Top of Form

Your users upload files to Amazon S3 Bucket. You have set up encryption using SSE-KMS. You have provided your uses with permission to do a PutObject on the specific bucket in Amazon S3. However, users are receiving access denied error when they upload new objects. Which of these could help the users to upload objects?

* 

**Apart from the PutObject permission, you should also give kms:GenerateDataKey permission to generate the data key**

**(Correct)**

* 

**Apart from the PutObject permission, you should also give kms:CreateDataKey permission to generate the data key**

* 

**Apart from the PutObject permission, you should also give kms:GenerateDataKey and kms:Decrypt permissions**

* 

**Apart from the PutObject permission, you should also give GetObject permission since once the file is placed, to give the response this permission is required**

**(Incorrect)**

**Explanation**

**KMS with S3 (or DynamoDB or SQS or ..)**

**What happens in the background?**

Envelope Encryption with API calls

GenerateDataKey while storing

Decrypt while retrieval

**What permissions are needed?**

KMS Key Policy on CMK (Resource Policy) allows access from the service (S3 or DynamoDB or ..)

Your IAM policy allows access to perform the operation on KMS

Call to s3:PutObject would need access to kms:GenerateDataKey if encryption is enabled on the S3 bucket!

**What could go wrong?**

No Permissions - Check KMS Key Policy and User's IAM policy

Throttling - Retry with Exponential Backoff or Increase KMS Quotas

Bottom of Form

Top of Form

Question 2: **Incorrect**

**You are building a Mobile app. You want to support SAML and Facebook authentication. You want to provide authorization to content in Amazon DynamoDB. Which of these options would you recommend?**

* 

**IAM Role**

**(Incorrect)**

* 

**Cognito IAM**

* 

**Cognito User pool**

* 

**Cognito Identity pool**

**(Correct)**

**Explanation**

Whenever you need to provide federated users with authorization for AWS resources, you would need to go for an Identity pool.

**Amazon Cognito - Identity pools**

Identity pools provide **AWS credentials** to **grant your users access to other AWS resources**

Connect identity pools with **authentication (identity) providers**: Your own user pool OR Amazon, Apple, Facebook, Google+, Twitter OR OpenID Connect provider OR SAML identity providers (SAML 2.0)

Configure **multiple** authentication (identity) providers for each identity pool

Bottom of Form

Top of Form

Question 3: **Incorrect**

**You would like to secure your website using HTTPS. But you do not want to add additional load to your EC2 instances to handle encryption. Which of these approaches would you recommend?**

* 

**Setup an SSL certificate on the Application Load Balancer using AWS Certificate Manager.**

* 

**Create the HTTPS listener on Application Load Balancer. Perform SSL pass through at the Application Load Balancer.**

* 

**Create the HTTPS listener on Application Load Balancer. Perform SSL termination at the Application Load Balancer.**

**(Correct)**

* 

**Create a HTTP listener on Application Load Balancer. Perform SSL pass through at the Application Load Balancer.**

**(Incorrect)**

**Explanation**

By performing SSL termination at the ELB, we ensure that the EC2 instances do not need about SSL

Bottom of Form

Top of Form

Question 4: **Incorrect**

**You are running an Amazon Kinesis streams based application with 4 shards. You are using Amazon Kinesis client library to process the data from the streams. Which of the below statements are true about KCL instances?**

* 

**Each shard can be read from multiple KCL instances. This way data can be processed quickly.**

* 

**One shard can only be read from one and only one KCL instance.**

**(Correct)**

* 

**A KCL instance has to run only on Docker instance and it can't run on EC2 instance**

* 

**One KCL instance can read from one and only one shard.**

**(Incorrect)**

**Explanation**

One shard can be read from only one KCL instance. A single KCL instance can read from multiple shards (However, it is recommended to have one KCL instance reading from one shard).

Bottom of Form

Top of Form

Question 5: **Correct**

**You are running web application on multiple EC2 instances load balanced using an Application Load Balancer. You would want to create your own user base and authenticate them. However, you do not want to burden EC2 instances with the authentication process. Which of these is the simplest solution to implement this?**

* 

**Use IAM roles and policies**

* 

**Integrate ALB with an Cognito user pool**

**(Correct)**

* 

**Integrate ALB with an Lambda Authorizer**

* 

**Integrate ALB with an Cognito Identity pool**

**Explanation**

Use the Cognito user pool.

*You can configure an Application Load Balancer to securely authenticate users as they access your applications. This enables you to offload the work of authenticating users to your load balancer so that your applications can focus on their business logic.*

***The following use cases are supported:***

*Authenticate users through an identity provider (IdP) that is OpenID Connect (OIDC) compliant.*

*Authenticate users through well-known social IdPs, such as Amazon, Facebook, or Google, through the user pools supported by Amazon Cognito.*

*Authenticate users through corporate identities, using SAML, LDAP, or Microsoft AD, through the user pools supported by Amazon Cognito.*

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

Bottom of Form

Top of Form

Question 6: **Incorrect**

You are running a website and you capture user activities in an Amazon DynamoDB table. Each user activity is stored in an item. To keep the data volume under control, you want to set up a mechanism to delete the items after a month. How you can achieve this in Amazon DynamoDB without incurring costs?

* 

**Add a timestamp column to the row and setup TTL based on the timestamp column. Amazon DynamoDB automatically deletes the records once the TTL is reached.**

**(Correct)**

* 

**Setup the TTL in the Amazon DynamoDB table at table level. There is no need to add a additional column. Once TTL is enabled, Amazon DynamoDB based on the created timestamp will automatically deletes the record.**

* 

**Setup the TTL in the Amazon DynamoDB table at the row level. There is no need to add a additional column. Once TTL is enabled, Amazon DynamoDB based on the created timestamp will automatically deletes the record.**

**(Incorrect)**

* 

**Add a timestamp column to the row in the Amazon DynamoDB and run a Lambda function which goes through this records and deletes records which are older than the desired period**

**Explanation**

You can use an existing column of type timestamp OR you need to add a column of type timestamp. After that, we can enable TTL for that column.

The item would be deleted if the TTL attribute value older than the current time

Does not consume WCU

Bottom of Form

Top of Form

Question 7: **Correct**

**You are working with a major legal firm that handles mergers and acquisitions. Your organization produces a lot of legal content that needs to be securely stored. Documents older than 10 years are rarely accessed. But, they have to be retained for compliance. You will have a 2-week notice if you need them. Which AWS storage solution is cost-effective for your documents older than 10 years?**

* 

**S3 Glacier Deep Archive**

**(Correct)**

* 

**S3 Glacier**

* 

**AWS EBS**

* 

**AWS EFS**

**Explanation**

**Standard-IA**Long-lived, infrequently accessed data (backups for disaster recovery)

**One Zone-IA**Long-lived, infrequently accessed, non-critical data (Easily re-creatable data - thumbnails for images)

**Intelligent-Tiering**Long-lived data with changing or unknown access patterns

**Glacier** Archive data with retrieval times ranging from minutes to hours

**Glacier Deep Archive** Archive data that rarely, if ever, needs to be accessed with retrieval times in hours

**Reduced Redundancy (Not recommended)** Frequently accessed, non-critical data

Bottom of Form

Top of Form

Question 8: **Incorrect**

**You are a Solution Architect for a video processing enterprise. Customers upload videos to your website and you convert them into video formats customized for different devices. You are using a Standard SQS queue to manage the conversion requests. EC2 instances running the video conversion application process the messages from the SQS queue. You are planning to start a premium service and offer immediate conversion for your premium customers. Which of these options would you recommend to give high priority to conversion requests from premium customers?**

* 

**Use two different SQS queues. One for free and other for premium users. Adjust the number of instances of video conversion application as needed.**

**(Correct)**

* 

**SQS does not support this feature. Replace SQS with SNS.**

* 

**Change from Standard SQS queue to FIFO SQS queue. FIFO SQS queue allows you to process messages with higher priority first.**

**(Incorrect)**

* 

**Increase the SQS message priority if the customer is a premium customer. Your video conversion application can process messages with higher message priority first.**

Bottom of Form

Top of Form

Question 9: **Correct**

**Your organization wants to store customer information in Amazon S3 with encryption at rest. You want to manage the encryption CMKs in an AWS Managed Service. Which of these options would you recommend?**

* 

**Use Server Side Encryption with Amazon S3 managed keys**

* 

**Use Server Side Encryption with Customer provided Keys**

* 

**Use Server Side Encryption with AWS KMS**

**(Correct)**

* 

**Use Client Side Encryption with Customer provided Keys**

**Explanation**

SSE-S3:

AWS S3 manages its own keys

Keys are rotated every month

Request Header - x-amz-server-side-encryption(AES256)

SSE-KMS:

Customer manages keys in KMS

Request Headers - x-amz-server-side-encryption(aws:kms) and x-amz-server-side-encryption-aws-kms-key-id(ARN for key in KMS)

SSE-C:

Customer sends the key with every request

S3 performs encryption and decryption without storing the key

HTTPS is mandatory

Bottom of Form

Top of Form

Question 10: **Incorrect**

**You are using AWS Elastic Beanstalk to deploy your application. Performing deployments quickly is a high priority for you. Application downtime during the deployment is acceptable. Which of these options would you recommend?**

* 

**Rolling deployment**

**(Incorrect)**

* 

**All at once**

**(Correct)**

* 

**Immutable**

* 

**Rolling with additional batch**

**Explanation**

**AWS Elastic Beanstalk - Deployment methods**

**All at once** – Deploy V2 to all existing instances in a SINGLE batch.

**Rolling** – Deploy V2 to existing instances in multiple batches. Deployment of the next batch starts after the current batch is successful.

**Rolling with additional batch** – Deploy V2 to new/existing instances in multiple batches. Launches a new batch with V2 first. Each batch with V2 will replace existing instances with V1 deployed.

**Immutable** – Second ASG created with V2. The new version and Old version serve traffic until all V2 instances pass health checks.

**Traffic splitting** – Canary testing approach. Deploy V2 to a few new instances. Send a portion of traffic to V2 (While serving the majority of users from V1).

**(ADDITIONAL OPTION) BLUE GREEN with SWAP URL** - Create New Environment with V2 instances. Test them. SWAP URL of V1 environment with V2 environment. One time switch! You can clone the V1 environment and deploy the V2 all at once!

Bottom of Form

Top of Form

Question 11: **Incorrect**

**You would want to create an application generating reports on a schedule using AWS Elastic Beanstalk. Which of these approaches would you recommend?**

* 

**Setup a web server environment using .ebextensions file**

* 

**Setup a docker environment using .ebextensions file**

**(Incorrect)**

* 

**Setup a worker environment and schedule using cron.yaml**

**(Correct)**

* 

**Setup a web server environment and schedule using cron.yaml**

Bottom of Form

Top of Form

Question 12: **Incorrect**

**You are using Amazon DynamoDB to store data. You are observing data overwrites during concurrent updates causing data quality issues. Which of these options would you recommend to avoid data overwrites?**

* 

**Conditional Update**

**(Correct)**

* 

**Strongly Consistent Update**

* 

**Atomic Update**

**(Incorrect)**

* 

**Consistent Update**

**Explanation**

**Conditional expression**

aws dynamodb delete-item --table-name MyTodos \

--key '{"id": {"S": "2"}}' \

--condition-expression "#desc=:desc" \

--expression-attribute-names '{"#desc":"desc"}' \

--expression-attribute-values '{":desc":{"S":"Learn to Dance"}}'

Update/delete an item only if the condition expression is true

Enables you to check for consistency of update/delete

Error message if the check fails - An error occurred (ConditionalCheckFailedException) when calling the DeleteItem operation: The conditional request failed

Bottom of Form

Top of Form

Question 13: **Incorrect**

**You are setting up an API Gateway to expose your Rest API. This REST API will be consumed from multiple global applications. You would want to implement authorization using a 3rd party authorization mechanism. Which of these approaches would you recommend?**

* 

**Cognito User Pool based authorization**

* 

**Cognito Identity Pool Based Authorization**

* 

**IAM & Resource Policy Based Authorization**

**(Incorrect)**

* 

**Write a Custom Lambda function and use Lambda Authorizer**

**(Correct)**

**Explanation**

**API Gateway - Authorization**

**Open** - No authentication or authorization

**IAM Permissions** - Use IAM Policies and AWS credentials to grant access

**Amazon Cognito authorizer** - Connect to Amazon Cognito User Pool (possible to use OAuth authorization)

**Lambda authorizers** - Write custom lambda function to validate the bearer token (OAuth or SAML for example), or request parameters

Bottom of Form

Top of Form

Question 14: **Correct**

**Your application in AWS uses Amazon DynamoDB. You are going to add a new client reading at a rate of 100 items per second. Size of each item is 4KB. Your client uses eventually consistent reads. How many additional RCU's are needed to support your new client?**

* 

**10**

* 

**25**

* 

**100**

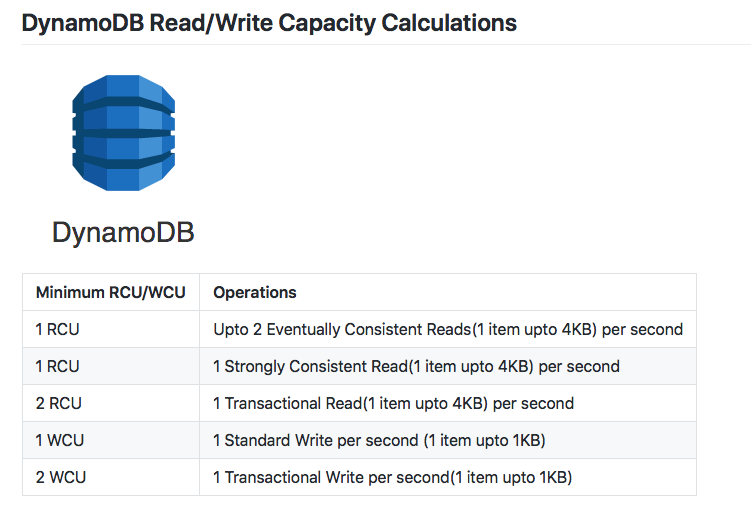
* 

**50**

**(Correct)**

**Explanation**

1 RCU will allow eventually consistent reads of 2 items of 4 KB size. So for 100 items, it will be 50 RCUs.



Bottom of Form

Top of Form

Question 15: **Incorrect**

**You are hosting a website using Amazon S3 Bucket. Your website has a global user base. It is getting popular by the day. You are looking to improve user experience by providing them with better performance. Which of these options would you recommend?**

* 

**Use Amazon CloudFront to distribute content from Amazon S3 Bucket.**

**(Correct)**

* 

**Amazon S3 is a managed service. So, you do not need to worry about performance.**

**(Incorrect)**

* 

**Use Cross Region Replication and host multiple Amazon S3 Buckets in different Regions.**

* 

**Create a Application Load Balancer and configure Amazon S3 Bucket as the target.**

**Explanation**

**Important things to remember about Amazon CloudFront**

Serve users from nearest edge location (based on user location)

Source content can be from S3, EC2, ELB and External Websites

If content is not available at the edge location, it is retrieved from the origin server and cached

No minimum usage commitment

Provides features to protect your private content

Bottom of Form

Top of Form

Question 16: **Incorrect**

**In the SAM template, which of these is mandatory (in addition to resources)?**

* 

**Variables**

* 

**Conditions**

**(Incorrect)**

* 

**Transform**

**(Correct)**

* 

**Parameters**

**Explanation**

Transform and Resources sections are mandatory in a SAML template.

AWSTemplateFormatVersion: '2010-09-09'

Transform: AWS::Serverless-2016-10-31

Resources:

CreateThumbnail:

Type: AWS::Serverless::Function

Properties:

Handler: handler

Runtime: runtime

Timeout: 60

Policies: AWSLambdaExecute

Events:

CreateThumbnailEvent:

Type: S3

Properties:

Bucket: !Ref SrcBucket

Events: s3:ObjectCreated:\*

SrcBucket:

Type: AWS::S3::Bucket

Bottom of Form

Top of Form

Question 17: **Incorrect**

**Your application uses an Amazon DynamoDB table to store information. There are quite a lot of updates happening to your tables everyday. You would like to capture the change history of the records - old records and new records. What are the recommended options? Choose TWO**

* 

**The default view type of the streams is new and previous image. So developer don't need to do anything extra.**

* 

**The developer should choose the view type previous image**

* 

**The developer must choose the view type new and old images of the item**

**(Correct)**

* 

**The developer must choose the view type new image**

* 

**The developer must enable Amazon DynamoDB streams**

**(Correct)**

**Explanation**

**DynamoDB Streams**

DynamoDB streams capture a time-ordered sequence of item modifications. Stored up to 24 hours.

StreamViewType decides what is captured on the stream record (**KEYS\_ONLY, NEW\_IMAGE, OLD\_IMAGE, NEW\_AND\_OLD\_IMAGES**)

Bottom of Form

Top of Form

Question 18: **Correct**

**You are running a Lambda function in AWS Account A. It needs to connect to Amazon DynamoDB running in another account (target account B). Which of these approaches would you recommend?**

* 

**Create a IAM role in Account B with Amazon DynamoDB access. Modify the trust policy of the Lambda execution role in Account A to allow to assume this role in Account B. Lambda function code has to be modified to add the AssumeRole API call.**

* 

**Create a IAM role in Account B with Amazon DynamoDB access. Modify the trust policy of the role in Account B to allow the Lambda execution role to assume this role. Lambda function code needs to be modified to make the AssumeRole API call.**

**(Correct)**

* 

**Update the Amazon DynamoDB resource policy in Account B to allow the Lambda execution role from Account A to make a call to the Amazon DynamoDB.**

* 

**Make the Lambda run inside the VPC and create an VPC end point to access DynamoDB.**

**Explanation**

**IAM Role: Cross-Account Access - Provide access to content in Amazon S3 from PROD Account to DEV account**