You have been asked to run your in-house application code using Lambda. Which of the following services could you use to deploy your code?

1. CodeBuild
2. AWS Serverless Application Model
3. CodeDeploy
4. CodeCommit
5. CloudFormation

Answer: b, c, e

EXPLANATION:

You cannot deploy code using CodeCommit or CodeBuild. All of the other services can be used to deploy code in a Serverless environment

You receive the following response from STS, What is happening here?

<AssumeRoleWithWebIdentityResult> <SubjectFromWebIdentityToken>amzn1.account.AF6RHO7KZU5XRVQJGXK6HB56KR2A</SubjectFromWebIdentityToken> <Audience>[client.5498841531868486423.1548@apps.example.com</Au](mailto:client.5498841531868486423.1548@apps.example.com%3c/Au) dience> <AssumedRoleUser> <Arn>arn:aws:sts::123456789012:assumed-role/FederatedWebIdentityRole/app1</Arn> <AssumedRoleId>AROACLKWSDQRAOEXAMPLE:app1</AssumedRoleId> </AssumedRoleUser> <Credentials> <SessionToken>AQoDYXdzEE0a8ANXXXXXXXXNO1ewxE5TijQyp+IEXAMPLE</SessionToken> <SecretAccessKey>wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY</SecretAccessKey> <Expiration>2014-10-24T23:00:23Z</Expiration> <AccessKeyId>ASgeIAIOSFODNN7EXAMPLE</AccessKeyId> </Credentials> <Provider>www.amazon.com</Provider> </AssumeRoleWithWebIdentityResult> <ResponseMetadata> <RequestId>ad4156e9-bce1-11e2-82e6-6b6efEXAMPLE</RequestId> </ResponseMetadata> </AssumeRoleWithWebIdentityResponse>

1. The user with the following ARN is given access to the application: arn:aws:sts::123456789012:assumed-role/FederatedWebIdentityRole/app1
2. STS is returning temporary security credentials to a user who has successfully authenticated with a web identity provider.
3. The web identity token that was passed could not be validated by AWS.
4. The user has requested permission to assume the following role: client.5498841531868486423.1548@apps.example.com
5. The user is allowed to assume the following role: arn:aws:sts::123456789012:assumed-role/FederatedWebIdentityRole/app1

Answer: b, d, e

EXPLANATION:

STS AssumeRoleWithWebIdentity returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider. Example providers include Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider. See the link below for an explanation of the sample response.

Your application is running on EC2 and you are trying to capture data related to incoming and outgoing HTTP requests, and send it to X-Ray. You have instrumented the application, but after 1 hour, you are still not seeing any data appear in X-Ray. What could be the problem?

1. You need to register your application in the X-Ray console
2. You need to make sure the X-Ray daemon is installed and running on your EC2 instances
3. You need to register your EC2 instances in the X-Ray console
4. you need to install the X-Ray telemetry agent on your EC2 instances

Answer: b

EXPLANATION:

You need the X-Ray daemon to be running on your EC2 instances in order to send data to X-Ray.

Which DynamoDB feature allows you to set an expiry on table items so that they can automatically be deleted to reduce storage costs?

1. DynamoDB Provisioned Throughput
2. DynamoDB AutoDelete
3. DynamoDB TTL
4. DynamoDB Streams

Answer: c

EXPLANATION:

Time To Live (TTL) for DynamoDB allows you to define when items in a table expire so that they can be automatically deleted from the database. TTL is provided at no extra cost as a way to reduce storage usage and reduce the cost of storing irrelevant data without using provisioned throughput. With TTL enabled on a table, you can set a timestamp for deletion on a per-item basis, allowing you to limit storage usage to only those records that are relevant.

Which of the following AWS services enables you to capture a time-ordered sequence of any modifications which happened to the items in your DynamoDB table over the past 24 hours?

1. CloudWatch
2. DynamoDB TTL
3. DynamoDB Streams
4. CloudTrail

Answer: c

EXPLANATION:

DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for up to 24 hours.

You have an application running on a number of Docker containers running on AWS Elastic Container Service. You have noticed significant performance degradation after you made a number of changes to the application and would like to troubleshoot the application end-to-end to find out where the problem lies. What should you do?

1. Deploy the AWS X-Ray daemon as a new container alongside your application
2. Deploy the AWS X-Ray daemon to each of the Docker containers that run your application
3. Deploy the AWS X-Ray daemon onto an EC2 instance
4. In the ECS console, configure the application to send telemetry records to AWS X-Ray

Answer: a

EXPLANATION:

Within a microservices architecture, each application component runs as its own service. Microservices are built around business capabilities, and each service performs a single function. So if you want to add X-Ray to a Dockerized application, it makes the most sense to run the X-Ray daemon in a new Docker container and have it run alongside the other microservices which make up your application.

If your table item's size is 3KB and you want to have 90 eventually consistent reads per second, how many read capacity units will you need to provision on the table?

1. 45
2. 48
3. 90
4. 24

Answer: a

EXPLANATION:

3 rounds up to 4. 4/4=1. 90\*1/2=45

What is the maximum size of an S3 object?

1. 500 GB
2. 50 TB
3. 50 GB
4. 5 TB

Answer: d

EXPLANATION:

The minimum size of an object is 0 bytes (empty or 'touched' files are permitted) and the maximum size of an object is 5TB.

Your application is running on Docker in an Elastic Beanstalk. You have been asked to deploy a new version of the application code. What is the process for doing this?

1. Delete your environment and redeploy using the new code
2. Use the Elastic Beanstalk console to upload and deploy the new version of your application using a zip file containing your code
3. Log in to the EC2 instance, update the dockerfile and restart the container
4. Log in to the underlying EC2 instance and replace the existing Docker image with the new code

Answer: b

EXPLANATION:

When you use the AWS Elastic Beanstalk console to deploy a new application or an application version, you'll need to upload a source bundle. Your source bundle must consist of a single ZIP file or WAR file which does not exceed 512 MB.

Your distributed application sends and receives a number of large SQS messages, each of which can be up to 2GB in size. You are finding that the messages in one particular queue are getting processed a few seconds faster than expected which is causing problems in your application. The application architect has asked you to introduce a sleep period of 5 seconds which should apply to all the messages in the queue and you have also been asked to avoid storing large amounts of data in SQS. Which of the following changes do you recommend?

1. Use a FIFO queue to postpone the delivery of SQS messages by 5 seconds
2. Store the large messages on S3
3. Use an SQS delay queue to let you postpone the delivery of SQS messages by 5 seconds
4. Store the large messages in DynamoDB
5. Store the large messages in a separate queue

Answer: b, c

EXPLANATION:

Delay queues let you postpone the delivery of new messages to a queue for a number of seconds. If you create a delay queue, any messages that you send to the queue remain invisible to consumers for the duration of the delay period. You can use Amazon S3 and the Amazon SQS Extended Client Library for Java to manage Amazon SQS messages. This is especially useful for storing and consuming messages up to 2 GB in size. Unless your application requires repeatedly creating queues and leaving them inactive or storing large amounts of data in your queue, consider using Amazon S3 for storing your data.

Your application needs 100 strongly consistent reads on items that are 9KB in size every second. How many units of read capacity units should you provision?

1. 350
2. 150
3. 300
4. 200

Answer: c

EXPLANATION:

9KB rounds up to 12KB. 12KB/4KB=3 strongly consistent read capacity units each. 3\*100=300 strongly consistent read capacity units.

You are creating a DynamoDB table to store customer order data, which of the following attributes would make a good Partition Key?

1. CustomerID
2. ProductType
3. Size
4. OrderDate

Answer: a

EXPLANATION:

A Partition key is a single attribute and is used as a Primary Key attribute to uniquely identify a record in the DynamoDB table. Customer ID is the best option here because each customer will have a unique ID

A developer is making changes to the CloudFormation template used to deploy an application. They would like to know if any existing resources will be deleted or replaced before applying the template updates. What service feature will enable this?

1. CloudFormation StackSets
2. CloudFormation Rolling Updates
3. CloudFormation Registry
4. CloudFormation Change Sets

Answer: d

EXPLANATION:

CloudFormation Change sets enable the preview of proposed changes to a stack in order to assess the impact on running resources. This functionality allows the developer to check if any existing resources will be deleted or replaced upon application of the CloudFormation template.

You are developing an online auction application which uses SQS to exchange messages between application components. Some of the messages are between 1GB and 2GB in size. What is the AWS recommended way of managing large messages in SQS?

1. Use the SQS API to manage SQS messages
2. Store the messages using DynamoDB
3. Use the SQS CLI to manage SQS messages
4. Use the AWS Java SDK to manage SQS messages
5. Store the messages in SQS
6. Store the messages using S3
7. Use the Amazon SQS Extended Client Library for Java to manage SQS messages

Answer: f, g

EXPLANATION:

You can use Amazon S3 and the Amazon SQS Extended Client Library for Java to manage Amazon SQS messages. This is especially useful for storing and consuming messages up to 2 GB in size. Unless your application requires repeatedly creating queues and leaving them inactive or storing large amounts of data in your queue, consider using Amazon S3 for storing your data. You can use the Amazon SQS Extended Client Library for Java to manage Amazon SQS messages using Amazon S3. However, you can't do this using the AWS CLI, the Amazon SQS console, the Amazon SQS HTTP API, or any of the AWS SDKs—except for the SDK for Java.

Your application is using SQS to send and receive messages, your application needs to receive the messages as soon as they arrive and you need to ensure the architecture is as cost efficient as possible. Which of the following approaches will optimise the cost and performance of the application?

1. Reduce the total number of message queues
2. Enable Short Polling
3. Enable Long Polling
4. Lower the message Visibility Timeout

Answer: c

EXPLANATION:

In almost all cases, Amazon SQS long polling is preferable to short polling and results in higher performance and reduced cost in the majority of use cases.

Your company is reaching the end of the financial year and the Finance team are running a lot of large database queries and scans against your DynamoDB tables. The database queries and scans are taking much longer to complete than expected, how can you make them more efficient?

1. Run parallel scans
2. Reduce the page size to return fewer items per results page
3. Set your queries to be eventually consistent
4. Filter your results based on the Primary Key and Sort Key

Answer: a, b

EXPLANATION:

Reducing page size for queries and running scans in parallel are both recommended approaches for making DynamoDB operations more efficient. DynamoDB uses eventually consistent reads by default and filtering the results will not improve efficiency

Your security team have brought in an external auditor to review the security standards across your AWS account. They have identified that your development team have elevated privileges across a number of services, which according to company policy, they should not have access to. You have been asked to help work out which of the IAM policies are granting too much access to the team. Which of the following can you use to find out which policies are granting too many privileges?

1. Cognito
2. Config
3. X-Ray
4. IAM Policy Simulator

Answer: d

EXPLANATION:

With the IAM policy simulator, you can test and troubleshoot IAM and resource-based policies attached to IAM users, groups, or roles in your AWS account. You can test which actions are allowed or denied by the selected policies for specific resources.

You are trying to diagnose a performance problem with your serverless application, which uses Lambda, API Gateway, S3 and DynamoDB. Your DynamoDB table is performing well and you suspect that your Lambda function is taking too long to execute. Which of the following could you use to investigate the source of the issue?

1. AWS X-Ray
2. API Gateway Latency metric in CloudWatch
3. API Gateway Integration Latency metric in CloudWatch
4. Lambda Invocations Sum metric in CloudWatch

Answer: a, c

EXPLANATION:

AWS X-Ray can be used to display a histogram showing the latency of your Lambda function. Latency is the amount of time between when a request starts and when it completes. API Gateway Integration Latency in the time between when API Gateway relays a request to the backend and when it receives a response from the backend. API Gateway Latency is the time between when API Gateway receives a request from a client and when it returns a response to the client. The latency includes the integration latency and other API Gateway overhead. Lambda Invocations Sum measures the number of times a function is invoked in response to an event or invocation API call.

You are troubleshooting a major incident which has resulted in data loss in your application. Your manager asks if you can provide a time-ordered sequence of any modifications which happened to the items in your DynamoDB table over the past 24 hours so that you can work out what happened. Which service could you use to most effectively provide this?

1. CloudTrail
2. DynamoDB Streams
3. CloudWatch
4. Kinesis Streams

Answer: b

EXPLANATION:

DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for up to 24 hours.

You are working on an application for an online training company which stores product data in DynamoDB. This week, the company is running a big promotion on a few courses and this is bringing lots of new traffic to your website, causing an increased number of queries to the database. Database queries are now running much slower than usual and the Operations Team are concerned that the DynamoDB table is being throttled. Which of the following approaches would you recommend to improve read performance?

1. Configure the application to use scans rather than queries and run multiple scans in parallel
2. Redesign your table to use a more distinct partition key to enable the I/O load to be more evenly distributed across partitions
3. Add a Read Replica and point the DynamoDB API calls at the Read Replica
4. Configure a DAX cluster and point the DynamoDB API calls at the DAX cluster

Answer: d

EXPLANATION:

Using DAX is the recommended approach to reducing response times for read-intensive applications, applications which read a small number of items frequently and also applications which perform repeated reads against a large set of data. Read Replicas are not a feature of DynamoDB. Configuring the application to use scans instead is not an efficient solution.

You have multiple applications running on a large number of EC2 instances. You need to access the application logs from a single central location, what should you do?

1. CloudWatch Logs
2. CloudWatch custom metrics
3. Write a script to send the application logs to CloudWatch. Install the script on each of your application servers
4. CloudTrail Logs

Answer: a

EXPLANATION:

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources. CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can create CloudWatch custom metrics for your EC2 instance statistics by creating a script through the AWS Command Line Interface and then monitor that metric by pushing it to CloudWatch. However, custom metrics are only metrics or findings reported by running a script, they are not pushing log files into CloudWatch.

You are using X-Ray to monitor your application for performance and troubleshooting purposes. You would like to be able to index and filter the traces based on values specific to your project. How can you do this?

1. Configure annotations in your traces so that they can be indexed and filtered in the X-Ray console, based on the annotations.
2. Use DynamoDB to index and query the traces. Filter the results using a projection expression
3. Use Athena to run a SQL query on the traces. Index and filter the results using the X-Ray console.
4. Configure annotations in the X-Ray console and use the X-Ray daemon to filter and index the traces.

Answer: a

EXPLANATION:

When you instrument your application, the X-Ray SDK records information about incoming and outgoing requests, the AWS resources used, and the application itself. You can add other information to the segment document as annotations and metadata. Annotations are simple key-value pairs that are indexed for use with filter expressions. Use annotations to record data that you want to use to group traces in the console.

How can you configure CodeBuild to notify the DevOps team of a failure in the build process?

1. Use the CodePipeline dashboard to view the CodeBuild events log
2. Use CloudWatch Events and SES notifications to send an email to the DevOps team
3. Use CloudWatch Events and an SNS topic to notify subscribers of build events
4. Add the name of the email group to the notifications section of the CodeBuild console

Answer: c

EXPLANATION:

CodeBuild natively supports CloudWatch Events, SNS is a subscription based notification service which integrates with CloudWatch.

You are attempting to upload a number of objects to S3, however you keep seeing the following error message: "AmazonS3Exception: Internal Error; Service: Amazon S3;" Which of the following is the best explanation for this kind of error?

1. This is a 400 type error, which is a server-side error
2. This is a 500 type error, which is a client-side error
3. This is a 500 type error, which is a server-side error
4. This is a 400 type error, which is a client-side error

Answer: c

EXPLANATION:

This is an Internal Error which indicates that Amazon S3 is unable to handle the request at that time. Internal errors or server-side errors have a 5xx status code, whereas client-side errors have a 4xx status code.

In the CodeDeploy AppSpec file, what are hooks used for?

1. To specify files that you want to copy during the deployment
2. Hooks are reserved for future use
3. To reference AWS resources that will be used during the deployment
4. To specify code, scripts or functions that you want to run at set points in the deployment lifecycle

Answer: d

EXPLANATION:

The hooks section for an EC2/On-Premises deployment contains mappings that link deployment lifecycle event hooks to one or more scripts. The hooks section for a Lambda deployment specifies Lambda validation functions to run during a deployment lifecycle event.

You are working on an application which runs inside a Docker container. All your images are stored in a repository named mydockerrepo AWS ECR. Which of the following commands could you use to pull the Docker image to your local workstation?

1. docker clone aws\_account\_id.dkr.ecr.us-west-2.amazonaws.com/mydockerrepo:latest
2. docker get aws\_account\_id.dkr.ecr.us-west-2.amazonaws.com/mydockerrepo:latest
3. docker pull aws\_account\_id.dkr.ecr.us-west-2.amazonaws.com/mydockerrepo:latest
4. docker push aws\_account\_id.dkr.ecr.us-west-2.amazonaws.com/mydockerrepo:latest

Answer: c

EXPLANATION:

If you would like to run a Docker image that is available in Amazon ECR, you can pull it to your local environment with the docker pull command.

You are working on a Serverless application written in Python and running in Lambda. You have uploaded multiple versions of your code to Lambda, but would like to make sure your test environment always utilizes the latest version. How can you configure this?

1. Reference the function using a qualified ARN and the $LATEST suffix
2. Create an alias to point to the correct version of your code
3. Reference the function using an unqualified ARN
4. Create another function to automatically update your function alias to point to the latest version of the code every time it is updated
5. Configure the alias to automatically update to point to the latest version of the code every time it is updated

Answer: a, c

EXPLANATION:

When you create a Lambda function, there is only one version: $LATEST. You can refer to the function using its Amazon Resource Name (ARN). There are two ARNs associated with this initial version, the qualified ARN which is the function ARN plus a version suffix e.g. $LATEST. Or the unqualified ARN which is the function ARN without the version suffix. The function version for an unqualified function always maps to $LATEST, so you can access the latest version using either the qualified ARN with $LATEST, or the unqualified function ARN. Lambda also supports creating aliases for each of your Lambda function versions. An alias is a pointer to a specific Lambda function version, aliases will not be updated automatically when a new version of the function becomes available.

Which of the following AWS services would you recommend using to store session state data for a scalable web application?

1. EC2 instance memory
2. Lambda
3. ElastiCache
4. Glacier
5. EC2 instance EBS volume

Answer: c

EXPLANATION:

Storing session state locally is not a good idea for a scalable application, so it doesn't make sense to store the session state on the EC2 instance. Lambda is generally for short-lived functions which do not persist, so is not suitable for managing session state. Glacier is designed for archiving infrequently used data so is not suitable for session data which could be frequently used for the lifetime of the session and then no longer required. In order to address scalability and to provide a shared data storage for sessions that can be accessed from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached, and in AWS the service to use is ElastiCache.

You are developing a web application which has been deployed using Lambda. Today you updated the code and uploaded the new version of your code to the Lambda console. Your test team have begun testing but have reported today that the application seems to still be using the original code. What could be the reason for this?

1. Your application is referencing the function using $LATEST
2. You forgot to publish the version
3. Your application is referencing the function using an alias which points to a previous version of the code
4. Your application is referencing the function using a qualified ARN
5. Your application is referencing the function using an unqualified ARN

Answer: c

EXPLANATION:

The problem is that the application is referencing the function using an alias pointing to a previous version of the code. When you use versioning in AWS Lambda, you can publish one or more versions of your function. So that you can use different variations of your Lambda function in your development workflow, such as development, beta, and production. Lambda also supports creating aliases for each of your Lambda function versions. Conceptually, an AWS Lambda alias is a pointer to a specific Lambda function version. You can update aliases to point to different versions of functions.

A transport company uses a mobile GPS application to track the location of each of their 60 vehicles. The application records each vehicle's location to a DynamoDB table every 6 seconds. Each transmission is just under 1KB and throughput is spread evenly within that minute. How many units of write capacity should you specify for this table?

1. 100
2. 60
3. 600
4. 10

Answer: d

EXPLANATION:

Writing to the database every six seconds, there are 10 writes/minute/vehicle. There are sixty vehicles in the fleet, so there are 600 writes/minute overall. 600/60 seconds = 10 writes/second.

You are using CodeBuild to create a Docker image and add the image to your Elastic Container Registry. Which of the following commands should you include in the buildspec.yml?

1. docker push $REPOSITORY\_URI:latest
2. aws ecr push $REPOSITORY\_URI:latest
3. docker add $REPOSITORY\_URI:latest
4. aws codebuild docker -t $REPOSITORY\_URI:latest .
5. docker build -t $REPOSITORY\_URI:latest .

Answer: a, e

EXPLANATION:

Use the docker push command to add your image to your Elastic Container Registry

Which AWS service allows you to build and model your serverless application as a visual workflow consisting of a series of steps where the output of one stage can be input into another?

1. Lambda
2. Simple Workflow Service
3. Step Functions
4. CloudFormation

Answer: c

EXPLANATION:

Step Functions provide this functionality

An application successfully updates an existing object in S3. When checking the file contents, the developer does not see the updated file contents. What is the cause of this issue?

1. S3 bucket policy permissions were not correct.
2. HTTP 200 response code was not received.
3. S3 Bucket Versioning was not enabled.
4. Overwrite PUTS in S3 have eventual consistency.

Answer: d

EXPLANATION:

Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all Regions. Amazon S3 provides high availability and high durability by replicating bucket objects across multiple availability zones and servers. This means that any updates to objects must replicate across all servers storing the data. This can take some time. Therefore, any updates to existing objects (using POST or DELETE), will take some time to be propagated across all of S3, and hence are eventually consistent.

You've been asked to create a Web application with an endpoint that can handle thousands of REST calls a minute. What AWS service can be used in front of an application to assist in achieving this?

1. CloudFront
2. Global Accelerator
3. Elastic Beanstalk
4. API Gateway

Answer: d

EXPLANATION:

Questions containing 'REST' are usually related to APIs, so API Gateway looks the best answer. Elastic Beanstalk is a service which allows you to run applications without understanding the infrastructure and can be discounted, as can Global Accelerator which is a networking service that improves the availability and performance of applications. CloudFront can be used in conjunction with API Gateway to assist in geographically disparate calls, but won't process calls by itself.

You are developing an application using multiple AWS services. You need to find a solution to decouple the application components, so that they can fail independently of one another. Which of the following AWS services will enable this?

1. Lambda
2. DynamoDB
3. SQS
4. SNS

Answer: c

EXPLANATION:

SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware, and empowers developers to focus on differentiating work.

Where should the appspec.yml be stored?

1. In the config directory in your application source directory
2. In the .ebextentions folder
3. In /opt
4. In the root of your application source directory

Answer: d

EXPLANATION:

The AppSpec file (appspec.yml) must always be in the root or your application source directory otherwise the deployment will not work. The .ebextensions folder is used to set custom environment variables in Elastic Beanstalk, not CodeDeploy.

You are the development lead on a large project to launch a new e-commerce website specialising in fishing supplies. Your developers are located in India, USA and the Middle East. You need to find a source code repository that everyone can use, and that will allow developers to continue to work on their code even when they are not connected to the internet. Which of the following would you suggest to the team?

1. Run an instance of Git in a docker container on AWS ECS
2. Use CodeCommit to manage your source code
3. Install Git on 2 EC2 instances in an auto-scaling group
4. Use CodeBuild in offline mode to manage your source code

Answer: b

EXPLANATION:

CodeCommit is based on Git, which is a distributed version control system, meaning there is no single, central place where everything is stored. In a distributed system, there are multiple backups in the event that you need one. This approach also means that you can work offline and commit your changes when you are ready.

You are developing a Lambda function which takes an average of 20 seconds to execute. During performance testing, you are trying to simulate peak loads, however soon after the testing begins, you notice that requests are failing with a throttling error. What could be the problem?

1. Your application does not have permission to invoke the Lambda function
2. The Lambda function is taking too long to execute
3. The deployment package is too large
4. You haven't allocated enough memory to your function
5. You have reached the limit of concurrent executions for Lambda

Answer: e

EXPLANATION:

When requests come in faster than your function can scale, or when your function is at maximum concurrency, additional requests fail with a throttling error (429 status code).

You are running a large distributed application using a mix of EC2 instances and Lambda. Your EC2 instances are spread across multiple availability zones for resilience and are configured inside a VPC. You have just developed a new Lambda function which you are testing. However, when you try to complete the testing, your function cannot access a number of application servers which are located in the same private subnet. Which of the following could be a possible reason for this?

1. The function execution role does not include permission to connect to the VPC
2. Your security group does not allow connectivity from the AWS Lambda endpoint
3. The EC2 instances need to be in the same subnet as the Lambda function
4. The EC2 instances are running in a different region to the Lambda function

Answer: a

EXPLANATION:

To connect to a VPC, your functions execution role must have the following permissions: ec2:CreateNetworkInterface, ec2:DescribeNetworkInterfaces, ec2:DeleteNetworkInterface. These permissions are included in the AWSLambdaVPCAccessExecutionRole managed policy.

You work for a company which facilitates and organizes technical conferences. You ran a large number of events this year with many high profile speakers and would like to enable your customers to access videos of the most popular presentations. You have stored all your content in S3, but you would like to restrict access so that people can only access the videos after logging into your website. How should you configure this?

1. Use CloudFront with HTTPS to enable secure access to the videos
2. Use SSE-S3 to generate a signed URL
3. Remove public read access from the S3 bucket where the videos are stored
4. Use web identity federation with temporary credentials allowing access to the videos
5. Share the videos by creating a pre-signed URL

Answer: c, e

EXPLANATION:

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects. Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

Your application communicates using messages in an SQS queue. You have noticed recently that you are seeing a large number of empty responses where no messages exist in the queue. You want to make sure that your application is responsive as possible, but the cost of the solution is also a concern. What can you do to ensure your application is both cost-effective and responsive?

1. Use short polling
2. Configure multiple queues
3. Use long polling
4. Configure multiple queues with short polling
5. Use a FIFO queue

Answer: c

EXPLANATION:

In almost all cases, Amazon SQS long polling is preferable to short polling. Long-polling requests let your queue consumers receive messages as soon as they arrive in your queue while reducing the number of empty ReceiveMessageResponse instances returned. In general, you should use maximum 20 seconds for a long-poll timeout. Because higher long-poll timeout values reduce the number of empty ReceiveMessageResponse instances returned, try to set your long-poll timeout as high as possible.

A Developer is implementing an application that must allow users to subscribe to e-mail notifications. Which AWS service is the best option for implementing this functionality?

1. WorkMail
2. SNS
3. SES
4. SQS

Answer: b

EXPLANATION:

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. In Amazon SNS, there are two types of clients: publishers and subscribers, which are also referred to as producers and consumers. Publishers communicate asynchronously with subscribers by producing and sending a message to a topic, which is a logical access point and communication channel. Subscribers (that is, web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (that is, Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.

You are planning to use CodeDeploy to deploy an application for the first time to a brand new fleet of EC2 instances. Which deployment approach would you recommend?

1. In-Place
2. Canary
3. Blue / Green
4. Rolling with additional batch

Answer: a

EXPLANATION:

In-Place is the one to use as you are installing to a new fleet of instances, therefore Blue/Green is not possible. Canary and Rolling updates are not an option for CodeDeploy

Which of the following protocols does API Gateway support?

1. O API
2. GraphQL
3. SOAP
4. REST

Answer: c, d

EXPLANATION:

API Gateway supports RESTful APIs, however the legacy SOAP protocol, which returns results in xml format, is also supported in pass-through mode.

Your application is experiencing a large number of failed requests when making calls to the S3 API. Which of the following best describes the approach used by AWS SDKs for regulating flow control when retrying failed API requests?

1. By default, the request is continuously retried until it is successful
2. Feedback Based Flow Control is used to avoid contention when retrying failed requests
3. AWS uses Exponential Backoff to manage error retries
4. AWS uses bandwidth throttling to manage flow control

Answer: c

EXPLANATION:

Numerous components on a network, such as DNS servers, switches, load balancers, and others can generate errors anywhere in the life of a given request. The usual technique for dealing with these error responses in a networked environment is to implement retries in the client application. In addition to simple retries, each AWS SDK implements exponential backoff algorithm for better flow control. The idea behind exponential backoff is to use progressively longer waits between retries for consecutive error responses.

You are working for an investment bank and have been asked to help the application support team with their annual Disaster Recovery testing. The main production PostgreSQL database is hosted in RDS Multi-AZ deployment, with multiple applications running on a combination of EC2 and Lambda. You have been asked to help the team to demonstrate the impact that a failed Availability Zone will have on the database. Which of the following do you suggest?

1. Simulate an AZ failure by deleting the primary RDS instance
2. Simulate an AZ failure by rebooting the underlying EC2 instance which is running the database
3. Simulate an AZ failure by moving your RDS instance to a different subnet
4. Simulate an AZ failure by disconnecting your RDS instance from the network
5. Simulate an AZ failure by performing a reboot with forced failover on the RDS instance

Answer: e

EXPLANATION:

If the Amazon RDS instance is configured for Multi-AZ, you can perform the reboot with a failover. An Amazon RDS event is created when the reboot is completed. If your DB instance is a Multi-AZ deployment, you can force a failover from one Availability Zone (AZ) to another when you reboot. When you force a failover of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone, and updates the DNS record for the DB instance to point to the standby DB instance. As a result, you need to clean up and re-establish any existing connections to your DB instance. Rebooting with failover is beneficial when you want to simulate a failure of a DB instance for testing, or restore operations to the original AZ after a failover occurs.

Your application is trying to upload a 6TB file to S3 and you receive an error message telling you that your proposed upload exceeds the maximum allowed object size. What is the best way to accomplish this file upload?

1. Contact AWS support to increase the maximum size of your S3 object.
2. You cannot fix this, as the maximum size of an S3 object is 5TB.
3. Use the Multipart Upload API for this object.
4. Use the S3 LargeObjectUpload API.

Answer: b

EXPLANATION:

Amazon S3 allows a maximum object size of 5TB. However, objects 5GB or larger are required to be uploaded using the multipart upload API.

You are working on social media application which allows users to share BBQ recipes and photos. You would like to schedule a Lambda function to run every 10 minutes which checks for the latest posts and sends a notification including an image thumbnail to users who have previously engaged with posts from the same user. How can you configure your function to automatically run at 10 minute intervals?

1. Use CloudWatch Events to schedule the function
2. Use EC2 with cron to schedule the function
3. Use Lambda with cron to schedule the function
4. Use AWS SWF to schedule the function

Answer: a

EXPLANATION:

You can direct AWS Lambda to execute a function on a regular schedule using CloudWatch Events. You can specify a fixed rate - for example, execute a Lambda function every hour or 15 minutes, or you can specify a cron expression.

You are building a serverless web application which will serve both static and dynamic content. Which of the following services would you use to create your application?

1. EC2
2. RDS
3. API Gateway
4. Lambda
5. Elasticache
6. S3

Answer: c, d, f

EXPLANATION:

Lambda lets you run code without provisioning servers, API Gateway is a managed service which makes APIs available to your user base in a secure way, S3 can be used to serve static web content. EC2 and RDS are not serverless. Elasticache is not required for this solution.

One of your junior developers has never had AWS Access before and needs access to an Elastic Load Balancer in your custom VPC. This is the first and only time she will need access. Which of the following choices is the most secure way to grant this access?

1. Let her log in with Admin credentials and change the Admin password when she is finished.
2. None of these.
3. Add that developer to a Group with the requisite access (although that group may have \*more\* permissions than are needed for the Dev to do her job).
4. Create a new IAM user with \*only\* the required credentials and delete that IAM user after the developer has finished her work.

Answer: d

EXPLANATION:

It's always best practice to grant users access via IAM roles and groups. In this case, we would \*not\* assign the junior Dev to an existing group, as most Dev groups will have \*more\* access than is required for this Dev to perform the single task she has been asked to accomplish. Remember - always grant the \*fewest\* privileges possible.

You need to allow another AWS account access to resources in your AWS account, what is the recommended mechanism to configure this?

1. Use Cognito to allow the third party to sign-up as a guest user to get temporary access to your account
2. Provide AWS credentials to the third party so that they can log into your account and access the resources they need
3. Configure Web Identity Federation to allow them to log in to your account
4. Configure cross account access by creating a role in your account which has permission to access only the resources they need. Allow the third party account to assume the role based on their account ID and unique external ID

Answer: d

EXPLANATION:

Roles are the primary way to grant cross-account access. With IAM roles, you can grant third parties access to your AWS resources without sharing your AWS security credentials. Instead, the third party can access your AWS resources by assuming a role that you create in your AWS account.

A developer needs to share an EBS volume with a second AWS account. What actions need to be performed to accomplish this task in the most optimal way?

1. Create an AMI from the EC2 instance. Modify image permissions and add a second AWS account ID to share the AMI. Ensure 'create volume' permissions are added. In the second AWS account, create an EC2 instance using the shared AMI.
2. Create an IAM policy granting necessary actions on the specific EBS volume. Add the second AWS account ID in the Principal element.
3. Create an EBS volume snapshot. Modify S3 bucket policy granting the second AWS account access to the S3 object of the snapshot. In the second AWS account, create an EBS volume from the S3 object.
4. Create an EBS volume snapshot. Modify EBS snapshot permissions and add the second AWS account ID to share the snapshot. In the second AWS account, create an EBS volume from the snapshot.

Answer: d

EXPLANATION:

It is not possible to directly share an EBS volume with another account. In order to accomplish the required task, it is required to create an EBS volume snapshot and grant permissions to that snapshot to the second AWS account. Although EBS volume snapshots are stored in S3, they are not in a user-visible bucket. Sharing a private AMI with a second account does not meet the specific requirement as defined in the question.

A financial services organization is using Amazon S3 service to store highly sensitive data. What is the correct IAM Policy that must be applied to ensure that all objects uploaded to the S3 bucket are encrypted?

1. { "Version":"2012-10-17", "Id":"PutObjPolicy", "Statement":[{ "Sid":"DenyUnEncryptedObjectUploads", "Effect":"Deny", "Principal":"\*", "Action":"s3:PutObject", "Resource":"arn:aws:s3:::SensitiveDataBucket/\*", "Condition":{ "StringNotEquals":{ "s3:sse-encryption-cipher":"AES256" } } } ] }
2. { "Version":"2012-10-17", "Id":"PutObjPolicy", "Statement":[{ "Sid":"DenyUnEncryptedObjectUploads", "Effect":"Deny", "Principal":"\*", "Action":"s3:PutObject", "Resource":"arn:aws:s3:::SensitiveDataBucket", "Condition":{ "StringNotEquals":{ "s3:x-amz-server-side-encryption":"AES256" } } } ] }
3. { "Version":"2012-10-17", "Id":"PutObjPolicy", "Statement":[{ "Sid":"DenyUnEncryptedObjectUploads", "Effect":"Deny", "Principal":"\*", "Action":"s3:PutObject", "Resource":"arn:aws:s3:::SensitiveDataBucket", "Condition":{ "StringNotEquals":{ "s3:sse-encryption-cipher":"AES256" } } } ] }
4. { "Version":"2012-10-17", "Id":"PutObjPolicy", "Statement":[{ "Sid":"DenyUnEncryptedObjectUploads", "Effect":"Deny", "Principal":"\*", "Action":"s3:PutObject", "Resource":"arn:aws:s3:::SensitiveDataBucket/\*", "Condition":{ "StringNotEquals":{ "s3:x-amz-server-side-encryption":"AES256" } } }

Answer: d

EXPLANATION:

In IAM Policy, the optional condition block enables specification of conditions for when a policy is in effect. In the Condition block, condition operators (such as equal, less than, etc.), the condition keys, and values can be combined into an expression to be evaluated. The IAM policy is applied when the condition expression is true. Condition key s3:x-amz-server-side-encryption must be used to validate that the object being uploaded is encrypted. Resource S3 ARN must include /\* at the end of the S3 bucket name to be a valid ARN.

Your EC2 instance needs to access a number of files which have been encrypted using KMS. Which of the following must be configured in order for the EC2 instance to successfully read the files?

1. The Key Policy must allow the instance role to use the CMK
2. The EC2 instance must have an instance role which has permission run the decrypt operation
3. The Key Policy must allow the IAM user to use the CMK
4. The IAM user associated with the application must have a role which has permission run the decrypt operation

Answer: a, b

EXPLANATION:

Manage access to KMS keys using a key policy. In the key policy, you must specify the principal (the identity) that the permissions apply to. You can specify AWS accounts (root), IAM users, IAM roles, and some AWS services as principals in a key policy. You can use IAM policies in combination with key policies to control access to your customer master keys (CMKs) in AWS KMS.

You are working on a mobile phone app for an online retailer which stores customer data in DynamoDB. You would like to allow new users to sign-up using their Facebook credentials. What is the recommended approach?

1. After the user has authenticated with Facebook, allow them to download encrypted AWS credentials to their device so that the mobile app can access DynamoDB
2. Embed encrypted AWS credentials into the application code, so that the application can access DynamoDB on the user's behalf.
3. Write your own custom code which allows the user to log in via Facebook and receive an authentication token, then calls the AssumeRoleWithWebIdentity API and exchanges the authentication tokens for temporary access to DynamoDB
4. After the user has successfully logged in to Facebook and received an authentication token, Cognito should be used to exchange the token for temporary access to DynamoDB

Answer: d

EXPLANATION:

For mobile applications, using Cognito as an ID broker is the recommended approach to enabling user sign-up, sign-in and guest access using Web Identity Providers like Facebook.

Which of the following does Cognito use to manage sign-up and sign-in functionality for mobile and web applications?

1. User Pools
2. IAM Users
3. Identity Pools
4. IAM Groups

Answer: a

EXPLANATION:

Cognito User Pools are like a directory, allowing users sign-up and sign-in. Identity pools are used to grant temporary access to unauthenticated guests. IAM users are user account entities which allow you to interact with AWS resources. IAM groups are collections of IAM users and are used to specify permissions for multiple users.

You are developing a video streaming application which users can access using multiple devices, for example, laptop, tablet and cell phone. You would like to be able to track usage across the different devices and limit the number of devices from which a user can stream content. Which of the following AWS technologies could you use to achieve this?

1. Use a Lambda function to store session state and device type in DynamoDB
2. Use S3 to store metadata about the device and link it to session state held in DynamoDB
3. Store device metadata linked to session state in ElastiCache
4. Use Cognito
5. Use MFA on the device

Answer: d

EXPLANATION:

Cognito enables developers to remember the devices on which end-users sign in to their application. You can see the remembered devices and associated metadata through the console. In addition, you can build custom functionality using the notion of remembered devices. For example, with a content distribution application (e.g., video streaming), you can limit the number of devices from which an end-user can stream their content.

You have provisioned an RDS database and then deployed your application servers using Elastic Beanstalk. You now need to connect your application servers to the database. What should you do?

1. Configure Elastic Beanstalk to install a database client on your application servers
2. Provide the database connection information to your application
3. Provide the ip address of the RDS instance to Elastic Beanstalk
4. Configure a security group allowing access to the database and add it to your environments auto-scaling group

Answer: b, d

EXPLANATION:

As you are connecting to a database that was not created within your Elastic Beanstalk environment, you will need to create the Security Group yourself and also provide connection string and credentials to allow your application servers to connect to the database

You have an application running on multiple EC2 instances, however every time an instance fails, your users complain that they lose their session. What can you do to prevent this from happening?

1. Store session state in on a dedicated EC2 instance
2. Store session state in RDS
3. Store session state in S3
4. Store session state in on the Elastic Load Balancer
5. Store session state in ElastiCache

Answer: e

EXPLANATION:

There are various ways to manage user sessions including storing those sessions locally to the node responding to the HTTP request or designating a layer in your architecture which can store those sessions in a scalable and robust manner. Common approaches used include utilizing Sticky sessions or using a Distributed Cache for your session management. In order to address scalability and to provide a shared data storage for sessions that can be accessed from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution for this is to leverage an In-Memory Key/Value store such as ElastiCache.

Your mobile application needs to read data from DynamoDB. What is the best way to give mobile devices permissions to read from DynamoDB?

1. Issue an access key and secret access key to each user.
2. Create an IAM role for your users.
3. Create an IAM role that can be assumed by an app that allows federated users.
4. Connect your application to an EC2 instance with permission to read from DynamoDB.

Answer: c

EXPLANATION:

Web identity federation removes the need for creating individual IAM users. Instead, users can sign in to an identity provider and then obtain temporary security credentials from the AWS Security Token Service.

You work for a large pharmaceuticals company which is conducting drug trials for a number of new products. You are using SQS to handle messaging between components of a distributed application. You need to ensure that confidential data relating to your patients is encrypted, which of the following services will you use to centrally rotate the encryption keys?

1. AWS KMS
2. SSE-S3
3. Client-side encryption
4. HTTPS

Answer: a

EXPLANATION:

You can use a CMK to encrypt and decrypt up to 4 KB (4096 bytes) of data. Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of AWS KMS to encrypt your data. This strategy is known as envelope encryption. CMKs are created in AWS KMS and never leave AWS KMS unencrypted. To use or manage your CMK, you access them through AWS KMS.

You are developing a healthy-eating application which tracks nutrition and water intake on a daily basis. Your users mainly access the application using a mobile device like a cell phone or tablet. You are planning to run a promotion to attract new users by providing a free trial period and you would like to make it easy for guest users to trial your application. Which of the following can you use to configure access for guest users?

1. Identity Federation with SAML
2. IAM User Pools
3. Identity Federation with AWS
4. Cognito Identity Pools

Answer: d

EXPLANATION:

With a Cognito identity pool, your users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB. Identity pools support anonymous guest users, as well as federation through third-party IdPs.

You are working on an application which handles online credit card applications. It consists of a number of web and application servers running on EC2, customer reference data stored in S3 and transactional data stored in RDS. The security team have noticed that you have a lot of sensitive customer information stored in S3 and you have been asked to configure encryption at rest to protect the data. How can you do this?

1. Select default encryption on your S3 bucket
2. Encrypt your local root disk before uploading the files
3. Encrypt the files locally using the AWS Encryption SDK
4. Use SSL to upload the files

Answer: a

EXPLANATION:

You can set default encryption on a bucket so that all objects are encrypted when they are stored in the bucket. When you use server-side encryption, Amazon S3 encrypts an object before saving it to disk in its data centers and decrypts it when you download the objects.

Your application uses the STS API call AssumeRoleWithWebIdentity to enable access for users who have authenticated using a Web ID provider. Which of the following best describe what is returned by a successful call to AssumeRoleWithWebIdentity?

1. AssumeRoleWithWebIdentity returns a set of temporary credentials (access key ID, secret access key and security token) which give temporary access to AWS services
2. AssumeRoleWithWebIdentity returns a the ARN of the IAM role that the user is allowed to assume temporarily
3. AssumeRoleWithWebIdentity returns a the ARN of the IAM user that the user is allowed to assume temporarily
4. AssumeRoleWithWebIdentity returns an assumed role ID which the user is allowed to assume temporarily

Answer: a

EXPLANATION:

AssumeRoleWithWebIdentity returns a set of temporary credentials, giving the user temporary access to AWS. It also returns an Amazon Resource Name (ARN) and the assumed role ID, which are identifiers that you can use to refer to the temporary security credentials.

What is the name of the service that allows users to use their social media account to gain temporary access to the AWS platform?

1. Web Identity Federation
2. Web Confederation Services
3. Active Directory Authentication Services
4. Facebook Sign In Service

Answer: a

EXPLANATION:

Web Identity Federation is the services which allows users to authenticate with web Identity Providers like Facebook, Google and Amazon receive an authentication token and then exchange that token for temporary security credentials in AWS.