWS components used are properly monitored with necessary logs, alarms and notifications. The company has also set up an on-call team to receive AWS alerts and notifications and react accordingly

when necessary. The AWS service of CodePipeline has been used as well by the development team for the new feature development. Relevant CodePipeline activities should be monitored such as the time and date of actions, the source IP address for an action, etc. What should the operation team do to ensure that CodePipeline is being properly monitored with enough logging? Select 2.

- ☐ **A.** AWS CloudTrail can be used to log AWS CodePipeline API calls and related events made by or on behalf of an AWS account. By CloudTrail, users can determine the request that was made to AWS CodePipeline, the IP address from which the request was made, who made the request, when it was made, and additional details. ✓
- ☐ **B.** AWS Cloudwatch Metrics can be used to determine CodePipeline activities. In Cloudwatch Metrics, there are CodePipeline events in the namespace of AWS/CodePipeline. Users can also create a dashboard to understand the CodePipeline status based on the metrics.
- ☐ **C.** Activate the CodePipeline Logging feature in the console. During the setup of that, the logs can be saved in real time to a S3 bucket that the operation team chooses. And the operation team can use an editor or analytic tool to open the txt files in the S3 bucket to analyze and monitor
- ☐ **D.** Amazon CloudWatch Events can be used to monitor the AWS Cloud resources including CodePipeline. The operation team can create a rule in Amazon CloudWatch Events based on CodePipeline metrics that you define such as “CodePipeline Pipeline Execution State Change”. And then use a SNS topic as the target of this Cloudwatch Event rule. ✓

### Explanation :

Correct Answer –A, D

Option A and D are Correct:

Logging and monitoring for AWS services are very important to ensure that the services are running smoothly. For CodePipeline, the below features are available in the following AWS services:

- AWS CloudTrail can be used to log AWS API calls and related events made by or on behalf of an AWS account. For more information, see ?Logging AWS CodePipeline

(<https://docs.aws.amazon.com/codepipeline/latest/userguide/monitoring-cloudtrail-logs.html>) API Calls with AWS CloudTrail

(<https://docs.aws.amazon.com/codepipeline/latest/userguide/monitoring-cloudtrail-logs.html>)?.

- Amazon CloudWatch Events can be used to monitor your AWS Cloud resources and the applications you run on AWS. You can create alerts in Amazon CloudWatch Events based on metrics that you define. For more information, see Detect and React (<https://docs.aws.amazon.com/codepipeline/latest/userguide/detect-state-changes-cloudwatch-events.html>) to Changes in Pipeline State with Amazon CloudWatch Events (<https://docs.aws.amazon.com/codepipeline/latest/userguide/detect-state-changes-cloudwatch-events.html>)

They are also the AWS CodePipeline Best Practices which are clearly stated in <https://docs.aws.amazon.com/codepipeline/latest/userguide/best-practices.html> (<https://docs.aws.amazon.com/codepipeline/latest/userguide/best-practices.html>) According to this, options A and D are correct as Cloudtrail and Cloudwatch Events are the proper tools to monitor CodePipeline activities.

Option B is incorrect: because there is no AWS/CodePipeline namespace in Cloudwatch Metrics. CodePipeline is not supported in Cloudwatch metrics as well. Refer to <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html> (<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html>)?.

Option C is incorrect: because there is no CodePipeline Logging feature. To trace the logging events, Cloudtrail/Cloudwatch Event is needed.

Ask our Experts



QUESTION 8

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

An IT consulting company starts to use CodePipeline to help manage its development lifecycle since AWS CodePipeline is a great DevOps service. They hope that starting

from CodeCommit, the pipeline is able to build the code, test the artifact?? and deploy the build automatically. They heard that CodePipeline is also very convenient to work together with Jenkins so they decided to use Jenkins as a build provider. Another reason is that they already have very strong experiences on Jenkins for their on-premise applications. ?Which one of the following options is correct?on how to use the CodePipeline together with Jenkins?

- ☐ A. Setup CodePipeline in one region and setup CodeCommit and Amazon EC2 instance key pair in another region. This is to address some safety concerns. Then create a new CodePipeline with 4 stages. In the build stage, choose "Add Jenkins" and configure correct "Provider name" and "Server URL".
- ☐ B. Make sure that all of the AWS resources for this procedure are created in the same AWS Region where you create your pipeline. Then create a new CodePipeline with 4 mandatory stages which are "Source Stage", "Jenkins Stage", "Test Stage" and "Deploy Stage".
- ☐ C. Launch an Amazon EC2 instance to host the Jenkins server and using a Secret Access Key/Access Key ID to grant the instance the required permissions for interacting with AWS CodePipeline. For the new CodePipeline configuration, make sure that Jenkins is selected as the build server in the build stage. The "Server URL" should match that in the Jenkins server however the "Provider name" can be anything.
- ☐ D. Launch an Amazon EC2 instance to host the Jenkins server and use an IAM role to grant the instance the required permissions for interacting with AWS CodePipeline. Then create a new CodePipeline. In the build stage, choose "Add Jenkins" and configure correct "Provider name" and "Server URL". ✓

#### Explanation :

Correct Answer –D

Option D is Correct:



At the moment, CodeBuild, Jenkins and Solano CI can be used as a build provider in the CodePipeline. During the setup of CodePipeline, the user needs to configure the build provider at the “Build Stage” and select Jenkins as below:

The screenshot shows the AWS CodePipeline console interface for creating a new pipeline. The breadcrumb navigation at the top reads: [Developer Tools](#) > [CodePipeline](#) > [Create new pipeline](#). On the left, a sidebar lists the steps: Step 1 (Choose pipeline settings), Step 2 (Add source stage), Step 3 (Add build stage), Step 4 (Add deploy stage), and Step 5 (Review). The 'Add build stage' step is currently active. The main content area is titled 'Add build stage' and contains a 'Build' section. Under 'Build provider', there is a description: 'This is the tool of your build project. Provide build artifact details like operating system, build spec file, and output file names.' Below this is a dropdown menu that is open, showing a search bar with a magnifying glass icon and three options: 'AWS CodeBuild', 'Add Jenkins' (which is highlighted), and 'Solano CI'. To the right of the dropdown are three buttons: 'Previous' (disabled), 'Skip', and 'Next' (active).

After “Add Jenkins” is selected, in Provider name, type the name of the action you provided in the AWS CodePipeline Plugin for Jenkins (for example `MyJenkinsProviderName`). This name must exactly match the name in the AWS CodePipeline Plugin for Jenkins. In Server URL, type the URL of the Amazon EC2 instance where Jenkins is installed. In Project name, type the name of the project you created in Jenkins, such as `MyDemoProject`, and then choose Next.

## Add Jenkins

Use the template below to connect a Jenkins instance as a build provider for pipelines in your AWS account. Before you connect your Jenkins instance, you should set up the AWS CodePipeline Plugin for Jenkins and configure it for your project. [Learn more](#)

### Provider name

Enter the provider name you configured in the Jenkins plugin

This name must match the name configured in the plugin.

### Server URL

Enter the URL for your Jenkins server

### Project name

Enter the name of the project you created in the Jenkins plugin

Cancel

Previous

Skip

Next

About the details on how to setup CodePipeline with Jenkins, refer to <https://docs.aws.amazon.com/codepipeline/latest/userguide/tutorials-four-stage-pipeline.html> (<https://docs.aws.amazon.com/codepipeline/latest/userguide/tutorials-four-stage-pipeline.html>)

Option A is incorrect: because all of the AWS resources for the CodePipeline should be in the same AWS Region where the CodePipeline is created. For example, if you create your pipeline in the US East (Ohio) Region, your Amazon S3 bucket or AWS CodeCommit repository, AWS CodeDeploy resources, and Amazon EC2 instance key pair must also be in the US East (Ohio) Region. Also, refer to <https://docs.aws.amazon.com/codepipeline/latest/userguide/tutorials-four-stage-pipeline.html> (<https://docs.aws.amazon.com/codepipeline/latest/userguide/tutorials-four-stage-pipeline.html>)

Option B is incorrect: because the stages of “Jenkins Stage” and “Test Stage” are incorrect. Also the stages are not mandatory and can be optionally skipped. The stages should be “Source Stage”, “Build Stage” and “Deploy Stage”.

Option C is incorrect: because it should not use Secret Access Key/Access Key ID for the Jenkins EC2 instance. The IAM should be used instead. Besides, both “Provider name” and “Server URL” should match those in the Jenkins server.

Ask our Experts



QUESTION 9

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Your team is developing a feature that is used to enhance the production usage rate. A DynamoDB table has been implemented to trace relevant activities such as how the feature helps boosting the usage frequency. The table has about 2k new items every day and keeps increasing. Your PM wants to have a look at the daily data in this DynamoDB table. How do you present the data to PM in a proper way?

- ☐ **A.** Create a new Data Pipeline to transfer the data from DynamoDB table to a S3. Activate the pipeline every day and then open the files in S3 using an editor.
- ☐ **B.** In the DynamoDB console, select all items, use the “Export to .csv” feature to download the whole data every day. Then use data analysis tool to manage the data.
- ☐ **C.** Create a new Data Pipeline to transfer the data from DynamoDB table to a S3. Add a schedule including a start time (8:00 AM) and end time (8:00PM) for this pipeline to run every day and collect files in S3 and get them presented to PM.

- D. Create a new Data Pipeline to transfer the data from DynamoDB table to a S3 bucket. Add a schedule for this pipeline to activate it every day at a suitable time and then open the collected files in S3. ✓

### Explanation :

Option D is Correct:


The AWS Data Pipeline lets you automate the movement and processing of any amount of data using data-driven workflows and built-in dependency checking.

You can now choose between the following options for each pipeline that you build:

- Run once
- Run a defined number of times
- Run on activation
- Run indefinitely
- Run repeatedly within a date range

When a Data Pipeline is being created, you could add a schedule such as starting every day with a start time:

#### Schedule

 You can run your pipeline once or specify a schedule. [More](#)

Run ☐ on pipeline activation  
☒ on a schedule

Run every  day(s)

Starting ☐ on pipeline activation  
☒ 2018-11-27 20:00 UTC (Current time is 00:34 UTC)  
YYYY-MM-DD HH:MM

Ending ☐ never  
☐ after  occurrence(s)  
☒ 2018-12-28 20:00 UTC (Current time is 00:34 UTC)  
YYYY-MM-DD HH:MM

To end the pipeline, you could use occurrences or a specific date. For example, the schedule will stop after 10 times or after 2 weeks.

Option A is incorrect: because in this case as the daily data is needed, the Data Pipeline should include a schedule to run otherwise it has to be run manually every day, which is not necessary.

Option B is incorrect: because you could only choose 100 items in a batch and export to a csv file. Considering that the table has 2k data and keeps increasing. This approach is not reasonable.

Option C is incorrect: because the end time is not used properly. For the schedule in Data Pipeline, the end date/time is a date/time that the whole schedule stops such as one month later. In this case, the end time of "8:00PM" is invalid and not required. Instead, you could add an ending date in which the whole schedule stops as required. Please also refer to <https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-object-schedule.html> (<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-object-schedule.html>) on how to use the end time.

Ask our Experts



QUESTION 10

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Your team is using an Elastic Beanstalk environment for a web production. The project needs to read/write to a PostgreSQL RDS database which other productions are using as well. Other than that, the Elastic Beanstalk environment uses Immutable deployment and totally new instances need to be created for new deployments. Which ways are suggested to connect to RDS database for this Elastic Beanstalk environment.

- ☐ A. For the Elastic Beanstalk, it is not possible to connect to a RDS instance if it is for production environment.
- ☐ B. You could add this RDS database to Elastic Beanstalk using the database configuration card in the console. Type in the correct username, password, instance class and other information.
- ☐ C. You could not add this RDS database to Elastic Beanstalk as Elastic Beanstalk does not support PostgreSQL.

- ☐ D. Since it is for production, it is suggested to put the RDS database outside of the Elastic Beanstalk environment. This can be done by using your application to connect to it on launch. ✓

### Explanation :

Option D is Correct:

AWS Elastic Beanstalk provides support for running Amazon Relational Database Service (Amazon RDS) instances in your Elastic Beanstalk environment. This works great for development and testing environments. However, it isn't ideal for a production environment because it ties the lifecycle of the database instance to the lifecycle of your application's environment.

For more information, refer to

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html>

(<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html>)

Option A is incorrect because it is still possible for the production environment.

Option B is incorrect: because this is a proper way if it is for development and test.

However this question talks about the Elastic Beanstalk environment for a production. For how to connect to the RDS in a Elastic Beanstalk environment, please refer to

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.db.html#using-features.managing.db.CON>

Option C is incorrect: because you can use Elastic Beanstalk to add a MySQL, PostgreSQL, Oracle, or SQL Server database to your environment during or after environment creation. In this case, we should put the RDS instance outside of the Elastic Beanstalk environment.

Ask our Experts



QUESTION 11

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Elastic Beanstalk environment has been used for your team recently for a feature development based on Java. When the team firstly created the environment, they were using a single instance as they did not consider the capacity. However, after a while you find that the application needs to

consume more memory and CPU than being expected sometimes during traffic spike. As a result, the application has some performance issues. Your AWS solution architect suggests you use multiple instances rather than one. What should you do?

- ☐ A. Change your environment type to a high available environment by editing your environment's configuration. In the Elastic Beanstalk console, select the environment, add multiple instances with autoscaling based on MemoryUtilization.
- ☐ B. Destroy the environment. Create a new environment type that has multiple instances as your old environment cannot be modified to a multiple instances environment.
- ☐ C. Modify the environment's capacity settings to a load balanced environment type with autoscaling. Select all availability zones. Also add a scaling trigger if average CPUUtilization is over 85% for a 5 minutes period. ✓
- ☐ D. Edit your environment's capacity configuration to a load balanced environment type. Make sure that all availability zones are selected. Add a scaling event when median CPUUtilization is over 85% for a period of 1 minute.
- ☐ E. Modify the instance type to t2.large to meet the need of high CPU and memory.

#### Explanation :

Option C is Correct:

In AWS Elastic Beanstalk, you can create a load-balancing, autoscaling environment or a single-instance environment. The type of environment that you require depends on the application that you deploy. For example, you can develop and test an application in a single-instance environment to save costs and then upgrade that environment to a load-balancing, autoscaling environment when the application is ready for production.

For more information, refer to

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html> (<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>)

To use Amazon EC2 Auto Scaling effectively, configure triggers that are appropriate for your application, instance type, and service requirements. You can scale based on several statistics including latency, disk I/O, CPU utilization, and request count. Refer to <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-triggers.html> (<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-triggers.html>)

for the Elastic Beanstalk AutoScaling triggers.

Option A is incorrect because MemoryUtilization is NOT a scaling trigger for Elastic Beanstalk multi instances environment. The valid triggers include CPUUtilization, NetworkIn, Latency, DiskReadOps, etc.

Option B is incorrect because you do not need to destroy this existing one to change the environment type.

Option D is incorrect because the valid statistics for scaling trigger are Max, Min, Sum and average. Median is not a valid one. Refer to the below:

### Scaling triggers

The screenshot shows the 'Scaling triggers' configuration page in the AWS Management Console. It features several fields for configuring a scaling trigger:

- Metric:** A dropdown menu with 'CPUUtilization' selected. A tooltip is visible next to it that says 'to determine if the environment's capacity is too low or too high.'
- Statistic:** A dropdown menu with 'Average' selected and marked with a checkmark. A tooltip below it says 'Choose how the metric is interpreted.'
- Unit:** A dropdown menu with 'Bytes' selected.
- Period:** A field with '5' and a 'Min' button. A tooltip below it says 'The period between metric evaluations.'
- Breach duration:** A field with '5' and a 'Min' button. A tooltip below it says 'The amount of time a metric can exceed a threshold before triggering a scaling operation.'

Option E is incorrect: because you are unsure if t2.large instance type is able to meet the need. Also the traffic is not stable so that a higher capacity instance type is not cost effective. The best solution is to use the auto scaling environment that Elastic Beanstalk provides.



Ask our Experts



QUESTION 12

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Your R&D team is doing some research on how to use Elastic Beanstalk for a legacy product. The legacy product is using Java application and also Nginx. Your AWS solution architect suggests using Multidocker environment. How should you implement that in the Elastic Beanstalk?

- ☐ A. Use two dockerfiles for the multidocker environment. One for Java and one for Nginx.
- ☐ B. Use dockerrun.aws.json v1 for the multidocker environment. This file describes the containers to deploy to each container instance.
- ☐ C. Use dockerrun.aws.json v2 for the multidocker environment. This file describes the containers to deploy to each container instance. ✓
- ☐ D. Use .ebextension config files to describe the multidocker environment.

#### Explanation :

Option C is Correct:

A Dockerrun.aws.json file is an Elastic Beanstalk-specific JSON file that describes how to deploy a set of Docker containers as an Elastic Beanstalk application. You can use a Dockerrun.aws.json file for a multicontainer Docker environment.

AWSEBDockerrunVersion is 2 for the multicontainer Docker environments.

For more information, refer to

[https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create\\_deploy\\_docker\\_v2config.html](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker_v2config.html)  
([https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create\\_deploy\\_docker\\_v2config.html](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker_v2config.html))

Option A is incorrect because dockerfile can be used only for a single docker environment.

Option B is incorrect: because V2 should be used for multi docker environment.

Option D is incorrect: because for docker environment, Dockerrun.aws.json should be

used rather than .ebextension config files.

Ask our Experts



QUESTION 13

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A designer is preparing for a demo to the development lead. He is using a Cloudformation template as the template could be version controlled. He wants the template to be able to get the SSH Key as a user input in order to SSH to an EC2 instance that will be created by the Cloudformation stack later on. Which below approach is the proper one to make this happen?

- ☐ A. Design the template using XML format and add a parameter as the SSH Key. Refer to this parameter for new EC2 instances.
- ☐ B. Use an editor to write a template using JSON, Add a parameter section for the SSH Key such as "MyKeyPair". For new instances, use the keyword of "Ref" to use this parameter. Save the template in S3 and upload it during stack creation. ✓
- ☐ C. In the template editor that has been provided by AWS, design the template using YAML. Add a parameter for the SSH Key such as "MyKeyPair". For new instances, use the keyword "Reference" to link to the "key" parameter.
- ☐ D. Design the template using YAML format. Add a parameter called "MyKeyPair" with the "Type" as "Key". For new EC2 instances, use the keyword of "Ref" to refer to this parameter in the Metadata section. Save the template in a S3 and refer to the S3 link during stack creation.

**Explanation :**

Option B is Correct:

You can author AWS CloudFormation templates in JSON or YAML formats.

For more information, refer to

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-formats.html>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-formats.html>)

The optional Parameters section is used to customize your templates. Parameters enable you to input custom values to your template each time you create or update a stack.

You use the **Ref** intrinsic function to reference a parameter, and AWS CloudFormation uses the parameter's value to provision the stack. You can reference parameters from the Resources and Outputs sections of the same template.

The below is an example of using "MyKeyPair" as a parameter:

```
{
  "Parameters": {
    "MyImageId": {
      "Description": "Image id",
      "Type": "String"
    },
    "MyKeyPair": {
      "Description": "Key Pair",
      "Type": "String"
    }
  },
  "Resources": {
    "MySecurityGroup": {
      "Type": "AWS::EC2::SecurityGroup",
      "Properties": {
        "GroupDescription": "Security Group with Ingress Rule for MyInstance",
        "SecurityGroupIngress": [
          {
            "IpProtocol": "tcp",
            "FromPort": "22",
            "ToPort": "22",
            "CidrIp": "0.0.0.0/0"
          }
        ]
      }
    },
    "MyInstance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId": { "Ref": "MyImageId" },
        "SecurityGroups": [
          { "Ref": "MySecurityGroup" }
        ],
        "KeyName": { "Ref": "MyKeyPair" }
      }
    }
  }
}
```

Option A is incorrect: because XML cannot be used for Cloudformation template.

Option C is incorrect: because the keyword to refer to parameter is “Ref” rather than “Reference”.

Option D is incorrect: because for Parameter, the type should be a string for this case. The type of “Key” is wrong. Please refer to

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section->

<http://https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section->

[structure.html](http://https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-) for the structure of parameter section. Other than that, to use the parameter for instances, the “Ref” should be put into “Properties” section rather than “Metadata”.

Ask our Experts



QUESTION 14

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A solutions architect of an IT company is considering to use CodeStar for a new project that needs high scalability and availability. More importantly, he prefers utilizing its powerful management features so that he could control the whole project status including team membership. The team that is working on this project contains 3 developers and 1 UI designer.

The UI designer only needs read access for the CodeStar project board. Moreover, a Scrum Master needs to monitor the project dashboard from time to time. Which below option is correct in terms of managing the team membership in CodeStar properly?

- ☐ A. In CodeStar management console, on the “Team members” page, add the developers as Contributor, add the UI designer as Viewer and add the scrum master as Moderator.

- B. For each IAM user, in the IAM console, attach relevant CodeStar policies. For example, add the below policy for the solutions architect who is the admin: { "Version": "2012-10-17", "Statement": [ { "Sid": "AdminPolicy", "Effect": "Allow", "Action": "codestar:\*", "Resource": "\*" } ] }
- C. For each IAM user, in the IAM console, attach relevant CodeStar policies. For example, add the below policy for the admin: { "Version": "2012-10-17", "Statement": [ { "Sid": "AdminRole", "Effect": "Allow", "Action": [ "codestar:DeleteProject", "codestar:DisassociateTeamMember", "codestar:AssociateTeamMember", "codestar:UpdateTeamMember", "codestar:CreateProject" ], "Resource": "\*" } ] }
- D. In CodeStar management console, on the “Team members” page, add the developers as Contributor, add the UI designer and the scrum master as Viewer as both of them need read-only access ✓

### Explanation :

Correct Answer – D

One key feature of CodeStar is that you could **Add Team Members** to an AWS CodeStar Project.

If you have the owner role in an AWS CodeStar project or have the AWSCodeStarFullAccess policy applied to your IAM user, you can add other IAM users to the project team. This is a simple process that applies an AWS CodeStar role (owner, contributor, or viewer) to the user. These roles are per-project and can be customized. Benefits of AWS CodeStar roles and team membership include:

- You do not have to manually configure permissions in IAM for your team members.
- You can easily change a team member's level of access to a project.
- Users can access project dashboards in the AWS CodeStar console only if they are team members.
- User access to a project is defined by role.

And details please refer to

<https://docs.aws.amazon.com/codestar/latest/userguide/how-to-add-team-member.html> (<https://docs.aws.amazon.com/codestar/latest/userguide/how-to-add-team-member.html>).

Option A is incorrect: Because there is no role of Moderator in CodeStar. For read-only access, the role of Viewer is needed.

Option B and C are incorrect: For CodeStar, the proper method to manage team membership is to use its "Team members" dashboard or CLI to allocate roles.

Ask our Experts



QUESTION 15

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

You are just promoted to be the Scrum Master of a new team. You want to try something new and start using CodeStar because of its wonderful project management features. You plan to create a sample project using Node.js template which CodeStar provides and demo to other team members. You create the demo project successfully and the Node.js project is deployed smoothly in Lambda. The project code is in CodeCommit. Later on you want to change the lambda resource name from "XXX-GetHelloWorld" to "XXX-DemoProject". What option should you use?

- ☐ A. As CodeStar has used CodeCommit as its Git repo, you should pull the code from CodeCommit and make relevant changes in buildspec.yml via a Git Commit. Then CodeBuild is able to rebuild the Lambda using the updated name and CodeStar will take care of the following deployment.
- ☐ B. Unfortunately, you could not change the Lambda name as you chose to use the sample template which is read-only for demo purpose.
- ☐ C. In this case, as CodeStar has used CodeCommit to manage the code repo, you can modify application resource name in the template.yml file in the CodeCommit Repo. This is also the AWS CloudFormation file that models your application's runtime environment. ✓

- D. The CodeStar template has created resources including lambda using its predefined name. To change the lambda name, you have to go to the lambda console and re-upload the code directly with the updated name.

### Explanation :

Correct Answer – C

Instead of manually modifying an infrastructure resource, use AWS CloudFormation to model and deploy your application's runtime resources.

You can modify or add an application resource, such as a Lambda function, in your runtime stack by editing the **template.yml** file in your project repository. You can add any resource that is available as a AWS CloudFormation resource. For example, you could modify the Lambda resource name in below code:

```
24
25 Resources:
26   GetHelloWorld:
27     Type: AWS::Serverless::Function
28     Properties:
29       Handler: index.get
30       Runtime: nodejs8.10
31       Role:
32         Fn::GetAtt:
33           - LambdaExecutionRole
34           - Arn
35       Events:
36         GetEvent:
37           Type: Api
38           Properties:
39             Path: /
40             Method: get
41   LambdaExecutionRole:
42     Description: Creating service role in IAM for AWS Lambda
43     Type: AWS::IAM::Role
44     Properties:
45       RoleName: !Sub 'CodeStar-${ProjectId}-Execution${Stage}'
```

Details please refer to

<https://docs.aws.amazon.com/codestar/latest/userguide/templates.html#update-project>

(<https://docs.aws.amazon.com/codestar/latest/userguide/templates.html#update-project>).

Option A is incorrect: Because buildspec.yml is for CodeBuild instead of CloudFormation.

Lambda belongs to CloudFormation stack so that template.yml is needed.

Option B is incorrect: Because you can still modify the sample code by changing the code in CodeCommit or Github repo.

Option D is incorrect: For CodeStar, although manually changing Lambda resource could work, it is not a good practice. Managing resources in CloudFormation is suggested so that the structure is regarded as Code and can be properly managed.

Ask our Experts



QUESTION 16

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Two Java developers are building up a short-term project using CodeStar as CodeStar is able to provide a clear dashboard to help control the project and hook up AWS services such as CodeCommit, CodePipeline, etc.

Their favourite IDE is Eclipse so they want to use that to directly make code changes and develop software in the AWS CodeStar project. They already got the AWS toolkit installed in Eclipse. Which below options are needed to ensure that they can use Eclipse properly with AWS CodeStar? Select 3.

- ☐ A. The developers must be members of the AWS CodeStar project team with the owner so that they are able to pull/submit the code.
- ☐ B. An IAM role that has enough AWS CodeStar permissions is added to Eclipse.
- ☐ C. Git credentials (user name and password) for the IAM users that the developers use. ✓
- ☐ D. The developers must be members of the AWS CodeStar project team with the owner or contributor role. ✓



- ☐ E. IAM users that have been added to an AWS CodeStar project as team members. ✓

### Explanation :

Correct Answer – C, D, E

If the AWS CodeStar project stores its source code in AWS CodeCommit, the user must also be a member of the AWS CodeStar project team with the owner or contributor role.

To use Eclipse, the user also need:

- An IAM user that has been added to an AWS CodeStar project as a team member.
- If the AWS CodeStar project stores its source code in AWS CodeCommit, Git credentials (<https://docs.aws.amazon.com/codestar/latest/userguide/getting-started.html#git-credentials>) (user name and password) for the IAM user.
- Sufficient permissions to install Eclipse and the AWS Toolkit for Eclipse on your local computer.

The details please refer to

<https://docs.aws.amazon.com/codestar/latest/userguide/setting-up-ide-ec.html>

(<https://docs.aws.amazon.com/codestar/latest/userguide/setting-up-ide-ec.html>).

According to this, Option C, D, E are needed at the same time. For Git credentials, refer to the below:

AWS CodeStar Project Checkout

### AWS CodeStar Project Selection

Select the AWS CodeStar project you want to checkout from the remote host.

Select AWS account and region:

Select Account:  [Configure AWS accounts...](#)

Select Region:

Select AWS CodeStar project and repository:

Project Name	Project ID	Project Description
My First Project	my-first-projec	AWS CodeStar created project

Select repository:

Configure Git credentials:

You can manually copy and paste Git credentials for AWS CodeCommit below. Alternately, you can import them from a downloaded .csv file. To learn how to generate Git credentials, see [Create Git Credentials for HTTPS Connections to AWS CodeCommit](#).

User name:

Password:

☐ Show password

Option A is incorrect: Because contributor role also works.

Option B is incorrect: Because the user does not need to add any role into Eclipse. For Eclipse AWS toolkit, an AWS profile configured with an access key and secret key is needed.

If the user does not have an AWS profile configured with an access key and secret key on the computer, choose **Configure AWS accounts** and follow the instructions.

Ask our Experts



QUESTION 17

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

OpsWorks is being used by a developer to setup a short term project. Basically, this project is about an independent component that needs to talk with other domains that are owned by other teams. One of them is a RDS MySQL database that records some important information such as user states. This database is owned and maintained by the operation team.

The OpsWorks stack has configured a linux Node.js layer for this project and relevant recipes are in place. What action should be performed by developer to connect with the MySQL database?

- ☐ A. Associate the Amazon RDS database server when the developer create the app or later by editing the app. When the app is deployed, AWS OpsWorks Stacks creates a file on each of the built-in application server instances containing the connection data. Then a custom recipe can be used to extract the connection information from the deploy attributes and put it in a file that can be read by the application. ✓
- ☐ B. The developer can only associate the Amazon RDS database server with an app when the app is created otherwise he has to rebuild the whole stack. When the app is deployed, AWS OpsWorks Stacks creates a file on each of the built-in application server instances containing the connection data. The application can read the deploy attributes and use them to connect to the database server.
- ☐ C. The developer can edit the app if he does not associate the database when creating the app. Under the lifecycle of Configure, AWS OpsWorks Stacks creates a file on each of the built-in application server instances containing the connection data. Then a recipe can be used to extract the connection information from the configure attributes and put it in a file that can be read by the application.

- ☐ D. The developer can only associate the Amazon RDS database server with an app when the app is created otherwise he has to rebuild the whole stack. After the RDS is associated, EC2 instances are able to connect with MySQL database automatically as long as proper roles have been attached to the application stack.

### Explanation :

Correct Answer-A

First, You can associate an Amazon RDS database server with an app when you create the app or later by editing the app.

Secondly, When you deploy an app, for Linux stacks, AWS OpsWorks Stacks creates a file on each of the built-in application server instances containing the connection data.

An application can use the connection information from the instance's deploy attributes to connect to a database. However, applications cannot access that information directly—only recipes can access the deploy attributes. You can address this issue by implementing a custom recipe that extracts the connection information from the deploy attributes and puts it in a file that can be read by the application. Details please refer to <https://docs.aws.amazon.com/opsworks/latest/userguide/workingapps-connectdb.html> (<https://docs.aws.amazon.com/opsworks/latest/userguide/workingapps-connectdb.html>).

Option? B is? incorrect: Because you can associate the database by editing the app after the app is created.

Option? C is? incorrect: Because it is not the lifecycle of Configure. When the app is deployed, the connection data is recorded under the file with deploy attributes.

Option? D is? incorrect: Because application still needs to get the credentials to connect to the MySQL database. It won't connect without knowing the login details.

Ask our Experts



A large finance company is utilizing OpsWorks for a website project. The website is already online for half a year. According to statistics, the average request volume varies sinusoidally over the day. The minimum average request volume requires five application server instances.

Starting from 12AM the load goes up gradually with about two more instances needed every hour and reaches the highest at 12PM. About 16 instances are needed maximum however there are chances for the spike that 1 or 2 more instances are required.

Starting from 12PM, the workload goes down gradually and reaches the lowest at 12AM. Which below option is suggested to manage the instances in the OpsWorks stack?

- ☐ A. The stack should have three 24/7 instances, which are always on and handle the base load. Add 12 schedule instances and modify the number of schedule instances every two hours, Add 2 spot instances to handle traffic spikes.
- ☐ B. The stack should have three On Demand instances, which are used to serve the base load. Add 12 schedule instances and modify the number of schedule instances every two hours. Add 2 spot instances to handle traffic spikes.
- ☐ C. The stack should have three 24/7 instances to handle with base load. Add an EC2 autoscaling group to OpsWorks Stack and make sure that the launch configuration is proper. The autoscaling group is able to handle with the load change automatically. No other instances types are required.
- ☐ D. The stack should have three 24/7 instances, which are always on and handle the base load. Add 12 time-based instances and modify the number of time-based instances every two hours. Add 2 load-based instances to handle traffic spikes. ✓

#### Explanation :

Correct Answer – D

AWS OpsWorks Stacks provides three ways to manage the number of server instances.

- 24/7 instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-starting.html>) are started manually and run until they are manually stopped.

- Time-based instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autoscaling.html>) are automatically started and stopped by AWS OpsWorks Stacks on a user-specified schedule.

- Load-based instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autoscaling.html>) are automatically started and stopped by AWS OpsWorks Stacks when they cross a threshold for a user-specified load metric such as CPU or memory utilization.

If you are managing stacks with more than a few application server instances, it is recommended to use a mix of all three instance types.

<https://docs.aws.amazon.com/opsworks/latest/userguide/best-practices-autoscale.html> (<https://docs.aws.amazon.com/opsworks/latest/userguide/best-practices-autoscale.html>)

has discussed this scenario in details.

Option A is incorrect: Because schedule instances and spot instances should not be used for OpsWorks stack.

Option B is incorrect: Because On demand/schedule/spot are EC2 instance types instead of OpsWorks instance types.

Option C is incorrect: Because it is improper to use EC2 autoscaling to maintain instance volume in OpsWorks. You can still configure that according to

<https://aws.amazon.com/blogs/devops/auto-scaling-aws-opsworks-instances/> (<https://aws.amazon.com/blogs/devops/auto-scaling-aws-opsworks-instances/>)

however it is not a straightforward approach. The best practice suggested by AWS is using 24/7 instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-starting.html>)/Time-based instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autoscaling.html>)/Load-based instances

(<https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autoscaling.html>) to optimize the Number of Application Servers.

**Ask our Experts**



A new development team is building up a web application to provide discount coupons to customer. They wrote a CloudFormation template to build up the infrastructure, 5 large Amazon linux EC2 instances, RDS, etc.

Later on they found that an autoscaling configuration needs to be updated. One of the developers edited the template in his PC, uploaded the template to S3 and updated the CloudFormation stack later on.

Which of the following should be considered as a first priority so as to adhere to the best practices of CloudFormation usage?

- ☐ A. The developer should edit the template in the CloudFormation console directly rather than his PC as the console has provided various features to help on the edit.
- ☐ B. The team should use revision control to manage the CloudFormation template for example using GitHub otherwise it is hard to track who and how the changes are made. The changes need code reviews as well to ensure the quality. ✓
- ☐ C. The developer should update the instance regularly. On all the Amazon EC2 Linux instances and Amazon EC2 Linux instances created with AWS CloudFormation, regularly run the yum update command to update the RPM package. This ensures that you get the latest fixes and security updates.
- ☐ D. In the template, use more intrinsic functions such as FN::BASE64, FN::Join, etc. These functions are able to help build up a clean and efficient template.

Explanation :

Correct Answer – B

About the AWS CloudFormation best practices, please refer to <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#code> (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#code)

on the details. For this case, the main problem is that there is no revision control as the developer just edits the template on his own and uploads directly. One best practice of CloudFormation template is to Use Code Reviews and Revision Controls to Manage Your Templates.

The stack templates describe the configuration of your AWS resources, such as their property values. To review changes and to keep an accurate history of your resources, use code reviews and revision controls. These methods can help you track changes between different versions of your templates, which can help you track changes to your stack resources. Also, by maintaining a history, you can always revert your stack to a certain version of your template.

Other options are partial correct to some extent however they are not first priority.

Option A is incorrect: It indeed helps when the template is edited in the console as some editor features can be used, however it is not necessary and not first priority for this case.

Option C is incorrect: because the case does not mention how the instances are updated and it is not a first priority either.

Option D is incorrect: Using intrinsic functions can help on the template however again they are not necessary and the case does not mention whether or not intrinsic functions are lacking.

Ask our Experts



QUESTION 20

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

The company that you are working for has strong security policies. And for AWS services, they want to track all API calls if possible. One team has just started using CloudFormation to migrate their legacy application to AWS.



The application is a PHP one that talks with MySQL database which will be deployed together with the CloudFormation. Which option is able to help on the security audit for the CloudFormation implementation?

- ☐ A. Create a new CloudTrail and configure a S3 bucket for the trail. By default, CloudFormation service is included and all CloudFormation API calls will be recorded as CloudTrail events. The events contain lots of useful information that security team cares about. ✓
- ☐ B. Create a new CloudTrail trail and configure a S3 bucket. Include the CloudFormation service for the new trail. All relevant CloudFormation API call informations are recorded such as Parameter names, Parameter values, IAM roles and Tags used during stack creation.
- ☐ C. The CloudTrail actually does not support CloudFormation specific api calls. For example, when CloudFormation stack is created or updated, the relevant events are not recorded in CloudTrail. The trail only captures the API events for resources that CloudFormation has created.
- ☐ D. For CloudFormation tracking, it is suggested to use AWS Config as it is able to monitor all CloudFormation activities such as stack creation, stack update and stack deletion.

#### Explanation :

Correct Answer - A

For API tracking in AWS, the first service to think about should be CloudTrail. Option D is eliminated. And CloudTrail supports CloudFormation and all API calls are recorded as event. For Option B, it is partially correct as "Only the input parameter key names are logged; no parameter values are logged." About how to use CloudTrail to track CloudFormation API calls, refer to

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-api-logging-cloudtrail.html>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-api-logging-cloudtrail.html>).

The below event is one for stack creation. It only has the parameter name:

```
"stackName": "my-test-stack",  
"disableRollback": true,  
"parameters": [  
  {
```

```
"parameterKey": "password"
},
{
  "parameterKey": "securitygroup"
}
]
```

Option B is incorrect: CloudTrail events do not record the parameter values for CloudFormation.

Option C is incorrect: because CloudTrail supports CloudFormation and is able to record its API calls.

Option D is incorrect: To trace API calls, the main service should be CloudTrail.

Ask our Experts



QUESTION 21

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

Last week, a developer has changed the name of an Amazon PostgreSQL RDS database instance from “employeeDatabase” to “employee\_DB” and then updated the CloudFormation stack.

However during the stack update, it was found that AWS CloudFormation created a new database and deleted the old one. This has resulted in the loss of data in the old database. Which below action can the team perform to prevent this from happening in the future?

- ☐ A. Use Change Sets to check how your changes might impact your running resources, especially for critical resources such as RDS. Change Sets is also able to tell if the stack update is successful or not so that it can greatly help on the CloudFormation resources management.

- ☐ B. Make sure that all RDSs are protected in the DeletePolicy by using “Keep” keyword then they are protected from deletion when stack update is happening. You could then make a snapshot of the the RDS to backup data to use in the future.
- ☐ C. Use a data pipeline to copy the data from RDS to S3 for backup before executing any stack update. By using this way, the RDS instance data is saved in a suitable manner.
- ☐ D. Create a new Change Set and use it to identify what changes may happen. Do the necessary backup before executing the Change Set. If everything is good, execute the Change Set and use the CloudFormation console to monitor. ✓

### Explanation :

Correct Answer – D

Change Sets is typically used to understand what changes may happen due to a stack update so that some unexpected consequences can be avoided. Refer to <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>)

on how to use Change Sets.

Option A is incorrect: It is proper to use Change Sets. However “Change sets don't indicate whether AWS CloudFormation will successfully update a stack.” This is stated in <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>). Change Sets is NOT able to tell whether the stack update is successful.

Option B is incorrect: Although DeletePolicy should be good to use, the keyword for RDS instance should be “Retain” rather than “Keep”.

To prevent deletion or updates to resources in a CloudFormation stack, you can:

- Set DeletionPolicy attributes to retain certain resources when the stack is deleted.
- Enable Termination Protection to prevent the stack from being deleted.
- Use a stack policy to prevent update actions (modify, replace, or delete) to resources in the stack.
- Apply IAM policies to allow only certain users to delete or update resources.

Option C is incorrect: Data pipeline is not a good use case for CloudFormation stack to keep resources.

Ask our Experts



QUESTION 22

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A developer is quite new to CloudFormation and he is trying to use CloudFormation for his new assignment which is a web service in the Sydney region only.

He needs to use an AMI id in the Sydney region to create EC2 instances with an Elastic Load Balancer in the template. What should he do to make this happen?

- ☐ A. In order to use AMI Id, the template needs to have a “mapping” which is inside the “Resources” section so that the template understand which AMI ID to be used during stack creation. The intrinsic function “FindInMap” is needed in the template to work with “mapping”.
- ☐ B. Use a parameter for the user to input the AMI ID when the stack is created. Make sure that the parameter has the type as `AWS::EC2::Image::Id`. ✓
- ☐ C. In the template, add a parameter section for the AMI ID. The type of the parameter should be a String. Make sure that proper limitations are added such as the maximum length, minimum length, etc.
- ☐ D. In the template, add a mapping section for all possible AMI IDs in all regions so that the CloudFormation does not need to remember any AMI IDs manually. Then in the Resource section, use `FN::FindInAMI` to refer the correct AMI ID.

### Explanation :

Correct Answer – B

Mapping and “FN::FindInMap” are good to use for AMI IDs however in this case, only 1 AMI ID is needed in a unique region so that mapping and FN::FindInMap are not necessary.

Besides, “Mapping” does not belong to “Resources” section so that option 1 is eliminated.

Another mistake for Option D is that the correct function should be “FN::FindInMap”.

The proper method is to use Parameter. Especially when the parameter is a AWS specific parameter type such as AMI ID, the AWS specific parameter type should be used. Details please refer to

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html#aws-specific-parameter-types>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html#aws-specific-parameter-types>). In this case, the parameter should use AWS::EC2::Image::Id as the parameter type.

Option A & D are incorrect and explained as above.

Option C is partially correct because the AWS specific parameter type should be used. In this case, it should be AWS::EC2::Image::Id. Option B is better than C.

Ask our Experts



QUESTION 23

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A big retail company A has various web/non-web services to support its routine companywide operations. The applications are using various EC2 instance types such as Amazon Linux EC2, Ubuntu EC2 and Windows Server 2016. There are also several on-premise linux Redhat servers. The DevOps team has used AWS service for 3 years and is considering to explore ECS service on these applications.

The team understands that the ECS agent is needed in order for these instances to work with ECS cluster. Which below option is correct in terms of how to set up ECS agent on these existing servers?

- ☐ A. For Amazon Linux and Ubuntu EC2 instances, the ECS agent can be installed using a package. However for Windows Server EC2 and on-premise Redhat server, unfortunately the ECS agent cannot be installed since the agent only works on linux.
- ☐ B. All the AWS EC2 instances and on-premise Redhat servers can install the ECS agent. The ECS agent is open sourced in Github and has detailed instructions.
- ☐ C. For EC2 instances including Amazon Linux, Ubuntu and Windows, the ECS agent can be installed. However for on-premise Redhat server, unfortunately the ECS agent cannot be installed since Amazon ECS container agent is only supported on Amazon EC2 instances. ✓
- ☐ D. Only Amazon ECS-optimized AMIs can use ECS agent and have that agent installed. Unless those EC2 instances can be replaced with ECS-optimized AMIs, they cannot use ECS services since there is no way to install ECS agent.

### Explanation :

Correct Answer – C

The Amazon ECS container agent allows container instances to connect to your cluster.

The Amazon ECS container agent is included in the Amazon ECS-optimized AMIs, but you can also install it on any Amazon EC2 instance that supports the Amazon ECS specification.

**One thing to note is that the Amazon ECS container agent is only supported on Amazon EC2 instances.** The source code for the Amazon ECS container agent is available on GitHub (<https://github.com/aws/amazon-ecs-agent>). It has listed the details on how to install/configure agent in linux and windows.

Some details also refer to

[https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS\\_agent.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_agent.html)  
([https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS\\_agent.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_agent.html)).

Option A is incorrect because Windows EC2 instance can install the agent as well.

Option B is incorrect because on-premise instances cannot install the agent. The ECS service only works for EC2 instances.

Option D is incorrect because although it is true that the Amazon ECS container agent is included in the Amazon ECS-optimized AMIs, you can also install it on other EC2 instances.

Ask our Experts



QUESTION 24

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

You are a new graduate and are trying to get an AWS DevOps job. To prepare for a tech interview, the recruiter has given you a task to use AWS to build up a Hello World web service in one week.

The requirement is that the project needs to use the services of CodeCommit, CodePipeline, CodeBuild, CloudFormation and ECS. Which below option should you use to finish the assignment in the most suitable way?

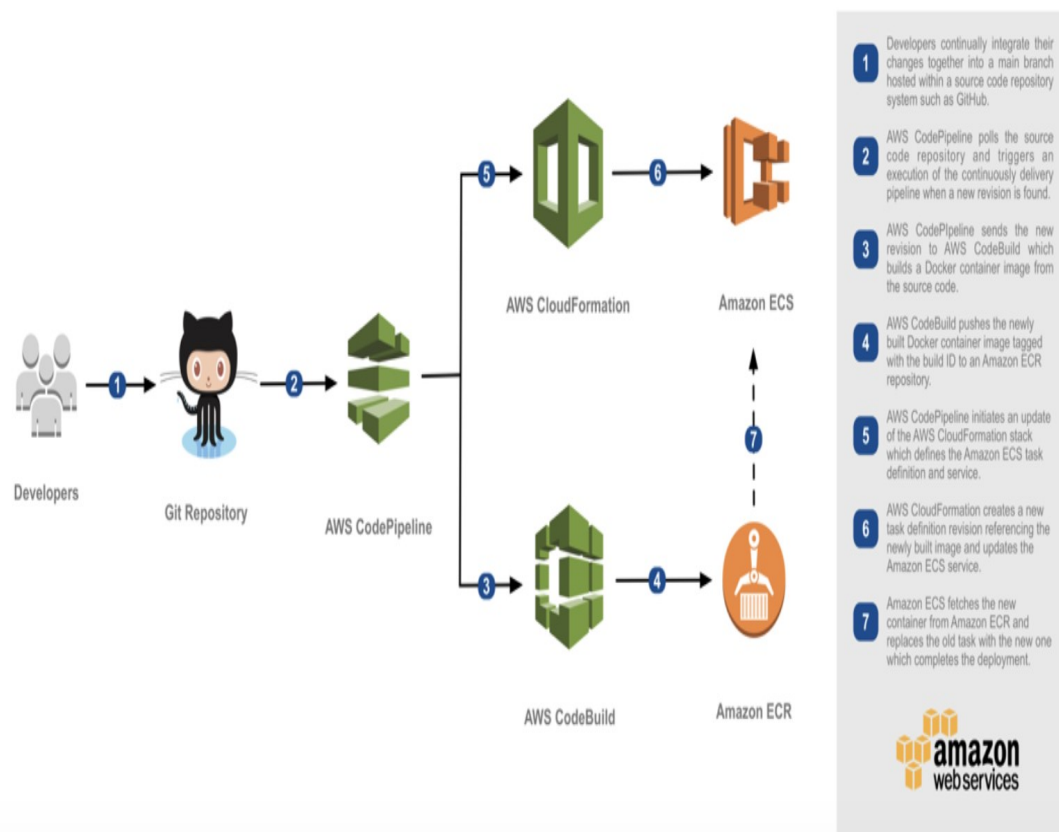
- ☐ A. In CodePipeline, add a Source stage with CodeCommit. Add a Staging stage with CodeBuild to build the new artifact which is a RPM package or an executable file and store it in S3. Add a Deploy stage that uses CloudFormation to create a new task definition revision that points to the installation package in S3 and updates the ECS service to use the new task definition revision.
- ☐ B. In CodePipeline, add a Source stage with CodeCommit. Add a Build stage with CodeBuild to build a new Docker container image and store it in S3. Add a Deploy stage that uses CloudFormation to create a new ECS Cluster that points to S3 URL with the newly built Docker container image and updates the relevant ECS service.
- ☐ C. In CodePipeline, add a Source stage with CodeCommit. Add a Build stage with CodeBuild to build a new Docker container image and push it to ECR. Add a Deploy stage that uses CloudFormation to create a new task definition revision that points to the newly built Docker container image and updates the ECS service to use the new task definition revision. ✓

- D. In CodePipeline, add a Source stage with CodeCommit. Add a Build stage with CodeBuild to build the new artifact which is a RPM package or an executable file and push it to ECR. Add a Deploy stage that uses CloudFormation to create a new task definition revision that points to the newly built Docker container image and updates the ECS service to use the new task definition revision.

### Explanation :

Correct Answer C

The below is a pipeline that has used the required services for a web service:



First, in the Source stage, the pipeline is configured with details for accessing a source code repository system. CodeCommit can be used at this stage.

Secondly, the Build stage uses CodeBuild to create a new Docker container image based upon the latest source code and pushes it to an ECR repository. CodePipeline also integrates with a number of third-party build systems, such as Jenkins, CloudBees, Solano CI, and TeamCity.



Finally, the Deploy stage uses CloudFormation to create a new task definition revision ([http://docs.aws.amazon.com/AmazonECS/latest/developerguide/task\\_definitions.html](http://docs.aws.amazon.com/AmazonECS/latest/developerguide/task_definitions.html)) that points to the newly built Docker container image and updates the ECS service to use the new task definition revision. After this is done, ECS initiates a deployment by fetching the new Docker container from ECR and restarting the service.

The details can be found in <https://aws.amazon.com/blogs/compute/continuous-deployment-to-amazon-ecs-using-aws-codepipeline-aws-codebuild-amazon-ecr-and-aws-cloudformation/> (<https://aws.amazon.com/blogs/compute/continuous-deployment-to-amazon-ecs-using-aws-codepipeline-aws-codebuild-amazon-ecr-and-aws-cloudformation/>).

Option? A is ?incorrect because firstly it should be a Build stage rather than a Staging stage. Secondly, it should generate a Docker image and push it to ECR for ECS to use later on.

Option? B is ?incorrect because the new Docker image should be put in ECR for ECS to use. S3 is not the correct place for Docker images. Moreover, in Deploy stage, CloudFormation should create an ECS task definition rather than an ECS cluster for each deployment activity.

Option? D? ?is? ?incorrect because in Build stage, CodeBuild should generate a Docker image and push it to ECR. A RPM package or an executable file cannot be put into ECR.

Ask our Experts



QUESTION 25

UNATTEMPTED

CONTINUOUS DELIVERY AND PROCESS AUTOMATION

A developer wants to use CodeBuild to build a docker image and push the image to ECR. Then CodePipeline uses CodeDeploy to deploy the latest docker image on EC2 clusters via ECS.

He just created a buildspec.yml file for CodeBuild with 3 logic steps including Pre-build stage, Build Stage and Post-build stage. He is sure that under Build Stage, he needs to build the latest docker image. Which option should be done for Pre-build stage and Post-build stage?

- ☐ A. Pre-build stage: Nothing needs to be done as what you need to do is just push the image to ECR, which will be done in Post-build stage. Post-build stage: Push the image to your ECR repository such as "docker push \$REPOSITORY\_URI:latest".
- ☐ B. Pre-build stage: Login into ECR using "aws ecr get-login" and set the repository URI. Post-build stage: Push the image to your ECR repository such as "docker push \$REPOSITORY\_URI:latest". ✓
- ☐ C. Pre-build stage: Set the repository URI and an image tag if needed. Post-build stage: Push the image to your ECR repository such as "docker push \$REPOSITORY\_URI:latest".
- ☐ D. Pre-build stage: Login into ECR using "aws ecr get-login" and set the repository URI. Post-build stage: Push the image to your ECR repository such as "aws ecr push \$REPOSITORY\_URI:latest".

#### Explanation :

Correct Answer B

The below is an example of what the buildspec.yml should look like for this case:

```

version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=012345678910.dkr.ecr.us-west-2.amazonaws.com/hello-world
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=${COMMIT_HASH:=latest}
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:latest .
      - docker tag $REPOSITORY_URI:latest $REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:latest
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf ' [{ "name": "hello-world", "imageUri": "%s"} ]' $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
  artifacts:
    files: imagedefinitions.json

```

- Pre-build stage:
  - **Log in to Amazon ECR.**
  - **Set the repository URI** to your ECR image and add an image tag with the first seven characters of the Git commit ID of the source.
- Build stage:
  - Build the Docker image and tag the image both as latest and with the Git commit ID.
- Post-build stage:
  - **Push the image to your ECR repository with both tags.**
  - Write a file called imagedefinitions.json in the build root that has your Amazon ECS service's container name and the image and tag. The deployment stage of your CD pipeline uses this information to create a new revision of your service's task definition,

and then it updates the service to use the new task definition. The imagedefinitions.json file is required for the AWS CodeDeploy ECS job worker.

The details can be found in

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-cd-pipeline.html>  
(<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-cd-pipeline.html>).

Option? A & C are ?incorrect because under Pre-build stage, you need to Log in to Amazon ECR and Set the repository URI.

Option? D? ?is? ?incorrect. Although the descriptions of Pre-build are correct, for Post-build stage, the CLI command should be “docker push \$REPOSITORY\_URI:latest”. Refer to <https://docs.aws.amazon.com/cli/latest/reference/ecr/index.html> (<https://docs.aws.amazon.com/cli/latest/reference/ecr/index.html>) for the supported ECR cli commands. After “aws ecr get-login” in the Pre-build stage, the following steps need the docker commands.

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-devops-professional-practice-test/quiz/14878>)

## Certification

- ➔ Cloud Certification  
(<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➔ Java Certification  
(<https://www.whizlabs.com/oracle-java-certifications/>)
- ➔ PM Certification  
(<https://www.whizlabs.com/project-management-certifications/>)

## Company

- ➔ Support  
(<https://help.whizlabs.com/hc/en-us>)
- ➔ Discussions (<http://ask.whizlabs.com/>)
- ➔ Blog (<https://www.whizlabs.com/blog/>)

➔ Big Data Certification  
(<https://www.whizlabs.com/big-data-certifications/>)

## Mobile App



Android Coming Soon



iOS Coming Soon

## Follow us



(<https://www.facebook.com/whizlabs.software/>)



(<https://in.linkedin.com/company/whizlabs-software>)



(<https://twitter.com/whizlabs?lang=en>)



(<https://plus.google.com/+WhizlabsSoftware>)