AWS_DOP-C00 Exam

Volume: 404 Questions

Question No:1
You have created a Lambda function to help automate an ETL process. The function is triggered by a SQS Queue Depth CloudWatch 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 No: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 DeploymentSpec 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 No:3
You are responsible for your company's AWS infrastructure, which is currently deployed using CloudFormation. 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 CloudFormation 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 No: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-troubleshooting

Question No: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 No: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 No: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 No: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: