



Amazon

AMZ AWS-CERTIFIED DEVOPS ENGINEER PROFESSIONAL

---

AMZ AWS Certified DevOps Enginee

Question & Answers

(Free – Demo Version)

*Buy Full Product by Clicking on the Giving Link:*

<https://certya.com/product/amz-aws-certified-devops-engineer-professional-exam-questions-answers/>



**QUESTION: 1**

You have created a Lambda function to help automate an ETL process. The function is triggered by a SQS Queue Depth Cloud Watch alarm, and is designed to process a message from the SQS and dump the results to an S3 bucket. During testing, you manually create a message in the SQS; however, no results show up in S3. What are some possible causes? (Choose 3 answers)

- A. Your Lambda function is outside of a VPC; it needs to reside within a VPC to access SQS and S3.
- B. Your Lambda function does not have the proper permissions to PUT to S3.
- C. Your function timed out.
- D. You did not provision enough compute resources and your function ran out of memory.

**Answer:** B, C, D

**Explanation:**

Common causes for Lambda errors are resource exhaustion or permissions. Although Lambda does need to be within a VPC to access certain resources, S3 and SQS are not on that list. Even if your function code is working as expected and responding correctly to test invokes, the function may not be receiving requests from Amazon S3. If Amazon S3 is able to invoke the function, you should see an increase in your CloudWatch requests metrics. If you do not see an increase in your CloudWatch requests, check the access permissions policy associated with the function.

**Reference:**

<http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions.html>

**QUESTION: 2**

You are a DevOps consultant hired by a start-up company to help automate deployments of their application, which is running on AWS. The application consists of a couple of EC2 instances in an auto-scaling group, and the code base is stored in GitHub. You set up your deployment groups and deployment configuration, and attempt to run a test; however, the deployment fails. You review the Deployment Details but cannot readily determine a cause for the failure. What are some additional items that you should check? (Choose 3 answers)

- A. Check the format for your Deployment Spec file.
- B. Check to see if the instance was tagged properly.
- C. Check the format of your AppSpec file.
- D. Check to see if the instance has the right service role.

**Answer:** B, C, D

**Explanation:**

Some common issues to check when you have a failed CodeDeploy deploy are tags, key pairs, and AppSpec settings.

**Reference:**

<http://docs.aws.amazon.com/codedeploy/latest/userguide/troubleshooting-general.html>

**QUESTION: 3**

You are responsible for your company's AWS infrastructure, which is currently deployed using Cloud Formation. Your supervisor has asked you to automate the installation of a new software package on a number of EC2 hosts. Since this package should be downloaded and installed each and every time an instance is provisioned, you decide to include an installation script as part of the instance's user-data. You make the appropriate changes to the Cloud Formation template, and attempt to deploy your stack to a dev environment to test out your changes. You immediately realize that although the stack deployed successfully, the new software package was not installed. What is the first step you would take to troubleshoot this issue?

- A. Log into the AWS Console and navigate to CloudWatch logs; any EC2 errors will automatically show up there.
- B. Examine the S3 bucket containing your VPC flow logs; it may be a network problem.
- C. Log into one of the instances that was supposed to install the software and take a look at cloud-init.log; any errors encountered with user-data will show up here.
- D. Log into the AWS console and navigate to CloudFormation; any EC2 errors will automatically show up there.

**Answer:** C

**Explanation:**

Any errors with user-data will be sent to the cloud-init.log.

**Reference:**

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html>

**QUESTION: 4**

You are a DevOps consultant helping a FinTech start-up design and build out an AWS environment, which will serve as the back-end for a new peer-to-peer payment app. Due to security requirements, you are helping the company set up VPC Flow Logs to monitor for nefarious activity. You create a flow log and verify that it's displayed as ACTIVE in the VPC console. However, you don't see any log streams showing up in CloudWatch Logs. What are some possible explanations for this behavior? (Choose 3 answers)

- A. Your flow log is still in the process of being created.
- B. Your VPC does not have the correct permissions to write to CloudWatch Logs.
- C. You don't have the correct permissions to view CloudWatch Logs.
- D. As yet, no traffic has been recorded on your interfaces.

**Answer:** A, C, D

**Explanation:**

CloudWatch Logs only records data from VPC Flow Logs when network traffic is present. In some cases, it can take up to 10 minutes for the log group and log streams to be created after enabling VPC Flow Logs.

**Reference:**

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#flow-logs-trouble> shooting

**QUESTION: 5**

You are a DevOps consultant helping a FinTech start-up design and build out an AWS environment, which will serve as the back-end for a new peer-to-peer payment app. You've just created their primary AWS account, and now you need to set up admin accounts for yourself and two other administrators. What is the best course of action recommended by AWS for this task?

- A. Create an IAM group, attach a policy with admin permissions, create individual IAM users, and add them to the group.
- B. Create individual IAM roles and attach a policy with admin permissions.
- C. Create individual IAM users and attach a policy with admin permissions.
- D. Create an IAM role, attach a policy with admin permissions, create individual IAM users, and add them to the group.

**Answer:** A

**Explanation:**

AWS recommends managing permissions at the group level, rather than at the individual user account level.

**QUESTION: 6**

In one of your Amazon CloudTrail logs, you come across this:

```
{
"CiphertextBlob":
"AQEDAHjRYf5WytIc0C857tFSnBaPn2F8DgfmThbJlGfR8P3WlwAAAH4wfAY",
"KeyId":
```

```
"arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab", "Plaintext": "VdzKNHGzUAzJeRBVY+uUmofUGGiD=" }
```

What code most likely produced this log?

- A. `String keyId = "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0"; ListKeysRequest req = new ListKeysRequest().withMarker(keyId).withLimit(10); ListKeysResult result = kms.listKeys(req);`
- B. `String keyId = "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0"; ByteBuffer plaintext = ByteBuffer.wrap(new byte[]{1,2,3,4,5,6,7,8,9,0}); EncryptRequest req = new EncryptRequest().withKeyId(keyId).withPlaintext(plaintext); ByteBuffer ciphertext = kms.encrypt(req).getCiphertextBlob();`
- C. `String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"; GenerateDataKeyRequest dataKeyRequest = new GenerateDataKeyRequest(); dataKeyRequest.setKeyId(keyId); dataKeyRequest.setKeySpec("AES_128"); GenerateDataKeyResult dataKeyResult = kmsClient.generateDataKey(dataKeyRequest);`
- D. `String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"; DescribeKeyRequest req = new DescribeKeyRequest().withKeyId(keyId); DescribeKeyResult result = kms.describeKey(req);`

**Answer:** C

**Explanation:**

The log is an example a response to when a data key is generated. Therefore, the code that calls the `generateDataKey()` method is correct.

**Reference:**

<http://docs.aws.amazon.com/kms/latest/developerguide/programming-keys.html#creating-keys>

**QUESTION: 7**

You are a DevOps consultant helping to migrate a mobile survey application to the AWS cloud. The environment consists of an ELB, EC2 instances, SQS queues, several DynamoDB tables, and some Lambda functions. To meet the variable demand expected on the EC2 tier, you decide to place the instances in an Auto Scaling group. You are now working on the launch configuration; what information must be specified there? (Choose 2 answers)

- A. ELB
- B. Scaling Policies
- C. AMI id
- D. Instance Type

**Answer:** C, D

**Explanation:**

Launch configuration describes what is to be launched, including instance type, storage type, AMI id, virtualization type, etc.

**Reference:**

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

**QUESTION: 8**

You have created CloudFormation templates for your organization that allow your developers to create and/or destroy environments with a few lines of code. While the effort has been successful, your security team is now having a hard time keeping track of who's launching what and what is currently running in the environment. How can you help them maintain visibility?

- A. Use IAM permissions to restrict the ability to launch CloudFormation templates to managers only.
- B. Enable CloudWatch Logs for CloudFormation.
- C. Use OpsWorks instead of CloudFormation.
- D. Provision an S3 bucket, and then enable CloudTrail for your account.

**Answer:** D

**Explanation:**

For security, troubleshooting, and auditing purposes, it is recommended that you enable CloudTrail to log all API calls within your account. CloudFormation does not support CloudWatch Logs.

**Reference:**

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>

**QUESTION: 9**

You are planning to migrate your company's source-code repositories into AWS CodeCommit. While you are discussing the plan with your supervisor, she mentions some concerns about the security of your company's intellectual property within this new system. Since you've done your research, you are confident in your response. What

do you tell her to alleviate her concerns? (Choose 2 answers)

- A. CodeCommit integrates with KMS to secure data-at-rest by default.
- B. The CodeCommit repos are logically separated by AWS account; there's no need for additional security.
- C. CodeCommit uses SSL/TLS to secure data-in-flight.
- D. The CodeCommit repos are physically separated by AWS account; there's no need for additional security.

**Answer:** A, C

**Explanation:**

CodeCommit has built-in features to encrypt data-at-rest and data-in-flight by default.

**Reference:**

<http://docs.aws.amazon.com/codecommit/latest/userguide/encryption.html>

**QUESTION:** 10

You are the DevOps engineer responsible for a social media site focused on sharing recipes. You are helping to develop a new feature that will recommend a set of recipes to users based on their history. You have decided to build this feature as a Lambda function, which will run once a day and produce a number of recommendations per user. You must now decide what to do with the results produced by your function. What are some valid options? (Choose 3 answers)

- A. Save the results to ephemeral storage on the instance that's running your Lambda function for best performance.
- B. Write the results to flat files in an S3 bucket.
- C. Write the results directly to a DynamoDB table.
- D. Write the results to RedShift.

**Answer:** B, C, D

**Explanation:**

Lambda is stateless, meaning it has no "local" storage. All data must be written to external storage in order to persist it beyond the life of the function.

**Reference:**

<http://docs.aws.amazon.com/lambda/latest/dg/best-practices.html>

**QUESTION: 11**

You are a DevOps consultant helping to migrate a mobile survey application to the AWS cloud. The environment consists of an ELB, EC2 instances, SQS queues, several DynamoDB tables, and some Lambda functions. The client requires that when instances are removed from the Auto Scaling group and terminated, the newer instances are removed last. Which termination policies should you enable to meet this requirement? (Choose 2 answers)

- A. OldestLaunchConfiguration
- B. NewestInstance
- C. OldestInstance
- D. Default

**Answer:** A, C

**Explanation:**

Termination policies of OldestInstance and OldestLaunchConfiguration will ensure the newest instances are removed/terminated last.

**Reference:**

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html>

**QUESTION: 12**

You are the DevOps engineer responsible for supporting your company's AWS infrastructure, which consists of EC2 instances in an Auto Scaling group, an ELB, and a MySQL RDS instance. You have recently modified your RDS instance to a multi-AZ deployment for high availability. What conditions would trigger a failover to the secondary instance? (Choose 3 answers)

- A. Storage failure on primary instance
- B. Loss of network connectivity to primary instance
- C. CloudWatch Alarm activated on primary instance
- D. Compute unit failure on primary instance

**Answer:** A, B, D

**Explanation:**

Loss of network connectivity, compute unit failure, and/or network issues can trigger an RDS failover.

**Reference:**

<https://aws.amazon.com/rds/details/multi-az/>

**QUESTION: 13**

You are the DevOps engineer for a medical devices start-up who recently migrated their infrastructure to AWS. The environment consists of multiple EC2 instances in auto-scaling groups, internal and external ELBs, a multi-AZ RDS deployment, and several DynamoDB tables. One day, while an auto-scaling (scale out) event is happening, you notice that one of your EC2 instances has failed one of its instance status checks. What are some possible reasons for this? (Choose 3 answers)

- A. Failed system status check
- B. Exhausted CPU
- C. Exhausted memory
- D. Incorrect networking configuration

**Answer:** A, C, D

**Explanation:**

Failed system status checks, incorrect networking or startup configuration, exhausted memory, or kernel issues will cause a failed status check.

**Reference:**

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html>

**QUESTION: 14**

Your supervisor has informed you that your company's monthly AWS spend has exceeded budget, and she has asked you to find ways to reduce cost. After some investigation, you realize that the engineering teams are leaving their development instances running 24/7, even though they are only utilized during the normal work week. What does AWS recommend as the best way to automate a solution?

- A. Write scripts that shut down and start up all development instances based on tags, upload the scripts as Lambda function(s), and configure the scheduled events trigger at the appropriate time(s).
- B. Write scripts that shut down and start up all development instances based on tags, and manually run these from your laptop at the appropriate time(s).
- C. Write scripts that shut down and start up all development instances based on tags, and configure the crontab or Windows scheduler on your local laptop to execute the scripts at the appropriate time(s).
- D. Write scripts that shut down and start up an instance, deploy the scripts to all development servers, and configure the crontab or Windows scheduler to execute the scripts at the appropriate time(s).

**Answer:** A

**Explanation:**

Lambda scheduled events are the best way to automate actions on a schedule across fleets of EC2 instances.

**Reference:**

<http://docs.aws.amazon.com/lambda/latest/dg/with-scheduled-events.html>

**QUESTION: 15**

You are a DevOps engineer responsible for supporting your company's AWS infrastructure, consisting of multiple EC2 instances running in a VPC, DynamoDB, SQS, and S3. You are working to provision a new S3 bucket, which will ultimately contain sensitive data. How can you encrypt that data in-flight, into, and out of S3? (Choose 2 answers)

- A. Enable encryption in the bucket policy.
- B. Use the encrypted SSL/TLS endpoint.
- C. Encrypt it on the client-side before uploading.
- D. Set the server-side encryption option after upload.

**Answer:** B, C

**Explanation:** To encrypt your S3 objects in-flight, you need to use the TLS endpoint; alternatively, you can encrypt the data yourself on the client side prior to upload.

**Reference:**

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

**QUESTION: 16**

You are a DevOps engineer responsible for supporting your company's AWS infrastructure, consisting of multiple EC2 instances running in a VPC, DynamoDB, SQS, and S3. You are working to provision a new S3 bucket, which will ultimately contain sensitive data. How could you restrict which users can access objects in the bucket? (Choose 2 answers)

- A. Bucket Policy
- B. S3 Policy
- C. IAM User Policy
- D. Multi-factor Authentication

**Answer:** A, C

**Explanation:**

IAM user policies or bucket policies can be used to apply permissions to the object, prefix, or bucket-level. Server-side encryption (SSE) can also be used to restrict access to those users with the proper key.

**Reference:**

<http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html>

**QUESTION: 17**

You are the DevOps engineer at a mobile gaming company, responsible for managing their AWS infrastructure. You are soon launching a new game, and are in the process of deploying and testing your auto-scaling groups. You have defined a scheduled scaling action that is intended to double the size of your EC2 fleet at a certain time. However, the designated time passes and no new instances are launched because the launch failed. What are some possible causes? (Choose 3 answers)

- A. The AZ specified to your auto-scaling group is not available.
- B. The key pair defined in your launch configuration does not exist.
- C. The key pair defined in your auto-scaling group does not exist.
- D. The security group defined in your launch configuration does not exist.

**Answer:** A, B, D

**Explanation:**

The key pairs and security groups defined in the launch configuration must exist, along with the designated AZ.

**Reference:**

<http://docs.aws.amazon.com/autoscaling/latest/userguide/ts-as-instancetypefailure.html>

**QUESTION: 18**

You are a DevOps consultant helping a FinTech start-up design and build out an AWS environment, which will serve as the back-end for a new peer-to-peer payment app. Due to security requirements, the company is planning to use VPC Flow Logs to monitor for nefarious activity. On what resources could VPC Flow Logs be enabled? (Choose 3 answers)

- A. VPC
- B. ELB

- C. Subnet
- D. ENI

**Answer:** A, C, D

**Explanation:**

VPC flow logs can be enabled at the VPC, subnet, or ENI level to capture and send all network traffic to an S3 bucket.

**QUESTION: 19**

You are the DevOps engineer for a major retail brand, which happens to host its online e-commerce site on AWS. You are planning to migrate your test and development environment(s) into OpsWorks Stacks in order to speed up the SDLC. Since this is a test and development environment, you need to be able to deploy changes quickly, with no need to roll back. Which OpsWorks Stacks deployment method would AWS recommend as most appropriate?

- A. Production deployment
- B. Blue / green deployment
- C. Default deployment
- D. Rolling deployment

**Answer:** C

**Explanation:**

The Default deploy command is the fastest and easiest way to deploy code to running instances; however, it does not leave much room for error.

**QUESTION: 20**

You are the DevOps engineer for a popular e-commerce site running on AWS and consisting of multiple EC2 instances in an Auto-scaling group running behind a load-balancer. Your CTO has just forwarded you an email describing a new security vulnerability affecting the version of web server software your company is using. You quickly identify the fix and write a small PowerShell script containing the mitigation steps. Which methods would AWS recommend to quickly deploy this fix to your running instances while minimizing impact? (Choose 2 answers)

- A. Use the EC2 Run Command to execute the script in parallel across all target instances.
- B. Terminate all EC2 instances and re-launch them with the script embedded as user data.

C. Write another script that logs into each instance in serial order and executes the fix. D. Bake the fix into a new AMI and launch configuration, update the Auto-scaling group, and perform a blue/green deployment.

**Answer:** A, D

**Explanation:**

The EC2 Run Command allows you to execute commands or scripts across a fleet of EC2 instances in parallel. This is the best choice for this scenario, along with a blue/green deployment at the Auto-scaling group level.

**Reference:**

[http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/tutorial\\_run\\_command.html](http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/tutorial_run_command.html)