Free Questions for DOP-C02

Shared by Mosley on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company wants to use AWS Systems Manager documents to bootstrap physical laptops for developers The bootstrap code Is stored in GitHub A DevOps engineer has already created a Systems Manager activation, installed the Systems Manager agent with the registration code, and installed an activation ID on all the laptops.

Which set of steps should be taken next?

Options:

A- Configure the Systems Manager document to use the AWS-RunShellScnpt command to copy the files from GitHub to Amazon S3, then use the aws-downloadContent plugin with a sourceType of S3
B- Configure the Systems Manager document to use the aws-configurePackage plugin with an install action and point to the Git repository
C- Configure the Systems Manager document to use the aws-downloadContent plugin with a sourceType of GitHub and sourcelnfo with the repository details.
D- Configure the Systems Manager document to use the aws:softwarelnventory plugin and run the script from the Git repository

Answer:

C

Explanation:

Configure the Systems Manager Document to Use the aws-downloadContent Plugin with a sourceType of GitHub and sourcelnfo with the Repository Details:

The aws-downloadContent plugin can download content from various sources, including GitHub, which is necessary for bootstrapping the laptops with the code stored in the GitHub repository.

schemaVersion: '2.2'

description: 'Download and run bootstrap script from GitHub'

mainSteps:

- action: aws:downloadContent

name: downloadBootstrapScript

inputs:

sourceType: GitHub

sourceInfo: '{'owner':'my-org','repository':'my-repo','path':'scripts/bootstrap.sh','getOptions':'branch:main'}'

destinationPath: /tmp/bootstrap.sh

- action: aws:runShellScript

name: runBootstrapScript

inputs:

runCommand:

- chmod +x /tmp/bootstrap.sh

- /tmp/bootstrap.sh

This setup ensures that the bootstrap code is downloaded from GitHub and executed on the laptops using Systems Manager.

AWS Systems Manager aws-downloadContent Plugin

Running Commands Using Systems Manager

Question 2

Question Type: MultipleChoice

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?

Options:

A- Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a buildspec.yml file in the CodeCommit repository. In the buildspec.yml file, define the actions to run a CodeGuru review.
B- Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a CodeBuild report group. 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 JUNITXML in the build phase section. Configure the test reports to be uploaded to the new CodeBuild report group.
C- Create a new AWS CodeArtifact repository. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create an appspec.yml file in the original CodeCommit repository. In the appspec.yml file, define the actions to run the unit tests with an output of CUCUMBERJSON in the build phase section. Configure the tests reports to be sent to the new CodeArtifact repository.
D- Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a new Amazon S3 bucket. 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 phases 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.

Question 3

Question Type: MultipleChoice

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.)

Options:

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 O.
D- Increase the Auto Scaling group's desired capacity by I.
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:

A, B, F

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.

Question 4

Question Type: MultipleChoice

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 companys 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?

Options:

A- Configure an Amazon EventBridge rule to receive new AMI events from Image Builder. Target an AWS Systems Manager Run Command document that updates the launch templates of the Auto Scaling groups with the newest AMI ID.
B- Configure an Amazon EventBridge rule to receive new AMI events from Image Builder. Target an AWS Lambda function that updates the launch templates of the Auto Scaling groups with the newest AMI ID.
C- Configure the launch template to use a value from AWS Systems Manager Parameter Store for the AMI ID. Configure the Image Builder pipeline to update the Parameter Store value with the newest AMI ID.
D- Configure the Image Builder distribution settings to update the launch templates with the newest AMI ID. 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 Store1to store the AMI ID and reference it in the launch template2. 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 ID3, 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.

Question 5

Question Type: MultipleChoice

A company has an AWS CodeDeploy application. The application has a deployment group that uses a single tag group to identify instances for the deployment of Application

Options:

A- The single tag group configuration identifies instances that have Environment=Production and Name=ApplicattonA tags for the deployment of ApplicationA.
The company launches an additional Amazon EC2 instance with Department=Marketing Environment^Production. and Name=ApplicationB tags. On the next CodeDeploy deployment of ApplicationA. the additional instance has ApplicationA installed on it. A DevOps engineer needs to configure the existing deployment group to prevent ApplicationA from being installed on the additional instance
Which solution will meet these requirements?
A- Change the current single tag group to include only the Environment=Production tag Add another single tag group that includes only the Name=ApplicationA tag.
B- Change the current single tag group to include the Department=Marketmg Environment=Production and Name=ApplicationAtags
C- Add another single tag group that includes only the Department=Marketing tag. Keep the Environment=Production and Name=ApplicationA tags with the current single tag group
D- Change the current single tag group to include only the Environment=Production tag Add another single tag group that includes only the Department=Marketing tag

Answer:

A, A

Explanation:

To prevent ApplicationA from being installed on the additional instance, the deployment group configuration needs to be more specific. By changing the current single tag group to include only

theEnvironment=Productiontag and adding another single tag group that includes only theName=ApplicationAtag, the deployment process will target only the instances that match both tag groups. This ensures that only instances intended for ApplicationA with the correct environment and name tags will receive the deployment, thus excluding the additional instance with theDepartment=MarketingandName=ApplicationBtags.

AWS CodeDeploy Documentation:Working with instances for CodeDeploy

AWS CodeDeploy Documentation:Stop a deployment with CodeDeploy

Stack Overflow Discussion:CodeDeploy Deployment failed to stop Application

Question 6

Question Type: MultipleChoice

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?

Options:

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

Question 7

Question Type: MultipleChoice

A company has a mission-critical application on AWS that uses automatic scaling The company wants the deployment lilecycle to meet the following parameters.

* The application must be deployed one instance at a time to ensure the remaining fleet continues to serve traffic

* The application is CPU intensive and must be closely monitored

* The deployment must automatically roll back if the CPU utilization of the deployment instance exceeds 85%.

Which solution will meet these requirements?

Options:

A- Use AWS CloudFormalion to create an AWS Step Functions state machine and Auto Scaling hfecycle hooks to move to one instance at a time into a wait state Use AWS Systems Manager automation to deploy the update to each instance and move it back into the Auto Scaling group using the heartbeat timeout

B- Use AWS CodeDeploy with Amazon EC2 Auto Scaling. Configure an alarm tied to the CPU utilization metric. Use the CodeDeployDefault OneAtAtime configuration as a deployment strategy Configure automatic rollbacks within the deployment group to roll back the deployment if the alarm thresholds are breached

C- Use AWS Elastic Beanstalk for load balancing and AWS Auto Scaling Configure an alarm tied to the CPU utilization metric Configure rolling deployments with a fixed batch size of one instance

Enable enhanced health to monitor the status of the deployment and roll back based on the alarm previously created.
D- Use AWS Systems Manager to perform a blue/green deployment with Amazon EC2 Auto Scaling Configure an alarm tied to the CPU utilization metric Deploy updates one at a time Configure automatic rollbacks within the Auto Scaling group to roll back the deployment if the alarm thresholds are breached

Answer:

B

Explanation:

https://aws.amazon.com/about-aws/whats-new/2016/09/aws-codedeploy-introduces-deployment-monitoring-with-amazon-cloudwatch-alarms-and-automatic-deployment-rollback/

Question 8

Question Type: MultipleChoice

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.)

Options:

A- In the monitoring account, download an AWS CloudFormation template from CloudWatch to use in Organizations. Use CloudFormation StackSets in the organization's management account to deploy the CloudFormation template to the entire organization.
B- Create an AWS CloudFormation template that defines an IAM role. Configure the role to allow logs-amazonaws.com to perform the logs:Link action if the aws:ResourceAccount property is equal to the monitoring account ID. Use CloudFormation StackSets in the organization's management account to deploy the CloudFormation template to the entire organization.
C- Create an IAM role in the monitoring account. Attach a trust policy that allows logs.amazonaws.com to perform the iam:CreateSink action if the aws:PrincipalOrgId property is

equal to the organization ID.
D- In the organization's management account, enable the logging policies for the organization.
E- use CloudWatch Observability Access Manager in the monitoring account to create a sink. Allow logs to be shared with the monitoring account. Configure the monitoring account data selection to view the Observability data from the organization ID.
F- In the monitoring account, attach the CloudWatchLogsReadOnlyAccess AWS managed policy to an IAM role that can be assumed to search the logs.

Answer:

B, C, F

Explanation:

To aggregate logs from multiple accounts in an organization, the DevOps engineer needs to create a cross-account subscription1that 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 account2.This can be done using a CloudFormation template and StackSets3to 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 accounts4. The role must have a trust policy that specifies the organization ID as a condition.

Finally, the DevOps engineer needs to attach the CloudWatchLogsReadOnlyAccess policy5to an IAM role in the monitoring account that can be used to search the logs from the cross-account subscription.

Question 9

Question Type: MultipleChoice

A company has an organization in AWS Organizations. A DevOps engineer needs to maintain multiple AWS accounts that belong to different OUs in the organization. All resources, including 1AM policies and Amazon S3 policies within an account, are deployed through AWS CloudFormation. All templates and code are maintained in an AWS CodeCommit repository Recently, some developers have not been able to access an S3 bucket from some accounts in the organization.

The following policy is attached to the S3 bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:PutObject*"
            ],
            "Principal": { "AWS": "arn:aws:sts::*:assumed-role/developer-role/access-session" },
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}
```

What should the DevOps engineer do to resolve this access issue?

Options:

A- Modify the S3 bucket policy Turn off the S3 Block Public Access setting on the S3 bucket In the S3 policy, add the awsSourceAccount condition. Add the AWS account IDs of all developers who are experiencing the issue.

B- Verify that no 1AM permissions boundaries are denying developers access to the S3 bucket Make the necessary changes to IAM permissions boundaries. Use an AWS Config recorder in the individual developer accounts that are experiencing the issue to revert any changes that are blocking access. Commit the fix back into the CodeCommit repository. Invoke deployment through Cloud Formation to apply the changes.

C- Configure an SCP that stops anyone from modifying 1AM resources in developer OUs. In the S3 policy, add the awsSourceAccount condition. Add the AWS account IDs of all developers who are experiencing the issue Commit the fix back into the CodeCommit repository Invoke deployment through CloudFormation to apply the changes

D- Ensure that no SCP is blocking access for developers to the S3 bucket Ensure that no 1AM policy permissions boundaries are denying access to developer 1AM users Make the necessary changes to the SCP and 1AM policy permissions boundaries in the CodeCommit repository Invoke deployment through CloudFormation to apply the changes

Answer:

D

Explanation:

Verify No SCP Blocking Access:

Ensure that no Service Control Policy (SCP) is blocking access for developers to the S3 bucket. SCPs are applied at the organization or organizational unit (OU) level in AWS Organizations and

can restrict what actions users and roles in the affected accounts can perform.

Verify No IAM Policy Permissions Boundaries Blocking Access:

IAM permissions boundaries can limit the maximum permissions that a user or role can have. Verify that these boundaries are not restricting access to the S3 bucket.

Make Necessary Changes to SCP and IAM Policy Permissions Boundaries:

Adjust the SCPs and IAM permissions boundaries if they are found to be the cause of the access issue. Make sure these changes are reflected in the code maintained in the AWS CodeCommit repository.

Invoke Deployment Through CloudFormation:

Commit the updated policies to the CodeCommit repository.

Use AWS CloudFormation to deploy the changes across the relevant accounts and resources to ensure that the updated permissions are applied consistently.

By ensuring no SCPs or IAM policy permissions boundaries are blocking access and making necessary changes if they are, the DevOps engineer can resolve the access issue for developers trying to access the S3 bucket.

AWS SCPs

IAM Permissions Boundaries

Deploying CloudFormation Templates

Question 10

Question Type: MultipleChoice

A company requires its internal business teams to launch resources through pre-approved AWS CloudFormation templates only. The security team requires automated monitoring when resources drift from their expected state.

Which strategy should be used to meet these requirements?

Options:

A- Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use CloudFormation drift detection to detect when resources have drifted from their expected state.
B- Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use

AWS Config rules to detect when resources have drifted from their expected state.
C- Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a launch constraint. Use AWS Config rules to detect when resources have drifted from their expected state.
D- Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a template constraint. Use Amazon EventBridge notifications to detect when resources have drifted from their expected state.

Answer:

C

Explanation:

The correct answer is C, Allowing users to deploy CloudFormation stacks using AWS Service Catalog only and enforcing the use of a launch constraint is the best way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only. AWS Service Catalog is a service that enables organizations to create and manage catalogs of IT services that are approved for use on AWS. A launch constraint is a rule that specifies the role that AWS Service Catalog assumes when launching a product. By using a launch constraint, the DevOps engineer can control the permissions that the users have when launching a product. Using AWS Config rules to detect when resources have drifted from their expected state is the best way to automate the monitoring of the resources. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config rules are custom or managed rules that AWS Config uses to evaluate whether your AWS resources comply with your desired configurations. By using AWS Config rules, the DevOps engineer can track the changes in the resources and identify any non-compliant resources.

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

Option B is incorrect because allowing users to deploy CloudFormation stacks using a CloudFormation service role only is not the best way to ensure that the internal business teams

launch resources through pre-approved CloudFormation templates only, as explained in option A. Using AWS Config rules to detect when resources have drifted from their expected state is a valid way to monitor the resources, as explained in option C,

Option D is incorrect because enforcing the use of a template constraint is not the best way to ensure that the internal business teams launch resources through pre-approved CloudFormation templates only. A template constraint is a rule that defines the values or properties that users can specify when launching a product. By using a template constraint, the DevOps engineer can control the parameters that the users can provide when launching a product, but not the permissions that the users have when launching a product. Therefore, option D does not prevent the users from launching resources that are not approved by the company. Using Amazon EventBridge notifications to detect when resources have drifted from their expected state is a less reliable and consistent solution than using AWS Config rules. Amazon EventBridge is a service that enables you to connect your applications with data from a variety of sources. Amazon EventBridge can deliver a stream of real-time data from event sources, such as AWS services, and route that data to targets, such as AWS Lambda functions. However, to use this solution, the DevOps engineer would need to configure the event source, the event bus, the event rule, and the event target for each resource type that needs to be monitored, which is more complex and error-prone than using AWS Config rules.

Question 11

Question Type: MultipleChoice

A company uses containers for its applications The company learns that some container Images are missing required security configurations

A DevOps engineer needs to implement a solution to create a standard base image The solution must publish the base image weekly to the us-west-2 Region, us-east-2 Region, and eu-central-1 Region.

Which solution will meet these requirements?

Options:

A- Create an EC2 Image Builder pipeline that uses a container recipe to build the image. Configure the pipeline to distribute the image to an Amazon Elastic Container Registry (Amazon ECR) repository in us-west-2. Configure ECR replication from us-west-2 to us-east-2 and from us-east-2 to eu-central-1 Configure the pipeline to run weekly

B- Create an AWS CodePipeline pipeline that uses an AWS CodeBuild project to build the image Use AWS CodeOeploy to publish the image to an Amazon Elastic Container Registry (Amazon ECR) repository in us-west-2 Configure ECR replication from us-west-2 to us-east-2 and from us-

east-2 to eu-central-1 Configure the pipeline to run weekly
C- Create an EC2 Image Builder pipeline that uses a container recipe to build the Image Configure the pipeline to distribute the image to Amazon Elastic Container Registry (Amazon ECR) repositories in all three Regions. Configure the pipeline to run weekly.
D- Create an AWS CodePipeline pipeline that uses an AWS CodeBuild project to build the image Use AWS CodeDeploy to publish the image to Amazon Elastic Container Registry (Amazon ECR) repositories in all three Regions. Configure the pipeline to run weekly.

Answer:

C

Explanation:

Create an EC2 Image Builder Pipeline that Uses a Container Recipe to Build the Image:

EC2 Image Builder simplifies the creation, maintenance, validation, and sharing of container images.

By using a container recipe, you can define the base image, components, and validation tests for your container image.

Configure the Pipeline to Distribute the Image to Amazon Elastic Container Registry (Amazon ECR) Repositories in All Three Regions:

Amazon ECR provides a secure, scalable, and reliable container registry.

Configuring the pipeline to distribute the image to ECR repositories in us-west-2, us-east-2, and eu-central-1 ensures that the image is available in all required regions.

Configure the Pipeline to Run Weekly:

Setting the pipeline to run on a weekly schedule ensures that the base image is regularly updated and published, incorporating any new security configurations or updates.

By using EC2 Image Builder to automate the creation and distribution of the container image, the solution ensures that the base image is consistently maintained and available across multiple regions with minimal management overhead.

EC2 Image Builder

Amazon ECR

Setting Up EC2 Image Builder Pipelines

To Get Premium Files for DOP-C02 Visit
https://www.p2pexams.com/products/dop-c02

For More Free Questions Visit
https://www.p2pexams.com/amazon/pdf/dop-c02

