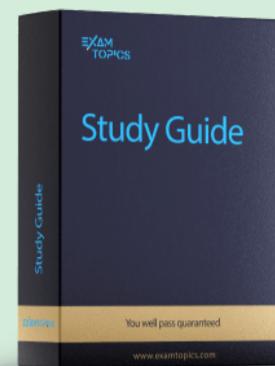




- Expert Verified, Online, **Free**.

Prepare for your AWS Certified Developer - Associate DVA-C02 exam with additional products



Study Guide

1091 PDF Pages

\$19.99

[Buy Now](#)

[Custom View Settings](#)

Question #151

Topic 1

A team of developers is using an AWS CodePipeline pipeline as a continuous integration and continuous delivery (CI/CD) mechanism for a web application. A developer has written unit tests to programmatically test the functionality of the application code. The unit tests produce a test report that shows the results of each individual check. The developer now wants to run these tests automatically during the CI/CD process.

Which solution will meet this requirement with the LEAST operational effort?

- A. Write a Git pre-commit hook that runs the tests before every commit. Ensure that each developer who is working on the project has the pre-commit hook installed locally. Review the test report and resolve any issues before pushing changes to AWS CodeCommit.
- B. Add a new stage to the pipeline. Use AWS CodeBuild as the provider. Add the new stage after the stage that deploys code revisions to the test environment. Write a buildspec that fails the CodeBuild stage if any test does not pass. Use the test reports feature of CodeBuild to integrate the report with the CodeBuild console. View the test results in CodeBuild. Resolve any issues.
- C. Add a new stage to the pipeline. Use AWS CodeBuild as the provider. Add the new stage before the stage that deploys code revisions to the test environment. Write a buildspec that fails the CodeBuild stage if any test does not pass. Use the test reports feature of CodeBuild to integrate the report with the CodeBuild console. View the test results in CodeBuild. Resolve any issues.
- D. Add a new stage to the pipeline. Use Jenkins as the provider. Configure CodePipeline to use Jenkins to run the unit tests. Write a Jenkinsfile that fails the stage if any test does not pass. Use the test report plugin for Jenkins to integrate the report with the Jenkins dashboard. View the test results in Jenkins. Resolve any issues.

Correct Answer: D

Community vote distribution

C (86%)

14%

https://shop335422782.taobao.com 淘宝搜索店铺:黑马专业认证
微信添加 hello23119

SerialiDr 1 month, 2 weeks ago

Selected Answer: C

This is the most efficient and integrated approach. AWS CodeBuild is fully integrated with AWS CodePipeline and can be used to run unit tests as part of the CI/CD process. Placing the testing stage before deployment ensures that only tested code is deployed. The buildspec can be configured to fail the build if tests do not pass, and CodeBuild's test reports feature allows for easy viewing and analysis of test results.

upvoted 1 times

NinjaCloud 4 months ago

Correct answer: B
upvoted 1 times

https://shop335422782.taobao.com 淘宝搜索店铺:黑马专业认证
微信添加 hello23119

Gold07 4 months, 3 weeks ago

c is the correct answer
upvoted 1 times

Cerakoted 4 months, 3 weeks ago

Selected Answer: C

I think C is correct.
Typical consists of stages are..
Build -> Test -> Deploy(test) -> Load Test -> and others
upvoted 2 times

dilleman 4 months, 3 weeks ago

Selected Answer: C

C should be correct.
upvoted 3 times

Digo30sp 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Solution (B) is the simplest and requires the least operational effort. It involves adding a new stage to the CodePipeline pipeline that uses AWS CodeBuild to run the unit tests. The CodeBuild stage can be configured to fail if any tests fail. The CodeBuild test report can be integrated into the CodeBuild console so that developers can view test results.

upvoted 1 times

dilleman 4 months, 3 weeks ago

This does not make sense. Why run the tests after the deploy when you can choose option C, to run the tests before the deploy? C should be best practice and the same amount of effort as B.

upvoted 5 times

✉  **Dibaal** 4 months, 1 week ago

funny 😂

upvoted 1 times

Question #152

Topic 1

A company has multiple Amazon VPC endpoints in the same VPC. A developer needs to configure an Amazon S3 bucket policy so users can access an S3 bucket only by using these VPC endpoints.

Which solution will meet these requirements?

- A. Create multiple S3 bucket policies by using each VPC endpoint ID that have the aws:SourceVpce value in the StringNotEquals condition.
- B. Create a single S3 bucket policy that has the aws:SourceVpc value and in the StringNotEquals condition to use VPC ID.
- C. Create a single S3 bucket policy that has the aws:SourceVpce value and in the StringNotEquals condition to use vpce*.
- D. Create a single S3 bucket policy that has multiple aws:sourceVpce value in the StringNotEquals condition. Repeat for all the VPC endpoint IDs.

Correct Answer: C

Community vote distribution



✉️ **CrescentShared** 3 months, 2 weeks ago

I don't think any of the options is correct. Seriously StringNotEquals not StringEquals?

upvoted 5 times

✉️ **shake76** 2 months, 3 weeks ago

I think the same "A developer needs to configure an Amazon S3 bucket policy so users can access an S3 bucket only by using these VPC endpoints"

upvoted 1 times

✉️ **dilleman** 4 months, 3 weeks ago

Selected Answer: D

C works as well but It is a broad solution I think it's better practice to use D and specify the exact endpoints that the user can access from.

"aws:sourceVpce": ["vpce-id1", "vpce-id2", "..."]

upvoted 5 times

✉️ **KarBiswa** 6 days, 14 hours ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html> typically explained the same scenario. D beyond doubt.

upvoted 1 times

✉️ **cajilaxu** 4 weeks, 1 day ago

Selected Answer: D

D is right answer

Get up-to-date <https://www.pinterest.com/pin/937522847419120392>

upvoted 1 times

✉️ **joshnort** 1 month ago

Selected Answer: D

D, based on the following documentation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html#example-bucket-policies-restrict-access-vpc-endpoint>

upvoted 1 times

✉️ **CrescentShared** 1 month ago

Why it's StringNotEquals instead of StringEquals? Is the question wrong or my English is too bad to understand this?

upvoted 2 times

✉️ **SerialiDr** 1 month, 2 weeks ago

Selected Answer: D

This option is the closest to being correct, but it should use StringEquals instead of StringNotEquals. The correct approach is to use a single S3 bucket policy with a condition that includes aws:SourceVpce with StringEquals for the specific VPC endpoint IDs. This will ensure that access is allowed only from those specified endpoints.

upvoted 2 times

✉️ **rrshah83** 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html#example-bucket-policies-restrict-access-vpc>

upvoted 2 times

✉ **Certified101** 2 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

✉ **PrakashM14** 4 months, 3 weeks ago

Selected Answer: D

in option C :

```
Condition": {  
    "StringNotEqualsIfExists": {  
        "aws:sourceVpce": "vpce*"  
    }  
}
```

it might Deny access from all VPC endpoints.

so the ans is D

upvoted 2 times

✉ **ekutas** 4 months ago

D says "aws:sourceVpce value in the StringNotEquals condition". StringNotEquals won't work, it deny access for specified VPC ids

upvoted 1 times

✉ **ekutas** 4 months ago

Of course if we use "Effect": "Allow")

upvoted 2 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Solution (C) is the simplest and will meet the company's requirements. It creates a single S3 bucket policy that has the value aws:SourceVpce and the StringNotEquals condition to use vpce*. This will only allow users who are using a VPC endpoint in the same VPC to access the S3 bucket.

upvoted 1 times

Question #153

Topic 1

A company uses a custom root certificate authority certificate chain (Root CA Cert) that is 10 KB in size to generate SSL certificates for its on-premises HTTPS endpoints. One of the company's cloud-based applications has hundreds of AWS Lambda functions that pull data from these endpoints. A developer updated the trust store of the Lambda execution environment to use the Root CA Cert when the Lambda execution environment is initialized. The developer bundled the Root CA Cert as a text file in the Lambda deployment bundle.

After 3 months of development, the Root CA Cert is no longer valid and must be updated. The developer needs a more efficient solution to update the Root CA Cert for all deployed Lambda functions. The solution must not include rebuilding or updating all Lambda functions that use the Root CA Cert. The solution must also work for all development, testing, and production environments. Each environment is managed in a separate AWS account.

Which combination of steps should the developer take to meet these requirements MOST cost-effectively? (Choose two.)

- A. Store the Root CA Cert as a secret in AWS Secrets Manager. Create a resource-based policy. Add IAM users to allow access to the secret.
- B. Store the Root CA Cert as a SecureString parameter in AWS Systems Manager Parameter Store. Create a resource-based policy. Add IAM users to allow access to the policy.
- C. Store the Root CA Cert in an Amazon S3 bucket. Create a resource-based policy to allow access to the bucket.
- D. Refactor the Lambda code to load the Root CA Cert from the Root CA Cert's location. Modify the runtime trust store inside the Lambda function handler.
- E. Refactor the Lambda code to load the Root CA Cert from the Root CA Cert's location. Modify the runtime trust store outside the Lambda function handler.

Correct Answer: CE*Community vote distribution*

kiwtirApp Highly Voted 4 months, 2 weeks ago

Selected Answer: AE

The max size of storage in Secrets Manager is 10kb. For SSM Parameter store, it's 8Kb.

Correct options are A and E.

upvoted 9 times

not_a_bot_definitely 3 months ago

Secrets Manager is not cost-effective compared to option C - S3 bucket.
Question clearly asks "MOST cost-effective"

<https://www.examtopics.com/discussions/amazon/view/96242-exam-aws-certified-developer-associate-topic-1-question-429/>

So answer is CE

upvoted 4 times

KarBiswa Most Recent 6 days, 14 hours ago

Selected Answer: AE

After going through the links :

A : <https://aws.amazon.com/blogs/security/use-aws-secrets-manager-to-simplify-the-management-of-private-certificates/>
E : <https://docs.aws.amazon.com/acm/latest/userguide/renew-private-cert.html>

upvoted 1 times

dostonbekabdullaev 1 month, 1 week ago

Selected Answer: CE

C.E.

Secrets Manager is the most expensive amongst all options. S3 seems more cost-effective.

B. is incorrect, because at the end it states about accessing to the policy, not to the parameter itself.

upvoted 2 times

SerialiDr 1 month, 2 weeks ago

Selected Answer: BE

Also AE works, but BE is more cost effective.

upvoted 1 times

 **dostonbekabdullaev** 1 month, 1 week ago

Pay attention on this part "Add IAM users to allow access to the policy." It should give an access to the parameter, not to the policy.
upvoted 1 times

 **CalvinL4** 1 month, 3 weeks ago

CE should be the answer. The string size is over 4/8 kb which the parameter store allows. So, the parameter store is out. Comparing the price, s3 is much cheaper than secrets manager.
upvoted 2 times

 **rrshah83** 2 months ago

Selected Answer: AE

<https://aws.amazon.com/blogs/security/use-aws-secrets-manager-to-simplify-the-management-of-private-certificates/>
upvoted 1 times

 **rrshah83** 2 months ago

Selected Answer: AE

can you do resource based policies for param store?
upvoted 1 times

 **Hanny** 2 months, 3 weeks ago

Selected Answer: CE

<https://www.examtopics.com/discussions/amazon/view/96242-exam-aws-certified-developer-associate-topic-1-question-429/>
upvoted 1 times

 **tqi654** 3 months ago

Selected Answer: BD

CHatGPT: BD
upvoted 1 times

 **wonder_man** 4 months, 1 week ago

Selected Answer: CE

I can't see why using AWS Secrets Manager can be cost-effective, so I'm voting for C
upvoted 4 times

 **Rameez1** 4 months, 1 week ago

Selected Answer: BE

Using Parameter store is more cost effective then secrets manager.
upvoted 2 times

 **TallManDan** 4 months, 2 weeks ago

Secrets Manager is an additional cost over Parameter Store. So if you see a question that looks for the least amount of overhead, Secrets Manager is much more versatile. But for least amount of cost, Parameter Store is included with the service for no additional costs.
upvoted 2 times

 **PrakashM14** 4 months, 3 weeks ago

Selected Answer: BC

Why the remaining answers are not suitable:

A. Storing the Root CA Cert in AWS Secrets Manager is a valid option, but Secrets Manager is typically used for managing sensitive information like database credentials. It might be overkill for just a certificate, and using Systems Manager Parameter Store or S3 is a more straightforward solution in this case.

D. Refactoring the Lambda code to load the Root CA Cert from its location and modifying the runtime trust store inside the Lambda function handler would require code changes and rebuilding the Lambda functions, which contradicts the requirement of not updating all Lambda functions.

E. Refactoring the Lambda code to load the Root CA Cert from its location and modifying the runtime trust store outside the Lambda function handler may still require code changes and may not be as scalable or easily manageable as using Systems Manager Parameter Store or S3.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: BE

B. AWS Systems Manager Parameter Store can store data both in plain text and encrypted format (using the SecureString type). It's a cost-effective solution for centralized configuration management across environments and accounts.

E. Modifying the runtime trust store outside the Lambda function handler ensures that the trust store is modified only once when the Lambda container is initialized, making it a more efficient approach than option D where it's initialized in every lambda function.

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: AD

the correct answers are (A) and (D).

Solution (A) is the most cost-effective as it uses AWS Secrets Manager, which is a managed service. The developer can simply store the root CA certificate as a secret in Secrets Manager and create a resource-based policy to allow IAM users to access the secret. This does not require any

modifications to the Lambda code.

Solution (D) is also cost-effective as it does not require any modifications to the Lambda code. The developer can simply refactor the Lambda code to load the root CA certificate from the root CA certificate location. This can be done by modifying the runtime trust store outside of the Lambda function handler.

upvoted 2 times

Question #154

Topic 1

A developer maintains applications that store several secrets in AWS Secrets Manager. The applications use secrets that have changed over time. The developer needs to identify required secrets that are still in use. The developer does not want to cause any application downtime.

What should the developer do to meet these requirements?

- A. Configure an AWS CloudTrail log file delivery to an Amazon S3 bucket. Create an Amazon CloudWatch alarm for the GetSecretValue Secrets Manager API operation requests.
- B. Create a secretsmanager-secret-unused AWS Config managed rule. Create an Amazon EventBridge rule to initiate notifications when the AWS Config managed rule is met.
- C. Deactivate the applications secrets and monitor the applications error logs temporarily.
- D. Configure AWS X-Ray for the applications. Create a sampling rule to match the GetSecretValue Secrets Manager API operation requests.

Correct Answer: A

Community vote distribution



✉️ **chris_777** Highly Voted 3 months, 4 weeks ago

Selected Answer: B

I think B is correct <https://docs.aws.amazon.com/config/latest/developerguide/secretsmanager-secret-unused.html>

- A. could work but requires additional work to identify unused secrets.
- C. is too risky and could cause downtime.
- D. not the right use case

upvoted 5 times

✉️ **KarBiswa** Most Recent 6 days, 14 hours ago

Selected Answer: B

We need "secrets that are still in use". "B" secretsmanager-secret-unused returns unused. So we can easily determine the used secrets if it is not falling under this scanner

upvoted 1 times

✉️ **rimaSamir** 1 month ago

My choice is "A".
We need "secrets that are still in use". "B" secretsmanager-secret-unused returns unused.

upvoted 1 times

✉️ **SerialiDr** 1 month, 1 week ago

Selected Answer: A

A. Use an AWS Step Functions state machine to monitor API failures. Use the Wait state to delay calling the Lambda function: This is a viable and efficient solution. AWS Step Functions can orchestrate the Lambda function invocations and manage the workflow, including handling API call rate limits. The Wait state can be used to introduce delays between API calls to ensure compliance with the rate limits. This approach also allows for handling errors and retries effectively.

B. Use an Amazon Simple Queue Service (Amazon SQS) queue to hold the API calls. Configure the Lambda function to poll the queue within the API threshold limits: While using SQS to queue API call requests is a good way to manage workload, it adds complexity to the solution. The Lambda function would need to be modified to manage the queue and ensure API calls are made within the threshold limits. This approach might not be as straightforward and efficient as using Step Functions.

upvoted 1 times

✉️ **tqiu654** 3 months ago

Selected Answer: A

ChatGPT:A

upvoted 1 times

✉️ **kaes** 3 months, 1 week ago

It's easier to use a built-in solution in AWS Config (check chris_777 answer)

upvoted 1 times

✉️ **kaes** 3 months, 1 week ago

Selected Answer: B

It's easier to use a default built-in solution in AWS Config (check chris_777 answer)

upvoted 1 times

✉ **CrescentShared** 3 months, 2 weeks ago

Selected Answer: A

I think A is a more direct way, while B needs an inference after receiving the notification for 'unused'.
upvoted 1 times

✉ **LemonGremlin** 4 months, 2 weeks ago

Selected Answer: B

B is correct for this one.
upvoted 1 times

✉ **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A is correct. AWS CloudTrail can track API calls, including the GetSecretValue call for AWS Secrets Manager. By setting up CloudTrail log delivery to an S3 bucket, the developer can analyze which secrets are being accessed. Using CloudWatch to create an alarm for the GetSecretValue API call provides insight into which secrets are actively being retrieved, thus indicating which secrets are in use.
upvoted 2 times

✉ **dilleman** 4 months, 3 weeks ago

I think i change my mind to B. B Must be correct..
upvoted 3 times

✉ **CrescentShared** 3 months, 2 weeks ago

Why did you change your mind, please? A looks super correct to me.
upvoted 1 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Solution (B) is the best option to meet the developer's requirements. It allows the developer to identify necessary secrets that are still in use without causing any application downtime.
upvoted 3 times

Question #155

Topic 1

A developer is writing a serverless application that requires an AWS Lambda function to be invoked every 10 minutes.

What is an automated and serverless way to invoke the function?

- A. Deploy an Amazon EC2 instance based on Linux, and edit its /etc/crontab file by adding a command to periodically invoke the Lambda function.
- B. Configure an environment variable named PERIOD for the Lambda function. Set the value to 600.
- C. Create an Amazon EventBridge rule that runs on a regular schedule to invoke the Lambda function.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic that has a subscription to the Lambda function with a 600-second timer.

Correct Answer: C

Community vote distribution

C (100%)

 **SerialiDr** 1 month, 2 weeks ago

Selected Answer: C

C. Create an Amazon EventBridge rule that runs on a regular schedule to invoke the Lambda function: This is the correct and most suitable option. Amazon EventBridge (formerly CloudWatch Events) allows you to set up rules that trigger on a schedule. You can create a rule with a cron or rate expression to invoke the Lambda function every 10 minutes. This approach is fully serverless and does not require managing any servers or additional infrastructure.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct.

Amazon EventBridge can be used to run Lambda functions on a regular schedule. You can set a cron or rate expression to define the schedule.

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Solution (C) is the best option to meet the developer's requirements. It allows the developer to invoke the Lambda function in an automated and serverless way.

upvoted 2 times

Question #156

Topic 1

A company is using Amazon OpenSearch Service to implement an audit monitoring system. A developer needs to create an AWS CloudFormation custom resource that is associated with an AWS Lambda function to configure the OpenSearch Service domain. The Lambda function must access the OpenSearch Service domain by using OpenSearch Service internal master user credentials.

What is the MOST secure way to pass these credentials to the Lambda function?

- A. Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and the Lambda function's environment variable. Set the NoEcho attribute to true.
- B. Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and to create a parameter in AWS Systems Manager Parameter Store. Set the NoEcho attribute to true. Create an IAM role that has the ssm:GetParameter permission. Assign the role to the Lambda function. Store the parameter name as the Lambda function's environment variable. Resolve the parameter's value at runtime.
- C. Use a CloudFormation parameter to pass the master user credentials at deployment to the OpenSearch Service domain's MasterUserOptions and the Lambda function's environment variable. Encrypt the parameter's value by using the AWS Key Management Service (AWS KMS) encrypt command.
- D. Use CloudFormation to create an AWS Secrets Manager secret. Use a CloudFormation dynamic reference to retrieve the secret's value for the OpenSearch Service domain's MasterUserOptions. Create an IAM role that has the secretsmanager:GetSecretValue permission. Assign the role to the Lambda function. Store the secret's name as the Lambda function's environment variable. Resolve the secret's value at runtime.

Correct Answer: D

Community vote distribution



D (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: D

This approach is the most secure and aligns with best practices for managing secrets. The credentials are stored in AWS Secrets Manager, which is specifically designed for managing and protecting secrets. The credentials are retrieved dynamically at runtime by the Lambda function, and the use of IAM roles ensures that only the Lambda function has access to these secrets. This method also benefits from the security and rotation features of AWS Secrets Manager.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

Solution (D) is the most secure way to pass the credentials to the Lambda function because it uses AWS Secrets Manager to store the credentials in encrypted form.

upvoted 3 times

Question #157

Topic 1

An application runs on multiple EC2 instances behind an ELB.

Where is the session data best written so that it can be served reliably across multiple requests?

- A. Write data to Amazon ElastiCache.
- B. Write data to Amazon Elastic Block Store.
- C. Write data to Amazon EC2 Instance Store.
- D. Write data to the root filesystem.

Correct Answer: A

Community vote distribution

A (100%)

SerialiDr 1 month, 1 week ago

Selected Answer: A

Amazon ElastiCache provides a fast, in-memory data store or cache. It is often used for session management in distributed applications. Data stored in ElastiCache can be accessed quickly and reliably by any of the EC2 instances behind the ELB, making it an ideal choice for session data that needs to be shared across multiple servers.

upvoted 1 times

dileman 4 months, 3 weeks ago

Selected Answer: A

A is correct.

By storing session data in ElastiCache, you ensure that regardless of which EC2 instance handles a given request, the session data can be consistently and rapidly accessed.

upvoted 3 times

Digo30sp 4 months, 4 weeks ago

Selected Answer: A

The correct answer is (A).

Amazon ElastiCache is a distributed memory caching solution that is ideal for session data. ElastiCache provides high-performance and durable session data storage that can be shared across multiple EC2 instances.

upvoted 3 times

Question #158

Topic 1

An ecommerce application is running behind an Application Load Balancer. A developer observes some unexpected load on the application during non-peak hours. The developer wants to analyze patterns for the client IP addresses that use the application.

Which HTTP header should the developer use for this analysis?

- A. The X-Forwarded-Proto header
- B. The X-Forwarded-Host header
- C. The X-Forwarded-For header
- D. The X-Forwarded-Port header

Correct Answer: A

Community vote distribution

C (100%)

✉  **chris_777** 3 months, 4 weeks ago

Selected Answer: C

C is correct.

X-Forwarded-Proto: protocol (HTTP/HTTPS)
X-Forwarded-Host: original Host header requested by the client
X-Forwarded-For: original IP address of a client (CORRECT)
X-Forwarded-Port header: original port that the client used to connect
upvoted 4 times

✉  **tapan666** 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

✉  **Cerakoted** 4 months, 3 weeks ago

Selected Answer: C

X-Forwarded-For HTTP header contains the IP address of the original client

upvoted 1 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

The X-Forwarded-For HTTP header contains the IP address of the original client that made the request. The developer can use this header to analyze patterns for the IP addresses of clients using the application.

upvoted 2 times

Question #159

Topic 1

A developer migrated a legacy application to an AWS Lambda function. The function uses a third-party service to pull data with a series of API calls at the end of each month. The function then processes the data to generate the monthly reports. The function has been working with no issues so far.

The third-party service recently issued a restriction to allow a fixed number of API calls each minute and each day. If the API calls exceed the limit for each minute or each day, then the service will produce errors. The API also provides the minute limit and daily limit in the response header. This restriction might extend the overall process to multiple days because the process is consuming more API calls than the available limit.

What is the MOST operationally efficient way to refactor the serverless application to accommodate this change?

- A. Use an AWS Step Functions state machine to monitor API failures. Use the Wait state to delay calling the Lambda function.
- B. Use an Amazon Simple Queue Service (Amazon SQS) queue to hold the API calls. Configure the Lambda function to poll the queue within the API threshold limits.
- C. Use an Amazon CloudWatch Logs metric to count the number of API calls. Configure an Amazon CloudWatch alarm that stops the currently running instance of the Lambda function when the metric exceeds the API threshold limits.
- D. Use Amazon Kinesis Data Firehose to batch the API calls and deliver them to an Amazon S3 bucket with an event notification to invoke the Lambda function.

Correct Answer: B*Community vote distribution*

KarBiswa 6 days, 13 hours ago

Selected Answer: C

I would go for option C because response value always contains the limit value and which can be retrieved into the cloudwatch and can be used to block the lambda calls

upvoted 1 times

KillThemWithKindness 1 week, 1 day ago

Selected Answer: A

The solution that will meet the requirements is to use an AWS Step Functions state machine to monitor API failures. Use the Wait state to delay calling the Lambda function. This way, the developer can refactor the serverless application to accommodate the change in a way that is automated and scalable. The developer can use Step Functions to orchestrate the Lambda function and handle any errors or retries. The developer can also use the Wait state to pause the execution for a specified duration or until a specified timestamp, which can help avoid exceeding the API limits. The other options either involve using additional services that are not necessary or appropriate for this scenario, or do not address the issue of API failures.

<https://www.freecram.net/question/Amazon.DVA-C02.v2023-11-29.q68/a-developer-migrated-a-legacy-application-to-an-aws-lambda-function-the-function-uses-a-third-party-18#>

upvoted 1 times

konieczny69 4 weeks, 1 day ago

Selected Answer: A

Who is going to orchestrate lambda invocation?
SQS is for decoupling, not for scheduled invocations.

A is the only option.

upvoted 1 times

CrescentShared 1 month ago

Selected Answer: B

Option A with AWS Step Functions can handle the frequency of API calls by introducing a delay (Wait state) between retries after a failure due to rate limiting, it doesn't inherently solve the problem of the total number of calls per day. If the total number of necessary API calls exceeds the daily limit set by the third-party service, simply adding a delay between retries will not prevent the overall daily limit from being exceeded.

upvoted 1 times

SerialiDr 1 month, 1 week ago

Selected Answer: A

A. Use an AWS Step Functions state machine to monitor API failures. Use the Wait state to delay calling the Lambda function: This is a viable and efficient solution. AWS Step Functions can orchestrate the Lambda function invocations and manage the workflow, including handling API call rate limits. The Wait state can be used to introduce delays between API calls to ensure compliance with the rate limits. This approach also allows for handling errors and retries effectively.

B. Use an Amazon Simple Queue Service (Amazon SQS) queue to hold the API calls. Configure the Lambda function to poll the queue within the API threshold limits: While using SQS to queue API call requests is a good way to manage workload, it adds complexity to the solution. The Lambda function would need to be modified to manage the queue and ensure API calls are made within the threshold limits. This approach might not be as straightforward and efficient as using Step Functions.

upvoted 1 times

 **JohnPI** 1 month, 3 weeks ago

Selected Answer: B
B is the most operationally efficient way
upvoted 1 times

 **Snapie** 1 month, 3 weeks ago

Selected Answer: B
b is the answer
upvoted 1 times

 **rrshah83** 2 months ago

Selected Answer: B
sqS decouples lambda from api service
upvoted 1 times

 **chewasa** 2 months, 1 week ago

Selected Answer: B
While Step Functions can be used for workflow orchestration, it may not be the most straightforward solution for handling rate limits in this scenario.
upvoted 1 times

 **tqiu654** 3 months ago

Selected Answer: A
ChatGPT: A
upvoted 2 times

 **ShawnWon** 3 months, 2 weeks ago

B.
Option A (AWS Step Functions) might introduce unnecessary complexity and does not directly address the need to control the rate of API calls within the specified limits.
Option C (CloudWatch Logs metric and alarm) provides monitoring capabilities but doesn't offer a direct mechanism to control the rate of API calls within the Lambda function.

Option D (Kinesis Data Firehose) is designed for real-time streaming and might not be the most suitable option for this scenario, as it may not provide the fine-grained control needed to stay within the API call limits.

upvoted 3 times

 **wonder_man** 4 months, 1 week ago

Selected Answer: A
B: I don't see how the Lambda function can be configured this way
upvoted 4 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: A
A is Correct. AWS Step Functions can be used to create a workflow to handle the API calls. You can make the Lambda function inspect the response headers from the third-party service to determine the current API call limits and then pass that to the Wait state of the state machine for proper delays.
upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B
The correct answer is (B).

Solution (B) is the most operationally efficient way to refactor the serverless application to accommodate this change. This solution allows the Lambda function to continue executing API calls even if the API call limit is reached. The Amazon SQS queue will act as a buffer for API calls that exceed the limit. The Lambda function can then poll the queue within the API limits.

upvoted 4 times

Question #160

Topic 1

A developer must analyze performance issues with production-distributed applications written as AWS Lambda functions. These distributed Lambda applications invoke other components that make up the applications.

How should the developer identify and troubleshoot the root cause of the performance issues in production?

- A. Add logging statements to the Lambda functions, then use Amazon CloudWatch to view the logs.
- B. Use AWS CloudTrail and then examine the logs.
- C. Use AWS X-Ray, then examine the segments and errors.
- D. Run Amazon Inspector agents and then analyze performance.

Correct Answer: C

Community vote distribution

C (100%)

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct.

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

AWS X-Ray is the best tool for identifying and addressing the root cause of performance issues in distributed production applications. X-Ray provides an overview of the entire call stack, including the Lambda functions and other components they invoke.

upvoted 4 times

Question #161

Topic 1

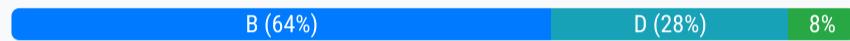
A developer wants to deploy a new version of an AWS Elastic Beanstalk application. During deployment, the application must maintain full capacity and avoid service interruption. Additionally, the developer must minimize the cost of additional resources that support the deployment.

Which deployment method should the developer use to meet these requirements?

- A. All at once
- B. Rolling with additional batch
- C. Blue/green
- D. Immutable

Correct Answer: B

Community vote distribution



✉ **Nagasoracle** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

B: Rolling with additional batch , considering "minimize the cost of additional resources"
C costly than B, due to double capacity

upvoted 11 times

✉ **KarBiswa** Most Recent 6 days, 13 hours ago

Selected Answer: B

<https://docs.aws.amazon.com/whitepapers/latest/practicing-continuous-integration-continuous-delivery/deployment-methods.html#:~:text=During%20the%20deployment%20process%20two%20software%20versions%2C%20new%20and%20old%2C%20are%20running%20on%20the%20same%20fleet.%20This%20method%20allows%20a%20zero%2Ddowntime%20update.%20If%20the%20deployment%20fails%2C%20only%20the%20updated%20portion%20of%20the%20fleet%20will%20be%20affected.>

It does not need a new instance

upvoted 1 times

✉ **SerialiDr** 1 month, 1 week ago

Selected Answer: D

D. Immutable

The immutable method strikes a balance between maintaining service availability and controlling costs. It avoids the downtime associated with the all-at-once method and doesn't require the more extensive resource duplication of the blue/green method. While it does temporarily increase resource usage (similar to rolling with an additional batch), it's generally more efficient and less risky than updating instances in-place.

upvoted 2 times

✉ **Roimasu** 4 months ago

Selected Answer: D

This method performs updates by launching a new set of instances in a new Auto Scaling group. Once the new instances pass health checks, they are moved into the existing Auto Scaling group, and the old instances are terminated. This method ensures full capacity, avoids downtime, and minimizes additional costs because it does not double the environment's running resources for an extended period. It adds resources temporarily and only in the amount necessary to maintain capacity.

upvoted 2 times

✉ **NinjaCloud** 4 months ago

Should be B "Ultimately, the choice between "Rolling with additional batch" and "Blue/green" deployments should depend on your specific requirements and constraints. If maintaining full capacity is a crucial factor, then "Rolling with additional batch" could be the better choice."

upvoted 4 times

✉ **ut18** 4 months, 1 week ago

MS Bing answer: B vs ChatGPT answer: C

Your choice?

upvoted 1 times

✉ **CrescentShared** 3 months, 2 weeks ago

ChatGPT4 changed its mind to select D today.

upvoted 1 times

✉ **Learning4life** 4 months, 2 weeks ago

C and D are wrong, since they both require additional resources.

upvoted 1 times

joosh96 4 months, 3 weeks ago

Selected Answer: C

chat gpt replied
upvoted 1 times

Cerakoted 4 months, 3 weeks ago

Selected Answer: B

Answer is B
One of requirement - the developer [must minimize the cost of additional resources] that support the deployment.
upvoted 4 times

dilleman 4 months, 3 weeks ago

Selected Answer: D

I vote for D since the requirement is to minimize the costs of resources. Blue/green is a good and safe way to solve this but it costs more resources than an Immutable rollout.
Immutable: Launches a new set of instances in a new temporary environment to ensure that the new version works as expected. Once the new version is verified, traffic is rerouted to the new set of instances, and the old instances are terminated. This method maintains full capacity, avoids service interruptions, and minimizes the cost compared to blue/green deployments since the overlap in running resources is shorter.
upvoted 3 times

Digo30sp 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

The blue/green deployment method is the best option to meet the developer's requirements. Blue/green allows the developer to deploy a new version of the application without service interruption. This is done by creating a blue production environment and a green production environment. The blue environment is the current production environment and the green environment is the new version of the application. The developer can then test the new version of the application in the green environment before putting it into production.

upvoted 1 times

Question #162

Topic 1

A developer has observed an increase in bugs in the AWS Lambda functions that a development team has deployed in its Node.js application. To minimize these bugs, the developer wants to implement automated testing of Lambda functions in an environment that closely simulates the Lambda environment.

The developer needs to give other developers the ability to run the tests locally. The developer also needs to integrate the tests into the team's continuous integration and continuous delivery (CI/CD) pipeline before the AWS Cloud Development Kit (AWS CDK) deployment.

Which solution will meet these requirements?

- A. Create sample events based on the Lambda documentation. Create automated test scripts that use the cdk local invoke command to invoke the Lambda functions. Check the response. Document the test scripts for the other developers on the team. Update the CI/CD pipeline to run the test scripts.
- B. Install a unit testing framework that reproduces the Lambda execution environment. Create sample events based on the Lambda documentation. Invoke the handler function by using a unit testing framework. Check the response. Document how to run the unit testing framework for the other developers on the team. Update the CI/CD pipeline to run the unit testing framework.
- C. Install the AWS Serverless Application Model (AWS SAM) CLI tool. Use the sam local generate-event command to generate sample events for the automated tests. Create automated test scripts that use the sam local invoke command to invoke the Lambda functions. Check the response. Document the test scripts for the other developers on the team. Update the CI/CD pipeline to run the test scripts.
- D. Create sample events based on the Lambda documentation. Create a Docker container from the Node.js base image to invoke the Lambda functions. Check the response. Document how to run the Docker container for the other developers on the team. Update the CI/CD pipeline to run the Docker container.

Correct Answer: B

Community vote distribution



C (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

This is the most suitable option. AWS SAM CLI is a tool designed for building, testing, and debugging serverless applications, and it includes the ability to locally test Lambda functions. The sam local invoke command allows you to invoke Lambda functions locally in a Docker container that simulates the Lambda execution environment. The sam local generate-event command can be used to generate sample events. This approach allows developers to run tests locally and can be integrated into CI/CD pipelines.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C should be correct

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Solution (C) is the best option to meet the developer's requirements. The AWS SAM CLI tool provides an easy way to generate sample events and invoke Lambda functions locally. The solution is also easy to document and integrate into the CI/CD pipeline.

upvoted 4 times

Question #163

Topic 1

A developer is troubleshooting an application that uses Amazon DynamoDB in the us-west-2 Region. The application is deployed to an Amazon EC2 instance. The application requires read-only permissions to a table that is named Cars. The EC2 instance has an attached IAM role that contains the following IAM policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAPIActions",
            "Effect": "Allow",
            "Action": [
                "dynamodb:GetItem",
                "dynamodb:BatchGetItem",
                "dynamodb:Scan",
                "dynamodb:Query",
                "dynamodb:ConditionCheckItem"
            ],
            "Resource": "arn:aws:dynamodb:us-west-2:account-id:table/Cars"
        }
    ]
}
```

When the application tries to read from the Cars table, an Access Denied error occurs.

How can the developer resolve this error?

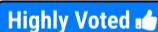
- A. Modify the IAM policy resource to be "arn:aws:dynamodb:us-west-2:account-id:table/*".
- B. Modify the IAM policy to include the dynamodb:* action.
- C. Create a trust policy that specifies the EC2 service principal. Associate the role with the policy.
- D. Create a trust relationship between the role and dynamodb.amazonaws.com.

Correct Answer: D

Community vote distribution

C (89%)

11%

✉️  LemonGremlin  4 months, 2 weeks ago

Selected Answer: C

The most reasonable answer here is C. But I think the question is missing some information.
<https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/>

upvoted 5 times

✉️  konieczny69 4 weeks, 1 day ago

What is a trust policy?

I know trust relationship, not a trust policy.

upvoted 1 times

✉️  PrakashM14  4 months, 2 weeks ago

Selected Answer: D

D.Create a trust relationship between the role and dynamodb.amazonaws.com.

Explanation:

Trust Relationship: In AWS, a trust relationship defines who or what entity can assume a role. In this case, the role attached to the EC2 instance needs to trust DynamoDB. The trust relationship is specified in a JSON policy document.

DynamoDB Service Principal: The correct service principal for DynamoDB is dynamodb.amazonaws.com. This is the entity that the role needs to trust to allow access to DynamoDB resources.

upvoted 1 times

✉️  konieczny69 4 weeks, 1 day ago

Complete nonsense. Role needs to trust EC2, since its the EC2 who is to assume the role.

upvoted 1 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/96497-exam-aws-certified-developer-associate-topic-1-question-380/>

upvoted 3 times

Question #164

Topic 1

When using the AWS Encryption SDK, how does the developer keep track of the data encryption keys used to encrypt data?

- A. The developer must manually keep track of the data encryption keys used for each data object.
- B. The SDK encrypts the data encryption key and stores it (encrypted) as part of the returned ciphertext.
- C. The SDK stores the data encryption keys automatically in Amazon S3.
- D. The data encryption key is stored in the Userdata for the EC2 instance.

Correct Answer: C

Community vote distribution

B (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: B

In the AWS Encryption SDK, data is encrypted using a DEK. This DEK is then encrypted with a Key Encryption Key (KEK), usually managed by AWS Key Management Service (AWS KMS) or another key management infrastructure. The encrypted DEK is stored alongside the encrypted data (ciphertext). This allows the SDK to manage the DEKs seamlessly.

upvoted 2 times

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: B

When using the AWS Encryption SDK, it is a common practice to encrypt the data encryption key (DEK) along with the data. The DEK is used to encrypt the actual data, and it is itself encrypted using a key management system, often called a key encryption key (KEK). This encrypted DEK is then stored alongside the encrypted data.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/96427-exam-aws-certified-developer-associate-topic-1-question-398/>

upvoted 3 times

Question #165

Topic 1

An application that runs on AWS Lambda requires access to specific highly confidential objects in an Amazon S3 bucket. In accordance with the principle of least privilege, a company grants access to the S3 bucket by using only temporary credentials.

How can a developer configure access to the S3 bucket in the MOST secure way?

- A. Hardcode the credentials that are required to access the S3 objects in the application code. Use the credentials to access the required S3 objects.
- B. Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID in AWS Secrets Manager. Configure the application to retrieve the Secrets Manager secret and use the credentials to access the S3 objects.
- C. Create a Lambda function execution role. Attach a policy to the role that grants access to specific objects in the S3 bucket.
- D. Create a secret access key and access key ID with permission to access the S3 bucket. Store the key and key ID as environment variables in Lambda. Use the environment variables to access the required S3 objects.

Correct Answer: D

Community vote distribution



✉ **dilleman** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

C should be correct:

<https://docs.aws.amazon.com/lambda/latest/operatorguide/least-privilege.html>

upvoted 10 times

✉ **SerialiDr** Most Recent 1 month, 1 week ago

Selected Answer: C

This is the most secure and recommended approach. By attaching an IAM policy to the Lambda execution role that grants access only to the specific S3 objects needed, you adhere to the principle of least privilege. This method also uses AWS's built-in mechanism for providing temporary credentials to the Lambda function, eliminating the need to manage access keys.

upvoted 2 times

✉ **LemonGremlin** 4 months, 2 weeks ago

Selected Answer: C

C. Create a Lambda function execution role. Attach a policy to the role that grants access to specific objects in the S3 bucket.

upvoted 4 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Option (B) is the most secure way to configure S3 bucket access because the credentials are stored in a safe and secure location. AWS Secrets Manager uses public key cryptography to protect stored secrets.

upvoted 4 times

✉ **dezoito** 4 months, 2 weeks ago

B goes against the least privilege principle because it gives access to the whole bucket

upvoted 5 times

Question #166

Topic 1

A developer has code that is stored in an Amazon S3 bucket. The code must be deployed as an AWS Lambda function across multiple accounts in the same AWS Region as the S3 bucket. An AWS CloudFormation template that runs for each account will deploy the Lambda function.

What is the MOST secure way to allow CloudFormation to access the Lambda code in the S3 bucket?

- A. Grant the CloudFormation service role the S3 ListBucket and GetObject permissions. Add a bucket policy to Amazon S3 with the principal of "AWS": [account numbers].
- B. Grant the CloudFormation service role the S3 GetObject permission. Add a bucket policy to Amazon S3 with the principal of "*".
- C. Use a service-based link to grant the Lambda function the S3 ListBucket and GetObject permissions by explicitly adding the S3 bucket's account number in the resource.
- D. Use a service-based link to grant the Lambda function the S3 GetObject permission. Add a resource of "*" to allow access to the S3 bucket.

Correct Answer: A

Community vote distribution



A (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

This approach is secure and provides a granular level of control. By granting the CloudFormation service role in each account the necessary S3 permissions and specifying the account numbers in the S3 bucket policy, you ensure that only the specified accounts can access the Lambda code. However, the ListBucket permission is not necessary if the CloudFormation template already knows the exact S3 object key.

upvoted 3 times

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: A

Following ChatGPT 3.5, Option A is the best choice. I guess.

- Follows the principle of least privilege by granting only the necessary permissions (ListBucket and GetObject) to the CloudFormation service role.
- Adding a bucket policy with the principal of "AWS": [account numbers] restricts access to only the specified AWS accounts, providing a more secure access control mechanism.
- This ensures that only the CloudFormation service role in the specified AWS accounts can access the Lambda code in the S3 bucket.

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

The correct answer is (A).

Option (A) is the safest way to allow CloudFormation to access the Lambda code in the S3 bucket because it limits access to the specific accounts that need to deploy the Lambda functions. The bucket policy grants S3 ListBucket and GetObject permissions to the CloudFormation service role only for the accounts specified in the principal.

upvoted 4 times

Question #167

Topic 1

A developer at a company needs to create a small application that makes the same API call once each day at a designated time. The company does not have infrastructure in the AWS Cloud yet, but the company wants to implement this functionality on AWS.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. Use a Kubernetes cron job that runs on Amazon Elastic Kubernetes Service (Amazon EKS).
- B. Use an Amazon Linux crontab scheduled job that runs on Amazon EC2.
- C. Use an AWS Lambda function that is invoked by an Amazon EventBridge scheduled event.
- D. Use an AWS Batch job that is submitted to an AWS Batch job queue.

Correct Answer: C

Community vote distribution

C (100%)

 **joshnort** 4 weeks, 1 day ago

Selected Answer: C

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-create-rule-schedule.html>
upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct
upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/88703-exam-aws-certified-developer-associate-topic-1-question-229/>
upvoted 2 times

Question #168

Topic 1

A developer is building a serverless application that is based on AWS Lambda. The developer initializes the AWS software development kit (SDK) outside of the Lambda handler function.

What is the PRIMARY benefit of this action?

- A. Improves legibility and stylistic convention
- B. Takes advantage of runtime environment reuse
- C. Provides better error handling
- D. Creates a new SDK instance for each invocation

Correct Answer: B

Community vote distribution

 B (100%)

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B it is!

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Initializing the AWS SDK outside of the Lambda handler function takes advantage of runtime environment reuse. This means that the SDK only needs to be initialized once for all Lambda function invocations. This can improve application performance and efficiency.

upvoted 3 times

Question #169

Topic 1

A company is using Amazon RDS as the backend database for its application. After a recent marketing campaign, a surge of read requests to the database increased the latency of data retrieval from the database. The company has decided to implement a caching layer in front of the database. The cached content must be encrypted and must be highly available.

Which solution will meet these requirements?

- A. Amazon CloudFront
- B. Amazon ElastiCache for Memcached
- C. Amazon ElastiCache for Redis in cluster mode
- D. Amazon DynamoDB Accelerator (DAX)

Correct Answer: C

Community vote distribution

C (100%)

✉ **dilleman** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

Should be C since ElastiCache for Redis supports encryption at rest and in transit. ElastiCache for Memcached does not support encryption at rest. DynamoDB Accelerator is for DynamoDB and does not fit this case.

upvoted 5 times

✉ **SerialiDr** Most Recent 1 month, 1 week ago

Selected Answer: C

ElastiCache for Redis provides both encryption in transit and at rest. In cluster mode, it also offers high availability and scalability. This makes it well-suited for caching database queries while ensuring data security and high availability.

upvoted 2 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/82917-exam-aws-certified-developer-associate-topic-1-question-95/>

upvoted 2 times

Question #170

Topic 1

A developer at a company recently created a serverless application to process and show data from business reports. The application's user interface (UI) allows users to select and start processing the files. The UI displays a message when the result is available to view. The application uses AWS Step Functions with AWS Lambda functions to process the files. The developer used Amazon API Gateway and Lambda functions to create an API to support the UI.

The company's UI team reports that the request to process a file is often returning timeout errors because of the size or complexity of the files. The UI team wants the API to provide an immediate response so that the UI can display a message while the files are being processed. The backend process that is invoked by the API needs to send an email message when the report processing is complete.

What should the developer do to configure the API to meet these requirements?

- A. Change the API Gateway route to add an X-Amz-Invocation-Type header with a static value of 'Event' in the integration request. Deploy the API Gateway stage to apply the changes.
- B. Change the configuration of the Lambda function that implements the request to process a file. Configure the maximum age of the event so that the Lambda function will run asynchronously.
- C. Change the API Gateway timeout value to match the Lambda function timeout value. Deploy the API Gateway stage to apply the changes.
- D. Change the API Gateway route to add an X-Amz-Target header with a static value of 'Async' in the integration request. Deploy the API Gateway stage to apply the changes.

Correct Answer: A

Community vote distribution



SerialiDr 1 month, 1 week ago

Selected Answer: A

Change the API Gateway route to add an X-Amz-Invocation-Type header with a static value of 'Event' in the integration request: This is the correct approach. By setting the X-Amz-Invocation-Type header to Event in the API Gateway integration request, the API Gateway will invoke the Lambda function asynchronously. In asynchronous execution, the Lambda function returns an immediate response (202 or Accepted status) to API Gateway, which can then relay it back to the UI. Meanwhile, the Lambda function processes the file in the background.

upvoted 2 times

JLLNOR 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-lambda-integration-async.html>

upvoted 3 times

Certified101 2 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/82655-exam-aws-certified-developer-associate-topic-1-question-85/>

upvoted 3 times

TanTran04 2 months, 3 weeks ago

Selected Answer: D

Option A is incorrect because the X-Amz-Invocation-Type header with a static value of 'Event' is used for the AWS Lambda asynchronous invocation, but it doesn't address the issue of providing an immediate response to the UI.

Option D is the correct choice. By adding an X-Amz-Target header with a static value of 'Async' in the integration request, the API Gateway will immediately return a response to the UI, allowing it to display a message while the backend processing continues asynchronously. This ensures that the UI team does not encounter timeout errors due to long-running processes.

upvoted 1 times

TanTran04 2 months, 1 week ago

I miss something, Option D is undocumented.

=> A is the best choice

upvoted 2 times

LemonGremlin 4 months, 2 weeks ago

Selected Answer: A

Reference: <https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-lambda-integration-async.html>

upvoted 2 times

Question #172

Topic 1

A mobile app stores blog posts in an Amazon DynamoDB table. Millions of posts are added every day, and each post represents a single item in the table. The mobile app requires only recent posts. Any post that is older than 48 hours can be removed.

What is the MOST cost-effective way to delete posts that are older than 48 hours?

- A. For each item, add a new attribute of type String that has a timestamp that is set to the blog post creation time. Create a script to find old posts with a table scan and remove posts that are older than 48 hours by using the BatchWriteItem API operation. Schedule a cron job on an Amazon EC2 instance once an hour to start the script.
- B. For each item, add a new attribute of type String that has a timestamp that is set to the blog post creation time. Create a script to find old posts with a table scan and remove posts that are older than 48 hours by using the BatchWriteItem API operation. Place the script in a container image. Schedule an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate that invokes the container every 5 minutes.
- C. For each item, add a new attribute of type Date that has a timestamp that is set to 48 hours after the blog post creation time. Create a global secondary index (GSI) that uses the new attribute as a sort key. Create an AWS Lambda function that references the GSI and removes expired items by using the BatchWriteItem API operation. Schedule the function with an Amazon CloudWatch event every minute.
- D. For each item, add a new attribute of type Number that has a timestamp that is set to 48 hours after the blog post creation time. Configure the DynamoDB table with a TTL that references the new attribute.

Correct Answer: B

Community vote distribution

D (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: D

This is the most cost-effective and efficient solution. The TTL feature allows DynamoDB to automatically delete items past a certain timestamp, which is perfect for this use case. By adding a TTL attribute to each item (set to 48 hours after the post creation time), DynamoDB will automatically delete the items when they expire, without any need for custom scripts, additional AWS services, or manual intervention.
upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D is correct. DynamoDB tables can clean up data itself based on provided configuration.
upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

Solution (D) is the most cost-effective because it uses DynamoDB's Time to Live (TTL) to automatically remove expired items. The TTL is an item attribute that specifies the duration of time that an item should remain in the table. When an item's TTL expires, the item is automatically deleted from the table.

upvoted 3 times

Question #173

Topic 1

A developer is modifying an existing AWS Lambda function. While checking the code, the developer notices hardcoded parameter values for an Amazon RDS for SQL Server user name, password, database, host, and port. There are also hardcoded parameter values for an Amazon DynamoDB table, an Amazon S3 bucket, and an Amazon Simple Notification Service (Amazon SNS) topic.

The developer wants to securely store the parameter values outside the code in an encrypted format and wants to turn on rotation for the credentials. The developer also wants to be able to reuse the parameter values from other applications and to update the parameter values without modifying code.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an RDS database secret in AWS Secrets Manager. Set the user name, password, database, host, and port. Turn on secret rotation. Create encrypted Lambda environment variables for the DynamoDB table, S3 bucket, and SNS topic.
- B. Create an RDS database secret in AWS Secrets Manager. Set the user name, password, database, host, and port. Turn on secret rotation. Create SecureString parameters in AWS Systems Manager Parameter Store for the DynamoDB table, S3 bucket, and SNS topic.
- C. Create RDS database parameters in AWS Systems Manager Parameter Store for the user name, password, database, host, and port. Create encrypted Lambda environment variables for the DynamoDB table, S3 bucket, and SNS topic. Create a Lambda function and set the logic for the credentials rotation task. Schedule the credentials rotation task in Amazon EventBridge.
- D. Create RDS database parameters in AWS Systems Manager Parameter Store for the user name, password, database, host, and port. Store the DynamoDB table, S3 bucket, and SNS topic in Amazon S3. Create a Lambda function and set the logic for the credentials rotation. Invoke the Lambda function on a schedule.

Correct Answer: B

Community vote distribution

B (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: B

AWS Secrets Manager is designed to handle sensitive information like database credentials and supports automatic rotation. Using SecureString parameters in Systems Manager Parameter Store for other parameters provides a secure and centralized way to manage them. This approach also enables reusability and easy updating without code modifications.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/88929-exam-aws-certified-developer-associate-topic-1-question-338/>
upvoted 3 times

Question #174

Topic 1

A developer accesses AWS CodeCommit over SSH. The SSH keys configured to access AWS CodeCommit are tied to a user with the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit>List*",
        "codecommit:GitPull"
      ],
      "Resource": "*"
    }
  ]
}
```

The developer needs to create/delete branches.

Which specific IAM permissions need to be added, based on the principle of least privilege?

- A. "codecommit>CreateBranch"
"codecommit>DeleteBranch"
- B. "codecommit:Put*"
- C. "codecommit:Update*"
- D. "codecommit:*"

Correct Answer: B

Community vote distribution

A (100%)

✉  **TanTran04** 2 months, 1 week ago

Selected Answer: A

Take a look at CodeCommit API Operations and Required Permissions for Actions on Branches in
<https://docs.aws.amazon.com/codecommit/latest/userguide/auth-and-access-control-permissions-reference.html#aa-branches> => A
 upvoted 1 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A of course
 upvoted 3 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

A) <https://www.examtopics.com/discussions/amazon/view/4364-exam-aws-certified-developer-associate-topic-1-question-190/>
 upvoted 2 times

Question #175

Topic 1

An application that is deployed to Amazon EC2 is using Amazon DynamoDB. The application calls the DynamoDB REST API. Periodically, the application receives a ProvisionedThroughputExceededException error when the application writes to a DynamoDB table.

Which solutions will mitigate this error MOST cost-effectively? (Choose two.)

- A. Modify the application code to perform exponential backoff when the error is received.
- B. Modify the application to use the AWS SDKs for DynamoDB.
- C. Increase the read and write throughput of the DynamoDB table.
- D. Create a DynamoDB Accelerator (DAX) cluster for the DynamoDB table.
- E. Create a second DynamoDB table. Distribute the reads and writes between the two tables.

Correct Answer: AB

Community vote distribution



✉️ **SerialiDr** 1 month, 1 week ago

Selected Answer: AB

A. Modify the application code to perform exponential backoff when the error is received: This is a cost-effective and recommended approach. Exponential backoff is a standard error-retry strategy where the time between retries gradually increases. This strategy helps to efficiently manage request retries without immediately consuming additional throughput, thus reducing the likelihood of repeatedly hitting the throughput limits.

B. Modify the application to use the AWS SDKs for DynamoDB: The AWS SDKs implement best practices, including automatic retry logic with exponential backoff. Using an AWS SDK for DynamoDB can simplify the implementation and is more efficient than directly calling the DynamoDB REST API. This change can help mitigate throughput exceedance errors.

upvoted 2 times

✉️ **TanTran04** 2 months, 3 weeks ago

Selected Answer: AC

Following ChatGPT 3.5, Option A and C

Option B (Modify the application to use the AWS SDKs for DynamoDB) is not directly related to resolving throughput issues. It's generally recommended to use the AWS SDKs as they provide more efficient and convenient ways to interact with AWS services, but it may not directly address the ProvisionedThroughputExceededException issue.

upvoted 1 times

✉️ **dilleman** 4 months, 3 weeks ago

Selected Answer: AB

A and B.

Exponential backoff is a standard error-handling strategy for network applications. The idea is to retry a failed request with increasing delays between each attempt.

And the AWS SDKs have built-in support for handling these errors.

upvoted 4 times

✉️ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: AB

A and B: <https://www.examtopics.com/discussions/amazon/view/69199-exam-aws-certified-developer-associate-topic-1-question-385/>

upvoted 4 times

Question #176

Topic 1

When a developer tries to run an AWS CodeBuild project, it raises an error because the length of all environment variables exceeds the limit for the combined maximum of characters.

What is the recommended solution?

- A. Add the export LC_ALL="en_US.utf8" command to the pre_build section to ensure POSIX localization.
- B. Use Amazon Cognito to store key-value pairs for large numbers of environment variables.
- C. Update the settings for the build project to use an Amazon S3 bucket for large numbers of environment variables.
- D. Use AWS Systems Manager Parameter Store to store large numbers of environment variables.

Correct Answer: D

Community vote distribution

D (100%)

SerialiDr 1 month, 1 week ago

Selected Answer: D

AWS Systems Manager Parameter Store is specifically designed for managing configuration data and secrets. It can store large numbers of parameters, including environment variables, and makes them easily accessible and manageable. It also provides features like versioning, fine-grained access control, and integration with AWS Identity and Access Management (IAM).

upvoted 2 times

dilleman 4 months, 3 weeks ago

Selected Answer: D

Best solution is D

upvoted 3 times

Digo30sp 4 months, 4 weeks ago

Selected Answer: D

D) <https://docs.aws.amazon.com/codebuild/latest/userguide/troubleshooting.html>

upvoted 3 times

Question #177

Topic 1

A company is expanding the compatibility of its photo-sharing mobile app to hundreds of additional devices with unique screen dimensions and resolutions. Photos are stored in Amazon S3 in their original format and resolution. The company uses an Amazon CloudFront distribution to serve the photos. The app includes the dimension and resolution of the display as GET parameters with every request.

A developer needs to implement a solution that optimizes the photos that are served to each device to reduce load time and increase photo quality.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Batch Operations to invoke an AWS Lambda function to create new variants of the photos with the required dimensions and resolutions. Create a dynamic CloudFront origin that automatically maps the request of each device to the corresponding photo variant.
- B. Use S3 Batch Operations to invoke an AWS Lambda function to create new variants of the photos with the required dimensions and resolutions. Create a Lambda@Edge function to route requests to the corresponding photo variant by using request headers.
- C. Create a Lambda@Edge function that optimizes the photos upon request and returns the photos as a response. Change the CloudFront TTL cache policy to the maximum value possible.
- D. Create a Lambda@Edge function that optimizes the photos upon request and returns the photos as a response. In the same function, store a copy of the processed photos on Amazon S3 for subsequent requests.

Correct Answer: D

Community vote distribution

D (100%)

 **joshnort** 4 weeks, 1 day ago

Selected Answer: D

<https://aws.amazon.com/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>
upvoted 1 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: D

This solution is the most cost-effective. Lambda@Edge processes the photos dynamically based on the device's requirements, which means no pre-generation of multiple variants is required. Processed photos are stored on S3, ensuring that subsequent requests for the same photo variant are served directly from S3, reducing Lambda@Edge invocations and further optimizing costs.
upvoted 2 times

 **Mimi666** 2 months, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/es/blogs/networking-and-content-delivery/image-optimization-using-amazon-cloudfront-and-aws-lambda/>
upvoted 2 times

 **jingle4944** 3 months, 3 weeks ago

According to <https://aws.amazon.com/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>, "static resources like images should have a long Time to Live (TTL) as possible to improve cache-hit ratios.". The photo cache here is likely to be static and should be preserved forever.
upvoted 1 times

 **ut18** 4 months ago

Why not B?

The developer can use S3 Batch Operations to create new variants of the photos with the required dimensions and resolutions.

upvoted 1 times

 **TallManDan** 4 months, 2 weeks ago

Selected Answer: D

You only want to convert the pictures that get requests. If you convert them all through batch processing, you have wasted time and expense on any possible photo that never gets viewed. The Minimum TTL is set to 60 seconds, the Default TTL is set to 300 seconds, and the Maximum TTL is set to 3600 seconds. S3 is the way to go.
upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/89564-exam-aws-certified-developer-associate-topic-1-question-320/>

upvoted 1 times

Question #178

Topic 1

A company is building an application for stock trading. The application needs sub-millisecond latency for processing trade requests. The company uses Amazon DynamoDB to store all the trading data that is used to process each trading request.

A development team performs load testing on the application and finds that the data retrieval time is higher than expected. The development team needs a solution that reduces the data retrieval time with the least possible effort.

Which solution meets these requirements?

- A. Add local secondary indexes (LSIs) for the trading data.
- B. Store the trading data in Amazon S3, and use S3 Transfer Acceleration.
- C. Add retries with exponential backoff for DynamoDB queries.
- D. Use DynamoDB Accelerator (DAX) to cache the trading data.**

Correct Answer: D

Community vote distribution

D (100%)

 **joshnort** 4 weeks, 1 day ago

Selected Answer: D

<https://aws.amazon.com/dynamodb/dax/>

upvoted 1 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: D

DAX is an in-memory cache for DynamoDB that delivers fast read performance for your tables at scale by enabling you to get sub-millisecond response times for accessing your data. DAX is particularly beneficial for read-heavy and bursty workloads. Since it reduces the time to retrieve data, it's the most appropriate solution for achieving sub-millisecond latency in data retrieval.

upvoted 2 times

 **JohnPI** 1 month, 2 weeks ago

Selected Answer: D

Use DynamoDB Accelerator (DAX)

upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/dynamodb/dax/>

DAX delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second. only pay for the capacity you provision.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

This is a perfect scenario for DAX so correct answer is D

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/4971-exam-aws-certified-developer-associate-topic-1-question-14/>

upvoted 3 times

Question #179

Topic 1

A developer is working on a Python application that runs on Amazon EC2 instances. The developer wants to enable tracing of application requests to debug performance issues in the code.

Which combination of actions should the developer take to achieve this goal? (Choose two.)

- A. Install the Amazon CloudWatch agent on the EC2 instances.
- B. Install the AWS X-Ray daemon on the EC2 instances.
- C. Configure the application to write JSON-formatted logs to /var/log/cloudwatch.
- D. Configure the application to write trace data to /var/log/xray.
- E. Install and configure the AWS X-Ray SDK for Python in the application.

Correct Answer: CE

Community vote distribution

BE (100%)

✉️  **Digo30sp**  4 months, 4 weeks ago

Selected Answer: BE

The correct answers are (E) and (B).

(E) is the most important action to enable application request tracking using AWS X-Ray. The AWS X-Ray SDK for Python provides a set of APIs that a developer can use to instrument their application code for tracing.

(B) is the second most important action. The AWS X-Ray daemon runs on each EC2 instance and collects application trace data upvoted 5 times

✉️  **SerialiDr**  1 month, 1 week ago

Selected Answer: BE

B. Install the AWS X-Ray daemon on the EC2 instances: This is a required step for enabling AWS X-Ray tracing. The X-Ray daemon listens for traffic on UDP port 2000, gathers raw segment data, and relays it to the AWS X-Ray API. This is necessary for collecting and sending trace data from the application to X-Ray.

E. Install and configure the AWS X-Ray SDK for Python in the application: This is a critical step for enabling X-Ray tracing in your Python application. The X-Ray SDK for Python provides classes and methods to collect data about the requests that your application serves, and sends this data to the X-Ray daemon.

upvoted 2 times

✉️  **NinjaCloud** 4 months ago

Answer: E,B

upvoted 3 times

✉️  **dilleman** 4 months, 3 weeks ago

Selected Answer: BE

B and E

upvoted 4 times

Question #180

Topic 1

A company has an application that runs as a series of AWS Lambda functions. Each Lambda function receives data from an Amazon Simple Notification Service (Amazon SNS) topic and writes the data to an Amazon Aurora DB instance.

To comply with an information security policy, the company must ensure that the Lambda functions all use a single securely encrypted database connection string to access Aurora.

Which solution will meet these requirements?

- A. Use IAM database authentication for Aurora to enable secure database connections for all the Lambda functions.
- B. Store the credentials and read the credentials from an encrypted Amazon RDS DB instance.
- C. Store the credentials in AWS Systems Manager Parameter Store as a secure string parameter.
- D. Use Lambda environment variables with a shared AWS Key Management Service (AWS KMS) key for encryption.

Correct Answer: D

Community vote distribution



✉ **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C.

AWS Systems Manager Parameter Store offers a more centralized way to manage encrypted secrets across multiple services than Lambda environment variables, making it a better fit for this scenario.

upvoted 9 times

✉ **ShawnWon** 3 months, 2 weeks ago

C.

Option A (IAM database authentication) may provide secure authentication, but it doesn't directly address the storage and retrieval of the connection string.

Option B (storing credentials in an encrypted RDS DB instance) might introduce unnecessary complexity and potential security risks.

Option D (Lambda environment variables with a shared AWS KMS key) is a viable option, but using Parameter Store is generally considered a more centralized and managed approach for storing and retrieving sensitive data in AWS.

Therefore, option C is the most appropriate choice for securely managing the database connection string in this scenario.

upvoted 5 times

✉ **KillThemWithKindness** 1 week, 1 day ago

Selected Answer: A

The developer can create an IAM role with permission to connect to Aurora DB instance and attach it to each Lambda function. The developer can also configure Aurora DB instance to use IAM database authentication and enable encryption in transit using SSL certificates.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

upvoted 1 times

✉ **rimaSamir** 1 month ago

The answer is A.

<https://aws.amazon.com/ru/blogs/database/iam-role-based-authentication-to-amazon-aurora-from-serverless-applications/>

upvoted 1 times

✉ **rimaSamir** 1 month ago

In Amazon Aurora, you can associate the database users with the IAM user and roles.

upvoted 1 times

✉ **SerialiDr** 1 month, 1 week ago

Selected Answer: C

C. Store the credentials in AWS Systems Manager Parameter Store as a secure string parameter: This is a strong option. Systems Manager Parameter Store provides secure, hierarchical storage for configuration data and secrets. It can store data such as passwords and database connection strings securely, and it integrates with AWS Key Management Service (AWS KMS) for encryption. Lambda functions can then retrieve the connection string securely at runtime.

D. Use Lambda environment variables with a shared AWS Key Management Service (AWS KMS) key for encryption: While Lambda environment variables can be encrypted with AWS KMS and used to store sensitive information like database connection strings, they are not as centrally manageable as Parameter Store. Each Lambda function's environment variables would need to be updated individually if the connection string changes, which is less efficient and more prone to error.

upvoted 2 times

 **TallManDan** 4 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/iam-role-based-authentication-to-amazon-aurora-from-serverless-applications/>

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

Solution (D) is the best option because it uses Lambda environment variables with an AWS Key Management Service (AWS KMS) shared key for encryption.

upvoted 3 times

Question #181

Topic 1

A developer is troubleshooting an Amazon API Gateway API. Clients are receiving HTTP 400 response errors when the clients try to access an endpoint of the API.

How can the developer determine the cause of these errors?

- A. Create an Amazon Kinesis Data Firehose delivery stream to receive API call logs from API Gateway. Configure Amazon CloudWatch Logs as the delivery stream's destination.
- B. Turn on AWS CloudTrail Insights and create a trail. Specify the Amazon Resource Name (ARN) of the trail for the stage of the API.
- C. Turn on AWS X-Ray for the API stage. Create an Amazon CloudWatch Logs log group. Specify the Amazon Resource Name (ARN) of the log group for the API stage.
- D. Turn on execution logging and access logging in Amazon CloudWatch Logs for the API stage. Create a CloudWatch Logs log group. Specify the Amazon Resource Name (ARN) of the log group for the API stage.

Correct Answer: A

Community vote distribution



✉ KarBiswa 20 hours, 7 minutes ago

Selected Answer: C

Always the rule of thumb is Cloud Trail to trace the logging events of API's.

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html#:~:text=AWS%20CloudTrail%20Insights,write%20management%20APIs>.

upvoted 1 times

✉ walala97 1 month, 4 weeks ago

Selected Answer: D

why not C,X-Ray is more focused on the internal workings and performance of the API rather than the validity or structure of incoming requests.according to the error 400,it should be the client side error like incorrect request syntax, invalid request message framing, or deceptive request routing

upvoted 2 times

✉ dezoito 4 months, 2 weeks ago

D according to <https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-logging.html>

upvoted 2 times

✉ dileman 4 months, 3 weeks ago

Selected Answer: D

D should be correct

upvoted 2 times

✉ Digo30sp 4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/88807-exam-aws-certified-developer-associate-topic-1-question-264/>

upvoted 2 times

Question #182

Topic 1

A company developed an API application on AWS by using Amazon CloudFront, Amazon API Gateway, and AWS Lambda. The API has a minimum of four requests every second. A developer notices that many API users run the same query by using the POST method. The developer wants to cache the POST request to optimize the API resources.

Which solution will meet these requirements?

- A. Configure the CloudFront cache. Update the application to return cached content based upon the default request headers.
- B. Override the cache method in the selected stage of API Gateway. Select the POST method.
- C. Save the latest request response in Lambda /tmp directory. Update the Lambda function to check the /tmp directory.
- D. Save the latest request in AWS Systems Manager Parameter Store. Modify the Lambda function to take the latest request response from Parameter Store.

Correct Answer: B

Community vote distribution



□ **KarBiswa** 20 hours, 1 minute ago

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html#:~:text=When%20you%20enable,caching%20is%20disabled.>

upvoted 1 times

□ **SerialiDr** 1 month, 1 week ago

Selected Answer: B

API Gateway allows caching of responses, and you can enable caching for specific methods, including POST. This option is a viable solution as it leverages the built-in capabilities of API Gateway to cache responses. By configuring caching at the API Gateway stage level, the developer can cache responses to POST requests based on defined parameters.

upvoted 3 times

□ **Jing2023** 4 months, 3 weeks ago

Selected Answer: B

Why A is not correct

Amazon CloudFront does not cache the responses to POST, PUT, DELETE, and PATCH requests – these requests are proxied back to the origin server. You may enable caching for the responses to OPTIONS requests.

upvoted 3 times

□ **kr5031** 4 months, 3 weeks ago

Selected Answer: B

A is incorrect, because of

CloudFront always caches responses to GET and HEAD requests. You can also configure CloudFront to cache responses to OPTIONS requests. CloudFront does not cache responses to requests that use the other methods.

(<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorCustomOrigin.html>)

upvoted 4 times

□ **dilleman** 4 months, 3 weeks ago

I agree, I think B is correct as well looking into it more.

upvoted 2 times

□ **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A is the correct answer here. CloudFront can be configured to cache based on request headers, query strings, and POST request bodies. Option B might work but it does not work by default and it's not an effective way to solve this.

upvoted 1 times

□ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Solution (B) is the best option because it uses the Amazon API Gateway cache to cache POST requests.

upvoted 2 times

Question #183

Topic 1

A company is building a microservices application that consists of many AWS Lambda functions. The development team wants to use AWS Serverless Application Model (AWS SAM) templates to automatically test the Lambda functions. The development team plans to test a small percentage of traffic that is directed to new updates before the team commits to a full deployment of the application.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Choose two.)

- A. Use AWS SAM CLI commands in AWS CodeDeploy to invoke the Lambda functions to test the deployment.
- B. Declare the EventInvokeConfig on the Lambda functions in the AWS SAM templates with OnSuccess and OnFailure configurations.
- C. Enable gradual deployments through AWS SAM templates.
- D. Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment.
- E. Set the deployment preference type to Linear10PercentEvery10Minutes. Use hooks to test the deployment.

Correct Answer: BD

Community vote distribution

CD (71%) AD (21%) 7%

✉ **dilleman** Highly Voted 4 months, 3 weeks ago

Selected Answer: CD

C and D should be correct.

Given that "The development team plans to test a small percentage of traffic that is directed to new updates before the team commits to a full deployment of the application." then Option D makes more sense than Option E.

upvoted 5 times

✉ **KarBiswa** Most Recent 19 hours, 57 minutes ago

Selected Answer: AD

I will got A & D

D is nice and clear no debates

For A - <https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-using-automated-tests.html#:~:text=You%20can%20use%20the%20sam%20local%20invoke%20command%20to%20manually%20test%20your%20code%20by%20running%20Lambda%20functions%20locally.%20With%20the%20AWS%20SAM%C2%A0CLI%C2%20you%20can%20easily%20author%20automated%20integration%20tests%20by%20first%20running%20tests%20against%20local%20Lambda%20functions%20before%20deploying%20to%20the%20AWS%20Cloud.>

upvoted 1 times

✉ **SerialiDr** 1 month, 1 week ago

Selected Answer: CD

C. Enable gradual deployments through AWS SAM templates: Gradual deployments allow you to safely deploy your application while exposing new versions to only a portion of your traffic. This approach is ideal for testing new updates in a production environment without impacting all users. AWS SAM supports the configuration of deployment preferences directly within the SAM template.

D. Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment: The Canary deployment type is suitable for gradually introducing a new version of the Lambda function. In this case, "Canary10Percent30Minutes" means that 10% of the traffic will be directed to the new version for 30 minutes. If no issues are detected, the rest of the traffic is shifted to the new version. The use of hooks allows for automated tests to run against the new deployment, ensuring its stability before full traffic shift.

upvoted 2 times

✉ **c9ebec2** 2 months, 2 weeks ago

Selected Answer: AD

A: test code during deploy <https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-using-automated-tests.html>

D: Canary, to deploy a small percentage

upvoted 2 times

✉ **PrakashM14** 4 months ago

Selected Answer: CD

C. Enable gradual deployments through AWS SAM templates.

D. Set the deployment preference type to Canary10Percent30Minutes. Use hooks to test the deployment.

upvoted 3 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: CE

The correct answers are (C) and (E).

(C) is the most important step because it allows you to deploy new Lambda function updates to a small percentage of your traffic.

(E) is the second most important step because it allows you to test new Lambda function updates using hooks.

upvoted 1 times

Question #184

Topic 1

A company is using AWS CloudFormation to deploy a two-tier application. The application will use Amazon RDS as its backend database. The company wants a solution that will randomly generate the database password during deployment. The solution also must automatically rotate the database password without requiring changes to the application.

What is the MOST operationally efficient solution that meets these requirements?

- A. Use an AWS Lambda function as a CloudFormation custom resource to generate and rotate the password.
- B. Use an AWS Systems Manager Parameter Store resource with the SecureString data type to generate and rotate the password.
- C. Use a cron daemon on the application's host to generate and rotate the password.
- D. Use an AWS Secrets Manager resource to generate and rotate the password.

Correct Answer: D

Community vote distribution

D (100%)

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/88814-exam-aws-certified-developer-associate-topic-1-question-270/>

upvoted 3 times

Question #185

Topic 1

A developer has been asked to create an AWS Lambda function that is invoked any time updates are made to items in an Amazon DynamoDB table. The function has been created, and appropriate permissions have been added to the Lambda execution role. Amazon DynamoDB streams have been enabled for the table, but the function is still not being invoked.

Which option would enable DynamoDB table updates to invoke the Lambda function?

- A. Change the StreamViewType parameter value to NEW_AND_OLD_IMAGES for the DynamoDB table.
- B. Configure event source mapping for the Lambda function.
- C. Map an Amazon Simple Notification Service (Amazon SNS) topic to the DynamoDB streams.
- D. Increase the maximum runtime (timeout) setting of the Lambda function.

Correct Answer: B

Community vote distribution

B (100%)

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119

✉  **joshnort** 4 weeks ago

Selected Answer: B

Configure event source mapping for the Lambda function after enabling Streams
upvoted 1 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B is the only option that makes sense here
upvoted 3 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/4365-exam-aws-certified-developer-associate-topic-1-question-35/#>
upvoted 3 times

Question #186

Topic 1

A developer needs to deploy an application running on AWS Fargate using Amazon ECS. The application has environment variables that must be passed to a container for the application to initialize.

How should the environment variables be passed to the container?

- A. Define an array that includes the environment variables under the environment parameter within the service definition.
- B. Define an array that includes the environment variables under the environment parameter within the task definition.
- C. Define an array that includes the environment variables under the entryPoint parameter within the task definition.
- D. Define an array that includes the environment variables under the entryPoint parameter within the service definition.

Correct Answer: A

Community vote distribution

B (100%)

✉  **joshnort** 4 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/taskdef-envfiles.html>

upvoted 2 times

✉  **TanTran04** 2 months, 3 weeks ago

Selected Answer: B

Following ChatGPT 3.5, The correct option is B

When using Amazon ECS, the task definition is where you define parameters for your containers, including environment variables. The environment parameter within the task definition allows you to specify environment variables for your containers. This approach provides a clear separation of concerns, allowing you to define the environment variables at the task definition level, which is then used by the service when running tasks. Option A is incorrect because the environment variables are typically defined in the task definition rather than the service definition.

Options C and D are incorrect because the entryPoint parameter is used for specifying the entry point (command) for the container, not for defining environment variables.

upvoted 2 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/28795-exam-aws-certified-developer-associate-topic-1-question-108/>

upvoted 4 times

Question #187

Topic 1

A development team maintains a web application by using a single AWS RDS template. The template defines web servers and an Amazon RDS database. The team uses the CloudFormation template to deploy the CloudFormation stack to different environments.

During a recent application deployment, a developer caused the primary development database to be dropped and recreated. The result of this incident was a loss of data. The team needs to avoid accidental database deletion in the future.

Which solutions will meet these requirements? (Choose two.)

- A. Add a CloudFormation DeletionPolicy attribute with the Retain value to the database resource.
- B. Update the CloudFormation stack policy to prevent updates to the database.
- C. Modify the database to use a Multi-AZ deployment.
- D. Create a CloudFormation stack set for the web application and database deployments.
- E. Add a CloudFormation DeletionPolicy attribute with the Retain value to the stack.

Correct Answer: AB
Community vote distribution


 **joshnort** 4 weeks ago

Selected Answer: AB

<https://repost.aws/knowledge-center/cloudformation-accidental-updates>
upvoted 2 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: AB

A. Add a CloudFormation DeletionPolicy attribute with the Retain value to the database resource.

The DeletionPolicy attribute can be used in the CloudFormation template to protect a resource from being accidentally deleted. By setting the DeletionPolicy to Retain, the resource is retained when the stack is deleted, thus preventing accidental data loss. This should be applied directly to the database resource in the CloudFormation template.

B. Update the CloudFormation stack policy to prevent updates to the database.

A stack policy can be used to prevent changes to certain resources during stack updates. By defining a stack policy that prohibits actions on the database resource, the team can prevent accidental modifications or deletions of the database during stack updates.

upvoted 2 times

 **Gold07** 4 months, 2 weeks ago

The answer is A and D

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: AB

A and B) <https://www.examtopics.com/discussions/amazon/view/103521-exam-aws-certified-developer-associate-dva-c02-topic-1/#>
upvoted 4 times

Question #188

Topic 1

A developer is storing sensitive data generated by an application in Amazon S3. The developer wants to encrypt the data at rest. A company policy requires an audit trail of when the AWS Key Management Service (AWS KMS) key was used and by whom.

Which encryption option will meet these requirements?

- A. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS)
- C. Server-side encryption with customer-provided keys (SSE-C)
- D. Server-side encryption with self-managed keys

Correct Answer: B

Community vote distribution

B (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: B

SSE-KMS provides an additional layer of security by requiring separate permissions for the use of an encryption key to the bucket. This option also provides an audit trail by logging the use of the key in AWS CloudTrail, which is a requirement according to the company policy. The audit trail includes information about who used the key and when it was used, which fulfills the requirement for auditing.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B, since we need an audit trail of the AWK KMS key then this is the one to use.

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/28801-exam-aws-certified-developer-associate-topic-1-question-217/>

upvoted 3 times

Question #189

Topic 1

A company has an ecommerce application. To track product reviews, the company's development team uses an Amazon DynamoDB table.

Every record includes the following:

- A Review ID, a 16-digit universally unique identifier (UUID)
- A Product ID and User ID, 16-digit UUIDs that reference other tables
- A Product Rating on a scale of 1-5
- An optional comment from the user

The table partition key is the Review ID. The most performed query against the table is to find the 10 reviews with the highest rating for a given product.

Which index will provide the FASTEST response for this query?

- A. A global secondary index (GSI) with Product ID as the partition key and Product Rating as the sort key
- B. A global secondary index (GSI) with Product ID as the partition key and Review ID as the sort key
- C. A local secondary index (LSI) with Product ID as the partition key and Product Rating as the sort key
- D. A local secondary index (LSI) with Review ID as the partition key and Product ID as the sort key

Correct Answer: B

Community vote distribution

A (100%)

✉  **SerialiDr** 1 month, 1 week ago

Selected Answer: A

This GSI allows for queries that are based on Product ID, efficiently narrowing down the reviews for a specific product. The Product Rating as the sort key enables sorting the reviews by their rating, which directly supports the need to find the top 10 reviews. GSIs also support a different partition key than the base table, which is necessary in this case since the base table's partition key is Review ID.

upvoted 2 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A should be correct

upvoted 3 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

A) <https://www.examtopics.com/discussions/amazon/view/88995-exam-aws-certified-developer-associate-topic-1-question-362/>
upvoted 3 times

Question #190

Topic 1

A company needs to distribute firmware updates to its customers around the world.

Which service will allow easy and secure control of the access to the downloads at the lowest cost?

- A. Use Amazon CloudFront with signed URLs for Amazon S3.
- B. Create a dedicated Amazon CloudFront Distribution for each customer.
- C. Use Amazon CloudFront with AWS Lambda@Edge.
- D. Use Amazon API Gateway and AWS Lambda to control access to an S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

✉  **SerialiDr** 1 month, 1 week ago

Selected Answer: A

Amazon CloudFront is a content delivery network (CDN) service that can efficiently distribute files globally. Using signed URLs provides a secure method to control access to the firmware updates. Only users with valid signed URLs can download the files, ensuring controlled access. This approach is cost-effective as it leverages CloudFront's caching capabilities to reduce load on the origin (Amazon S3) and reduces data transfer costs.

upvoted 2 times

✉  **walala97** 1 month, 3 weeks ago

Selected Answer: A

obtion B,for each customer,will bring high costs

upvoted 2 times

✉  **TanTran04** 2 months, 3 weeks ago

Selected Answer: A

A. Use Amazon CloudFront with signed URLs for Amazon S3.

Using Amazon CloudFront with signed URLs is a secure and cost-effective way to control access to downloads. With signed URLs, you can generate URLs with limited time validity, ensuring that only users with the correct URL and during the specified time window can access the firmware updates. This provides both security and control over access.

Option B (Create a dedicated Amazon CloudFront Distribution for each customer) may result in higher costs and increased complexity. Option C (Use Amazon CloudFront with AWS Lambda@Edge) is more focused on customization and additional processing at the edge locations, which may not be necessary for simple access control. Option D (Use Amazon API Gateway and AWS Lambda) is more suited for managing APIs and might be an overkill for a straightforward firmware update distribution scenario.

upvoted 3 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 3 times

✉  **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

A) <https://www.examtopics.com/discussions/amazon/view/8792-exam-aws-certified-developer-associate-topic-1-question-179/#>

upvoted 4 times

Question #191

Topic 1

A developer is testing an application that invokes an AWS Lambda function asynchronously. During the testing phase, the Lambda function fails to process after two retries.

How can the developer troubleshoot the failure?

- A. Configure AWS CloudTrail logging to investigate the invocation failures.
- B. Configure Dead Letter Queues by sending events to Amazon SQS for investigation.
- C. Configure Amazon Simple Workflow Service to process any direct unprocessed events.
- D. Configure AWS Config to process any direct unprocessed events.

Correct Answer: B

Community vote distribution

B (100%)

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: B

In AWS Lambda, you can use Dead Letter Queues (DLQ) to capture and retain events that couldn't be processed successfully after a specified number of retries. By configuring a DLQ, the failed events are sent to an Amazon SQS queue, allowing you to investigate and analyze the reasons for the failures.

upvoted 3 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

Dead Letter Queues (DLQ) can be configured for Lambda functions to capture failed asynchronous invocations. Events that cannot be processed will be sent to an SQS queue (or an SNS topic) you specify, allowing for further investigation and reprocessing.

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/28638-exam-aws-certified-developer-associate-topic-1-question-317/#>

upvoted 2 times

Question #192

Topic 1

A company is migrating its PostgreSQL database into the AWS Cloud. The company wants to use a database that will securely and regularly rotate database credentials. The company wants a solution that does not require additional programming overhead.

Which solution will meet these requirements?

- A. Use Amazon Aurora PostgreSQL for the database. Store the database credentials in AWS Systems Manager Parameter Store. Turn on rotation.
- B. Use Amazon Aurora PostgreSQL for the database. Store the database credentials in AWS Secrets Manager. Turn on rotation.
- C. Use Amazon DynamoDB for the database. Store the database credentials in AWS Systems Manager Parameter Store. Turn on rotation.
- D. Use Amazon DynamoDB for the database. Store the database credentials in AWS Secrets Manager. Turn on rotation.

Correct Answer: C

Community vote distribution

B (100%)

✉️  **Digo30sp**  4 months, 4 weeks ago

Selected Answer: B

B) The correct answer is (B).

Solution (B) is the best option because it meets all the requirements:

Using a database that secures and regularly changes database credentials: Amazon Aurora PostgreSQL offers built-in credential rotation, which allows you to change database credentials at regular intervals.

Solution that requires no additional programming overhead: Amazon Aurora PostgreSQL credential rotation is fully automated, so it requires no additional programming overhead.

upvoted 6 times

✉️  **TanTran04**  2 months, 3 weeks ago

Selected Answer: B

AWS Secrets Manager is a service designed to rotate, manage, and retrieve database credentials, API keys, and other secrets. In this scenario, storing the database credentials in AWS Secrets Manager and enabling rotation ensures that your database credentials are regularly rotated without requiring additional programming overhead.

Option B is the most suitable because it specifically addresses the need for securing and regularly rotating database credentials in the AWS Cloud. Amazon Aurora PostgreSQL is a fully managed relational database service, and AWS Secrets Manager seamlessly integrates with it for secure credential management.

upvoted 1 times

Question #193

Topic 1

A developer is creating a mobile application that will not require users to log in.

What is the MOST efficient method to grant users access to AWS resources?

- A. Use an identity provider to securely authenticate with the application.
- B. Create an AWS Lambda function to create an IAM user when a user accesses the application.
- C. Create credentials using AWS KMS and apply these credentials to users when using the application.
- D. Use Amazon Cognito to associate unauthenticated users with an IAM role that has limited access to resources.

Correct Answer: D

Community vote distribution

D (100%)

 **Digo30sp**  4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/4245-exam-aws-certified-developer-associate-topic-1-question-79/>
upvoted 5 times

 **SerialiDr**  1 month, 1 week ago

Selected Answer: D

Amazon Cognito allows you to create unique identities for users of your application and assign permissions to these identities using IAM roles. By using Cognito's unauthenticated identities (also known as guest users), you can grant limited AWS resource access to users without requiring them to log in. This approach is secure, scalable, and does not require managing user credentials.
upvoted 1 times

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: D

Amazon Cognito is designed to handle user identity and access management for mobile and web applications
upvoted 1 times

Question #194

Topic 1

A company has developed a new serverless application using AWS Lambda functions that will be deployed using the AWS Serverless Application Model (AWS SAM) CLI.

Which step should the developer complete prior to deploying the application?

- A. Compress the application to a .zip file and upload it into AWS Lambda.
- B. Test the new AWS Lambda function by first tracing it in AWS X-Ray.
- C. Bundle the serverless application using a SAM package.
- D. Create the application environment using the eb create my-env command.

Correct Answer: B

Community vote distribution

C (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

Using sam package (or aws cloudformation package) command, the developer can package the Lambda functions, along with any dependencies and resources defined in the SAM template, into a deployment package. This command uploads local artifacts (like Lambda function code and Swagger files) to an S3 bucket and produces a modified SAM template file, formatted for deployment.

upvoted 1 times

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: C

C. Bundle the serverless application using a SAM package.

Before deploying a serverless application using the AWS Serverless Application Model (AWS SAM) CLI, the developer should bundle the application using the sam package command. This command packages and uploads the local artifacts of your serverless application to Amazon S3, and it produces a packaged AWS SAM template file that you can deploy with the sam deploy command.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

C) <https://www.examtopics.com/discussions/amazon/view/28650-exam-aws-certified-developer-associate-topic-1-question-312/>

upvoted 4 times

Question #195

Topic 1

A company wants to automate part of its deployment process. A developer needs to automate the process of checking for and deleting unused resources that supported previously deployed stacks but that are no longer used.

The company has a central application that uses the AWS Cloud Development Kit (AWS CDK) to manage all deployment stacks. The stacks are spread out across multiple accounts. The developer's solution must integrate as seamlessly as possible within the current deployment process.

Which solution will meet these requirements with the LEAST amount of configuration?

- A. In the central AWS CDK application, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CloudFormation template from a JSON file. Use the template to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- B. In the central AWS CDK application, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CDK custom resource. Use the custom resource to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- C. In the central AWS CDK, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an API in AWS Amplify. Use the API to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.
- D. In the AWS Lambda console, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CDK custom resource. Use the custom resource to import the Lambda function into the stack and to invoke the Lambda function when the deployment stack runs.

Correct Answer: B

Community vote distribution

B (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: B

This approach integrates directly into the existing AWS CDK deployment process. By writing a handler function within the CDK application, the developer can leverage the AWS SDK to programmatically identify and delete unused resources. The AWS CDK custom resource can then be used to invoke this function as part of the deployment process. This solution is efficient as it keeps everything within the CDK ecosystem and minimizes additional external configurations.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B. In the central AWS CDK application, write a handler function in the code that uses AWS SDK calls to check for and delete unused resources. Create an AWS CDK custom resource. Use the custom resource to attach the function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs.

upvoted 1 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

Solution (B) is the best option because:

Requires the LEAST amount of configuration: Solution (B) uses an AWS CDK custom resource, which is a type of resource that can be defined in AWS CDK code. Custom resources are a convenient way to add custom functionality to your AWS CloudFormation stacks.

Integrates seamlessly into the current deployment process: Solution (B) uses the AWS CDK custom resource to attach function code to an AWS Lambda function and to invoke the Lambda function when the deployment stack runs. This means that the solution does not require any changes to the existing AWS CDK code.

upvoted 4 times

Question #196

Topic 1

A company built a new application in the AWS Cloud. The company automated the bootstrapping of new resources with an Auto Scaling group by using AWS CloudFormation templates. The bootstrap scripts contain sensitive data.

The company needs a solution that is integrated with CloudFormation to manage the sensitive data in the bootstrap scripts.

Which solution will meet these requirements in the MOST secure way?

- A. Put the sensitive data into a CloudFormation parameter. Encrypt the CloudFormation templates by using an AWS Key Management Service (AWS KMS) key.
- B. Put the sensitive data into an Amazon S3 bucket. Update the CloudFormation templates to download the object from Amazon S3 during bootstrap.
- C. Put the sensitive data into AWS Systems Manager Parameter Store as a secure string parameter. Update the CloudFormation templates to use dynamic references to specify template values.
- D. Put the sensitive data into Amazon Elastic File System (Amazon EFS). Enforce EFS encryption after file system creation. Update the CloudFormation templates to retrieve data from Amazon EFS.

Correct Answer: D

Community vote distribution



Digo30sp Highly Voted 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Solution (C) is the best option because:

It's the most secure solution: Sensitive data is stored in AWS Systems Manager Parameter Store, which is a secret management service managed by AWS. Secure string parameters in AWS Systems Manager Parameter Store are encrypted with an AWS KMS key. It's integrated with CloudFormation: Secure string parameters can be referenced in CloudFormation templates using dynamic references. This means that sensitive data does not need to be stored in CloudFormation code.

upvoted 5 times

TanTran04 Most Recent 2 months, 3 weeks ago

Selected Answer: C

AWS Systems Manager Parameter Store is a secure and scalable solution for storing configuration data, including sensitive information. In this case, using a secure string parameter allows you to store the sensitive data in Parameter Store in an encrypted form.

Option C is the most secure because it leverages AWS Systems Manager Parameter Store's capabilities for securely storing sensitive data, and dynamic references allow you to directly reference the parameter values in CloudFormation templates. This approach avoids exposing sensitive data in the templates themselves and provides a central and secure storage solution for sensitive configuration information.

upvoted 2 times

kashtelyan 4 months, 2 weeks ago

Selected Answer: A

A option leverages CloudFormation parameters, which can securely store sensitive data. By using an AWS KMS key to encrypt the CloudFormation templates, you ensure that the sensitive data is protected. It follows the principle of least privilege and provides secure access to sensitive information directly within CloudFormation.

Option B is less secure because it involves storing sensitive data in an S3 bucket, which could be compromised.

Option C suggests using AWS Systems Manager Parameter Store, which is secure, but using CloudFormation parameters and KMS keys provides an integrated solution directly within CloudFormation.

Option D involves Amazon EFS, which is typically used for file storage and is not designed for securely storing sensitive data directly within CloudFormation.

upvoted 1 times

dilleman 4 months, 3 weeks ago

Selected Answer: C

C is the correct choice. Parameter Store's secure string parameter encrypts the data using AWS KMS

upvoted 4 times

Question #197

Topic 1

A company needs to set up secure database credentials for all its AWS Cloud resources. The company's resources include Amazon RDS DB instances, Amazon DocumentDB clusters, and Amazon Aurora DB instances. The company's security policy mandates that database credentials be encrypted at rest and rotated at a regular interval.

Which solution will meet these requirements MOST securely?

- A. Set up IAM database authentication for token-based access. Generate user tokens to provide centralized access to RDS DB instances, Amazon DocumentDB clusters, and Aurora DB instances.
- B. Create parameters for the database credentials in AWS Systems Manager Parameter Store. Set the Type parameter to SecureString. Set up automatic rotation on the parameters.
- C. Store the database access credentials as an encrypted Amazon S3 object in an S3 bucket. Block all public access on the S3 bucket. Use S3 server-side encryption to set up automatic rotation on the encryption key.
- D. Create an AWS Lambda function by using the SecretsManagerRotationTemplate template in the AWS Secrets Manager console. Create secrets for the database credentials in Secrets Manager. Set up secrets rotation on a schedule.

Correct Answer: C

Community vote distribution

D (100%)

 **TanTran04** 2 months, 3 weeks ago

Selected Answer: D

Rotate auto SecretsManager
upvoted 2 times

 **nickolaj** 4 months, 2 weeks ago

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>
upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

the best and most secure option is:
D. Create an AWS Lambda function by using the SecretsManagerRotationTemplate template in the AWS Secrets Manager console.
upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

Solution (D) is the best option because:

It's the most secure solution: AWS Secrets Manager is an AWS-managed secrets management service that provides encryption at rest and automatic secret rotation.

Meets the company's security requirements: The solution meets the company's security requirements because:

Database credentials are encrypted at rest using AWS Key Management Service (AWS KMS).

Database credentials are automatically rotated at regular intervals.

upvoted 3 times

 **fordiscussiontwo** 4 months, 4 weeks ago

DDDDDDDD

upvoted 3 times

Question #198

Topic 1

A developer has created an AWS Lambda function that makes queries to an Amazon Aurora MySQL DB instance. When the developer performs a test, the DB instance shows an error for too many connections.

Which solution will meet these requirements with the LEAST operational effort?

- A. Create a read replica for the DB instance. Query the replica DB instance instead of the primary DB instance.
- B. Migrate the data to an Amazon DynamoDB database.
- C. Configure the Amazon Aurora MySQL DB instance for Multi-AZ deployment.
- D. Create a proxy in Amazon RDS Proxy. Query the proxy instead of the DB instance.

Correct Answer: D

Community vote distribution

D (100%)

 **TanTran04** 2 months, 3 weeks ago

too many connections => proxy
upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D.
RDS Proxy sits between the application and the database to manage and pool connections, reducing the chance of exhausting database connections when many Lambda functions try to connect simultaneously.
upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

D) <https://www.examtopics.com/discussions/amazon/view/88969-exam-aws-certified-developer-associate-topic-1-question-358/>
upvoted 1 times

 **fordiscussionstwo** 4 months, 4 weeks ago

DDDDDDDDDDDD
upvoted 3 times

Question #199

Topic 1

A developer is creating a new REST API by using Amazon API Gateway and AWS Lambda. The development team tests the API and validates responses for the known use cases before deploying the API to the production environment.

The developer wants to make the REST API available for testing by using API Gateway locally.

Which AWS Serverless Application Model Command Line Interface (AWS SAM CLI) subcommand will meet these requirements?

- A. Sam local invoke
- B. Sam local generate-event
- C. Sam local start-lambda
- D. Sam local start-api

Correct Answer: D*Community vote distribution* D (100%)

 **Digo30sp**  4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

The AWS SAM CLI sam local start-api subcommand is used to start a local API Gateway instance. This allows you to test your REST API locally before deploying it to the production environment.

The other subcommands will not meet the developer's requirements:

Local invocation of Sam is used to invoke a Lambda function locally.

Sam's local event generation is used to generate a local event file to be used to invoke a Lambda function locally.

Sam local start-lambda is used to start a local instance of a Lambda function.

upvoted 7 times

 **dilleman**  4 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

 **fordiscussiontwo** 4 months, 4 weeks ago

DDDDDDDDDDDD

upvoted 4 times

Question #200

Topic 1

A company has a serverless application on AWS that uses a fleet of AWS Lambda functions that have aliases. The company regularly publishes new Lambda function by using an in-house deployment solution. The company wants to improve the release process and to use traffic shifting. A newly published function version should initially make available only to a fixed percentage of production users.

Which solution will meet these requirements?

- A. Configure routing on the alias of the new function by using a weighted alias.
- B. Configure a canary deployment type for Lambda.
- C. Configure routing on the new versions by using environment variables.
- D. Configure a linear deployment type for Lambda.

Correct Answer: B

Community vote distribution

A (100%)

✉  **Digo30sp**  4 months, 4 weeks ago

Selected Answer: A

The correct answer is (A).

Weighted aliases allow you to route traffic to different versions of a function based on weights that you assign. This allows you to implement a canary deployment, where you initially route a small percentage of your traffic to the new version of the function, and then gradually increase the percentage as you gain confidence in the new version.

upvoted 5 times

✉  **rimaSamir** 2 weeks ago

If we need Canary deployment, then why not B ?

How you will use A in automated deployment?

upvoted 1 times

✉  **KarBiswa**  18 hours, 4 minutes ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html#configuring-alias-routing>:~:text=function%20version.%20For%20example%2C%20you%20can%20reduce%20the%20risk%20of%20deploying%20a%20new%20version%20by%20configuring%20the%20alias%20to%20send%20most%20of%20the%20traffic%20to%20the%20existing%20version%2C%20and%20only%20a%20small%20percentage%20of%20traffic%20to%20the%20new%20version.

upvoted 1 times

✉  **NijeshT** 3 months ago

Answer is A.

weighted aliases offer fixed, predefined percentages

upvoted 3 times

✉  **fordiscussiontwo** 4 months, 4 weeks ago

AAAAAAAAAAAA

upvoted 3 times

Question #201

Topic 1

A company has an application that stores data in Amazon RDS instances. The application periodically experiences surges of high traffic that cause performance problems. During periods of peak traffic, a developer notices a reduction in query speed in all database queries.

The team's technical lead determines that a multi-threaded and scalable caching solution should be used to offload the heavy read traffic. The solution needs to improve performance.

Which solution will meet these requirements with the LEAST complexity?

- A. Use Amazon ElastiCache for Memcached to offload read requests from the main database.
- B. Replicate the data to Amazon DynamoDB and set up a DynamoDB Accelerator (DAX) cluster.
- C. Configure the Amazon RDS instances to use Multi-AZ deployment with one standby instance. Offload read requests from the main database to the standby instance.
- D. Use Amazon ElastiCache for Redis to offload read requests from the main database.

Correct Answer: A
Community vote distribution
 A (100%)

 **kashtelyan**  4 months, 3 weeks ago

Selected Answer: A

When deciding between Memcached and Redis, here are a few questions to consider:

Is object caching your primary goal, for example to offload your database? If so, use Memcached.

<https://docs.aws.amazon.com/whitepapers/latest/scale-performance-elastichache/memcached-vs.-redis.html>

upvoted 6 times

 **tsdsmth**  3 weeks, 5 days ago

Selected Answer: A

A. If you're looking for a multi-threaded solution, then ElastiCache for Memcached (not Redis) is the solution.

upvoted 1 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

A. Use Amazon ElastiCache for Memcached to offload read requests from the main database.

ElastiCache for Memcached is a good fit for this scenario. It's a high-performance, distributed, in-memory caching system that can easily scale to manage surges in read traffic. It's simple to set up and integrate with an existing RDS instance.

D. Use Amazon ElastiCache for Redis to offload read requests from the main database.

ElastiCache for Redis also offers high performance and is capable of handling surges in read traffic. Redis provides more advanced data structures and features compared to Memcached, like persistence, built-in replication, and support for complex data types. However, it might be more complex to set up and manage than Memcached, depending on the use case.

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

The correct answer is (A).

Amazon ElastiCache for Memcached is a scalable, multithreaded caching solution that can be used to offload heavy read traffic from Amazon RDS instances. ElastiCache for Memcached is easy to configure and manage, making it a low-effort solution to meet technical lead requirements.

upvoted 3 times

 **fordiscussiontwo** 4 months, 4 weeks ago

AAAAAAAAAA

upvoted 3 times

Question #202

Topic 1

A developer must provide an API key to an AWS Lambda function to authenticate with a third-party system. The Lambda function will run on a schedule. The developer needs to ensure that the API key remains encrypted at rest.

Which solution will meet these requirements?

- A. Store the API key as a Lambda environment variable by using an AWS Key Management Service (AWS KMS) customer managed key.
- B. Configure the application to prompt the user to provide the password to the Lambda function on the first run.
- C. Store the API key as a value in the application code.
- D. Use Lambda@Edge and only communicate over the HTTPS protocol.

Correct Answer: C

Community vote distribution

A (100%)

✉  **Digo30sp**  4 months, 4 weeks ago

Selected Answer: A

The correct answer is (A).

Storing the API key as a Lambda environment variable using an AWS Key Management Service (AWS KMS) customer-managed key is the most secure solution. AWS KMS is a managed encryption service that provides customer-managed keys. Customer-managed keys are encrypted with an AWS KMS master key, which is stored in an AWS KMS vault.

upvoted 6 times

✉  **SerialiDr**  1 month, 1 week ago

Selected Answer: A

Lambda environment variables can be encrypted using a customer managed key in AWS KMS. This approach ensures that the API key is encrypted at rest and seamlessly integrated into the Lambda function. When the function is executed, it can access the decrypted value of the API key for authenticating with the third-party system.

upvoted 2 times

✉  **fordiscussiontwo** 4 months, 4 weeks ago

AAAAAAAAAA

upvoted 2 times

Question #203

Topic 1

An IT department uses Amazon S3 to store sensitive images. After more than 1 year, the company moves the images into archival storage. The company rarely accesses the images, but the company wants a storage solution that maximizes resiliency. The IT department needs access to the images that have been moved to archival storage within 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Standard-Infrequent Access (S3 Standard-IA) to store the images. Use S3 Glacier Deep Archive with standard retrieval to store and retrieve archived images.
- B. Use S3 Standard-Infrequent Access (S3 Standard-IA) to store the images. Use S3 Glacier Deep Archive with bulk retrieval to store and retrieve archived images.
- C. Use S3 Intelligent-Tiering to store the images. Use S3 Glacier Deep Archive with standard retrieval to store and retrieve archived images.
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA) to store the images. Use S3 Glacier Deep Archive with bulk retrieval to store and retrieve archived images.

Correct Answer: D

Community vote distribution



Learning4life Highly Voted 4 months, 2 weeks ago

A is correct. The requirement of maximizing resiliency rules out One Zone. Standard recover is within 12 hours, which fits the requirement of within 24 hours. [https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html#:~:text=Deep%20Archive%20or,-S3%20Intelligent%2DTiering%20Deep%20Archive%20Access,-Not%20available](https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html)

upvoted 7 times

KarBiswa Most Recent 17 hours, 51 minutes ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html#:~:text=Deep%20Archive%20or,-S3%20Intelligent%2DTiering%20Deep%20Archive%20Access,-Not%20available>

upvoted 1 times

SerialiDr 1 month, 1 week ago

Selected Answer: A

S3 Standard-IA is designed for data that is accessed less frequently but requires rapid access when needed. It offers a lower storage cost while still providing high durability, availability, and performance.

S3 Glacier Deep Archive is the most cost-effective option for archival storage in AWS and is designed for data that is accessed very rarely. The standard retrieval option in Glacier Deep Archive typically returns data within 12 hours, meeting the requirement of access within 24 hours.

upvoted 2 times

_YaWeb 1 month, 1 week ago

ChatGPT goes with B

upvoted 1 times

dostonbekabdullaev 1 month, 2 weeks ago

Selected Answer: A

AAAAAAA

upvoted 1 times

Certified101 2 months, 2 weeks ago

Selected Answer: A

A is correct -Bulk retrieval is 48hours

upvoted 1 times

TanTran04 2 months, 2 weeks ago

Selected Answer: B

With Option A: Standard retrieval would provide faster access to the archived images (typically within 3-5 hours), it is more expensive than Bulk retrieval. Since the company has indicated they can wait up to 24 hours for access, the slower but cheaper

=> Option B is the best choice.

upvoted 1 times

Hanny 2 months, 3 weeks ago

Selected Answer: C

C. Use S3 Intelligent-Tiering to store the images. Use S3 Glacier Deep Archive with standard retrieval to store and retrieve archived images.

upvoted 1 times

✉ **tqiu654** 2 months, 4 weeks ago

Selected Answer: B

GPT: B. Use S3 Standard-Infrequent Access (S3 Standard-IA) to store the images. Use S3 Glacier Deep Archive and select Batch Retrieval to store and retrieve archived images.

upvoted 2 times

✉ **hcsaba1982** 4 months, 1 week ago

Selected Answer: C

A : Glacier Deep Archive is cheaper than Standard-IA.
C : Standard archival is 12h.
B : bulk retrieval is 48h
D : S3 One Zone-IA - cross-out due to "maximizes resiliency"

upvoted 4 times

✉ **ut18** 4 months ago

Check the requirement :

The IT department needs access to the images that have been moved to archival storage within 24 hours.

upvoted 1 times

✉ **Cerakoted** 4 months, 3 weeks ago

Selected Answer: A

It is A

upvoted 2 times

✉ **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

A) Correct A) because the standard recovery is carried out within 12 hours and the requirement says that it must be recovered within 24 hours.
Bulk recovery takes up to 48 hours

upvoted 4 times

✉ **fordiscussionstwo** 4 months, 4 weeks ago

BBBBBBBBBB

upvoted 2 times

Question #204

Topic 1

A developer is building a serverless application by using the AWS Serverless Application Model (AWS SAM). The developer is currently testing the application in a development environment. When the application is nearly finished, the developer will need to set up additional testing and staging environments for a quality assurance team.

The developer wants to use a feature of the AWS SAM to set up deployments to multiple environments.

Which solution will meet these requirements with the LEAST development effort?

- A. Add a configuration file in TOML format to group configuration entries to every environment. Add a table for each testing and staging environment. Deploy updates to the environments by using the `sam deploy` command and the `--config-env` flag that corresponds to each environment.
- B. Create additional AWS SAM templates for each testing and staging environment. Write a custom shell script that uses the `sam deploy` command and the `--template-file` flag to deploy updates to the environments.
- C. Create one AWS SAM configuration file that has default parameters. Perform updates to the testing and staging environments by using the `--parameter-overrides` flag in the AWS SAM CLI and the parameters that the updates will override.
- D. Use the existing AWS SAM template. Add additional parameters to configure specific attributes for the serverless function and database table resources that are in each environment. Deploy updates to the testing and staging environments by using the `sam deploy` command.

Correct Answer: B*Community vote distribution*

NinjaCloud Highly Voted 4 months ago

Correct Answer: C,

You can create a single AWS SAM configuration file with default parameters and then use the `--parameter-overrides` flag with the AWS SAM CLI to specify parameters that override the defaults for each testing and staging environment. This approach keeps the AWS SAM template file (the infrastructure-as-code) consistent and minimizes duplication. It's a clean and simple way to manage multiple environments without having to create separate templates or custom scripts.

upvoted 6 times

Jing2023 Highly Voted 4 months, 2 weeks ago

Selected Answer: A

A should be correct

reference this stackoverflow post <https://stackoverflow.com/questions/68826108/how-to-deploy-to-different-environments-with-aws-sam>

upvoted 5 times

KarBiswa Most Recent 17 hours, 43 minutes ago

Selected Answer: A

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-config.html>

upvoted 1 times

SerialiDr 1 month, 1 week ago

Selected Answer: A

To set up deployments to multiple environments with the least development effort in a serverless application using the AWS Serverless Application Model (AWS SAM), the developer can utilize a configuration file in TOML format with grouped configuration entries for each environment. This approach allows for easy management of different environment configurations and streamlines the deployment process. The specific steps would include:

Creating a configuration file in TOML format: This file will include a table for each testing and staging environment, where each table contains the specific configuration for that environment.

Using the `sam deploy` command with the `--config-env` flag: This flag allows specifying which environment configuration to use for the deployment, corresponding to the tables defined in the configuration file.

This solution aligns with Option A:

upvoted 2 times

Certified101 2 months, 2 weeks ago

Selected Answer: C

C with least development overhead

upvoted 1 times

TanTran04 2 months, 3 weeks ago

Selected Answer: C

With at LEAST development effort, Option C is better than A

While this approach may work, it introduces additional complexity with the need for a separate configuration file, and it may not be as straightforward as using parameter overrides, as suggested in option C. The use of TOML format might be more suited for certain scenarios, but in the context of AWS SAM, which commonly relies on YAML or JSON configurations, it might be an extra layer of complexity that isn't necessary.

Option C, on the other hand, recommends using a single AWS SAM configuration file with default parameters and updating testing and staging environments using the --parameter-overrides flag. This approach is more aligned with typical AWS SAM practices and is simpler and more straightforward than managing multiple configuration files.

upvoted 3 times

 **TanTran04** 2 months, 3 weeks ago

With at LEAST development effort, Option C is better than A

While this approach may work, it introduces additional complexity with the need for a separate configuration file, and it may not be as straightforward as using parameter overrides, as suggested in option C. The use of TOML format might be more suited for certain scenarios, but in the context of AWS SAM, which commonly relies on YAML or JSON configurations, it might be an extra layer of complexity that isn't necessary.

Option C, on the other hand, recommends using a single AWS SAM configuration file with default parameters and updating testing and staging environments using the --parameter-overrides flag. This approach is more aligned with typical AWS SAM practices and is simpler and more straightforward than managing multiple configuration files.

upvoted 1 times

 **Hanny** 2 months, 3 weeks ago

C. Create one AWS SAM configuration file that has default parameters. Perform updates to the testing and staging environments by using the --parameter-overrides flag in the AWS SAM CLI and the parameters that the updates will override.

upvoted 2 times

 **Rameez1** 4 months, 2 weeks ago

Selected Answer: C

Here all the options can do the Job but option C does it with least effort.

upvoted 2 times

 **PrakashM14** 4 months, 2 weeks ago

Selected Answer: C

Options A and B introduce additional complexities such as configuration files in TOML format or writing custom shell scripts. These might require more effort and maintenance.

Option D involves adding additional parameters to the existing AWS SAM template, which can work but may lead to a more complex and less maintainable template as the number of environments grows.

Therefore, option C is a straightforward and efficient solution for deploying to multiple environments with AWS SAM.

upvoted 2 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

Using the existing AWS SAM template is the option that requires the LEAST development effort. To configure deployments across multiple environments, you can add additional parameters to your AWS SAM template to configure specific attributes for the serverless function and database table resources that are in each environment.

upvoted 2 times

 **fordiscussiontwo** 4 months, 4 weeks ago

AAAAAAAAAA

upvoted 2 times

Question #205

Topic 1

A developer is working on an application that processes operating data from IoT devices. Each IoT device uploads a data file once every hour to an Amazon S3 bucket. The developer wants to immediately process each data file when the data file is uploaded to Amazon S3.

The developer will use an AWS Lambda function to process the data files from Amazon S3. The Lambda function is configured with the S3 bucket information where the files are uploaded. The developer wants to configure the Lambda function to immediately invoke after each data file is uploaded.

Which solution will meet these requirements?

- A. Add an asynchronous invocation to the Lambda function. Select the S3 bucket as the source.
- B. Add an Amazon EventBridge event to the Lambda function. Select the S3 bucket as the source.
- C. Add a trigger to the Lambda function. Select the S3 bucket as the source.
- D. Add a layer to the Lambda function. Select the S3 bucket as the source.

Correct Answer: B

Community vote distribution

C (90%) 10%

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

To meet the requirement of processing data files immediately after they are uploaded to an Amazon S3 bucket, the best solution is to add a trigger to the AWS Lambda function with the S3 bucket as the source. This will configure the Lambda function to be automatically invoked when a new file is uploaded to the specified S3 bucket.

upvoted 1 times

 **Certified101** 2 months, 2 weeks ago

Selected Answer: C

C using S3 Events, no need for EventBridge here.

upvoted 1 times

 **LR2023** 2 months, 3 weeks ago

Selected Answer: B

EventBridge can be employed to collect real-time data streams from various sources like IoT devices, mobile apps, or web applications. Lambda functions can then process this data to perform analytics, generate alerts, or update dashboards.

upvoted 1 times

 **LR2023** 2 months, 3 weeks ago

You can use Amazon EventBridge to monitor an S3 bucket for new image uploads. When a new image is detected, EventBridge triggers a Lambda function that processes the image, applies filters, and generates thumbnails, all without manual intervention

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Adding a trigger to your Lambda function is the solution that will meet these requirements. A trigger is an event that can invoke a Lambda function. In the case of this issue, the trigger must be an Amazon S3 event that fires when a new file is uploaded to the bucket.

upvoted 4 times

 **fordiscussionstwo** 4 months, 4 weeks ago

CCCCCCCCCC

upvoted 4 times

Question #206

Topic 1

A developer is setting up infrastructure by using AWS CloudFormation. If an error occurs when the resources described in the CloudFormation template are provisioned, successfully provisioned resources must be preserved. The developer must provision and update the CloudFormation stack by using the AWS CLI.

Which solution will meet these requirements?

- A. Add an --enable-termination-protection command line option to the create-stack command and the update-stack command.
- B. Add a --disable-rollback command line option to the create-stack command and the update-stack command.
- C. Add a --parameters ParameterKey=PreserveResources,ParameterValue=True command line option to the create-stack command and the update-stack command.
- D. Add a --tags Key=PreserveResources,Value=True command line option to the create-stack command and the update-stack command.

Correct Answer: C

Community vote distribution


 B (100%)

 **Digo30sp**  4 months, 4 weeks ago

Selected Answer: B

The correct answer is (B).

The --disable-rollback command-line option will prevent CloudFormation from rolling back the stack to the previous state if an error occurs. This will ensure that successfully provisioned resources are preserved.

upvoted 5 times

 **joshnort**  4 weeks ago

Selected Answer: B

It should look like this:

```
aws cloudformation create-stack --stack-name myteststack --template-body file://DOC-EXAMPLE-BUCKET.json --disable-rollback
```

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stack-failure-options.html#stack-failure-options-cli>
upvoted 2 times

 **kaes** 3 months, 1 week ago

Selected Answer: B

"Specify the disable-rollback option or on-failure DO NOTHING enumeration during a create-stack operation"
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stack-failure-options.html>

upvoted 3 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 3 times

 **kashtelyan** 4 months, 3 weeks ago

Selected Answer: B

<https://www.cloudhesive.com/blog-posts/cloudformation-disable-rollback/>
upvoted 4 times

 **fordiscussiontwo** 4 months, 4 weeks ago

BBBBBBBBBBBBBBBBBB

upvoted 3 times

Question #207

Topic 1

A developer is building a serverless application that connects to an Amazon Aurora PostgreSQL database. The serverless application consists of hundreds of AWS Lambda functions. During every Lambda function scale out, a new database connection is made that increases database resource consumption.

The developer needs to decrease the number of connections made to the database. The solution must not impact the scalability of the Lambda functions.

Which solution will meet these requirements?

- A. Configure provisioned concurrency for each Lambda function by setting the ProvisionedConcurrentExecutions parameter to 10.
- B. Enable cluster cache management for Aurora PostgreSQL. Change the connection string of each Lambda function to point to cluster cache management.
- C. Use Amazon RDS Proxy to create a connection pool to manage the database connections. Change the connection string of each Lambda function to reference the proxy.
- D. Configure reserved concurrency for each Lambda function by setting the ReservedConcurrentExecutions parameter to 10.

Correct Answer: A*Community vote distribution*

C (100%)

 **dilleman** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

C: Amazon RDS Proxy is designed to improve application scalability and resilience by pooling and reusing database connections. This can significantly reduce the number of connections each Lambda function has to establish

upvoted 5 times

 **Digo30sp** Most Recent 4 months, 4 weeks ago

Selected Answer: C

The correct answer is (C).

Amazon RDS Proxy is a solution that allows you to create a connection pool to manage database connections. This can help reduce the number of connections made to the database.

upvoted 2 times

 **fordiscussiontwo** 4 months, 4 weeks ago

CCCCCCCCCC

upvoted 3 times

Question #208

Topic 1

A developer is preparing to begin development of a new version of an application. The previous version of the application is deployed in a production environment. The developer needs to deploy fixes and updates to the current version during the development of the new version of the application. The code for the new version of the application is stored in AWS CodeCommit.

Which solution will meet these requirements?

- A. From the main branch, create a feature branch for production bug fixes. Create a second feature branch from the main branch for development of the new version.
- B. Create a Git tag of the code that is currently deployed in production. Create a Git tag for the development of the new version. Push the two tags to the CodeCommit repository.
- C. From the main branch, create a branch of the code that is currently deployed in production. Apply an IAM policy that ensures no other users can push or merge to the branch.
- D. Create a new CodeCommit repository for development of the new version of the application. Create a Git tag for the development of the new version.

Correct Answer: A

Community vote distribution



A (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

The best option here is:

- A. From the main branch, create a feature branch for production bug fixes. Create a second feature branch from the main branch for development of the new version.

Here's why this solution is the most suitable:

Separation of Concerns: Creating separate branches for bug fixes and new feature development ensures that changes made for the current production version and the new version do not interfere with each other. This separation is crucial to avoid introducing new bugs into the production version from the development version.

Continuous Integration and Delivery (CI/CD): This approach supports CI/CD practices. Bug fixes can be developed, tested, and merged into the main branch and deployed without impacting the ongoing development of the new version.

upvoted 1 times

 **dilleman** 4 months, 3 weeks ago

Selected Answer: A

A is a common code version control strategy

upvoted 3 times

 **Digo30sp** 4 months, 4 weeks ago

Selected Answer: A

A resposta correta é (A).

Criar uma ramificação de recursos para correções de bugs de produção e uma segunda ramificação de recursos para desenvolvimento da nova versão é a solução que atenderá a esses requisitos.

A primeira ramificação de recursos pode ser usada para corrigir bugs ou implementar atualizações para a versão atual do aplicativo. A segunda ramificação de recursos pode ser usada para desenvolver a nova versão do aplicativo.

upvoted 2 times

 **fordiscussiontwo** 4 months, 4 weeks ago

AAAAAAAAAAAAAA

upvoted 3 times

Question #209

Topic 1

A developer is creating an AWS CloudFormation stack. The stack contains IAM resources with custom names. When the developer tries to deploy the stack, they receive an InsufficientCapabilities error.

What should the developer do to resolve this issue?

- A. Specify the CAPABILITY_AUTO_EXPAND capability in the CloudFormation stack.
- B. Use an administrators role to deploy IAM resources with CloudFormation.
- C. Specify the CAPABILITY_IAM capability in the CloudFormation stack.
- D. Specify the CAPABILITY_NAMED_IAM capability in the CloudFormation stack.

Correct Answer: B

Community vote distribution

D (100%)

✉  **Digo30sp**  4 months, 4 weeks ago

Selected Answer: D

The correct answer is (D).

To deploy IAM resources with custom names, you must specify the CAPABILITY_NAMED_IAM resource in the CloudFormation stack.

The CAPABILITY_IAM resource allows CloudFormation to create and modify IAM resources. The CAPABILITY_NAMED_IAM resource allows CloudFormation to create IAM resources with custom names.

To resolve the issue, the developer must specify the CAPABILITY_NAMED_IAM resource in the CloudFormation stack.
upvoted 5 times

✉  **Learning4life**  4 months, 2 weeks ago

D.

If you have IAM resources with custom names, you must specify CAPABILITY_NAMED_IAM. See more details in this link
https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html

upvoted 4 times

✉  **dilleman** 4 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

✉  **Patel_ajay745** 4 months, 4 weeks ago

CCC

ccccccc

upvoted 1 times

✉  **fordiscussiontwo** 4 months, 4 weeks ago

DDDDDDDDDD

upvoted 3 times

Question #210

Topic 1

A company uses Amazon API Gateway to expose a set of APIs to customers. The APIs have caching enabled in API Gateway. Customers need a way to invalidate the cache for each API when they test the API.

What should a developer do to give customers the ability to invalidate the API cache?

- A. Ask the customers to use AWS credentials to call the InvalidateCache API operation.
- B. Attach an InvalidateCache policy to the IAM execution role that the customers use to invoke the API. Ask the customers to send a request that contains the Cache-Control:max-age=0 HTTP header when they make an API call.
- C. Ask the customers to use the AWS SDK API Gateway class to invoke the InvalidateCache API operation.
- D. Attach an InvalidateCache policy to the IAM execution role that the customers use to invoke the API. Ask the customers to add the INVALIDATE_CACHE query string parameter when they make an API call.

Correct Answer: D

Community vote distribution

 B (100%)

 **Digo30sp**  4 months, 4 weeks ago

Selected Answer: B

B) <https://www.examtopics.com/discussions/amazon/view/4166-exam-aws-certified-developer-associate-topic-1-question-69/>
upvoted 6 times

 **KillThemWithKindness**  1 week, 1 day ago

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html>
upvoted 1 times

 **Mimi666** 2 months, 4 weeks ago

invalidate an API Gateway cache entry

A client of your API can invalidate an existing cache entry and reload it from the integration endpoint for individual requests. The client must send a request that contains the Cache-Control: max-age=0 header. The client receives the response directly from the integration endpoint instead of the cache, provided that the client is authorized to do so. This replaces the existing cache entry with the new response, which is fetched from the integration endpoint. <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html>

upvoted 1 times

 **dezoito** 4 months, 2 weeks ago

Seems to be B but policies/roles have nothing to do with cache

upvoted 1 times

 **Patel_ajay745** 4 months, 4 weeks ago

it is DDDDDD

upvoted 1 times

 **fordiscussionstwo** 4 months, 3 weeks ago

why? because chatGPT said that? all your answers are wrong.

upvoted 5 times

 **fordiscussionstwo** 4 months, 4 weeks ago

BBBBBBBBBBBBBBB

upvoted 3 times

Question #211

Topic 1

A developer is creating an AWS Lambda function that will generate and export a file. The function requires 100 MB of temporary storage for temporary files while running. These files will not be needed after the function is complete.

How can the developer MOST efficiently handle the temporary files?

- A. Store the files in Amazon Elastic Block Store (Amazon EBS) and delete the files at the end of the Lambda function.
- B. Copy the files to Amazon Elastic File System (Amazon EFS) and delete the files at the end of the Lambda function.
- C. Store the files in the /tmp directory and delete the files at the end of the Lambda function.
- D. Copy the files to an Amazon S3 bucket with a lifecycle policy to delete the files.

Correct Answer: A

Community vote distribution

C (100%)

 **RPRAMSUBU** 3 weeks, 4 days ago

C is the correct answer

upvoted 2 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

This is the most efficient and straightforward option. AWS Lambda provides a /tmp directory in its execution environment with a storage limit of 512 MB. This space can be used for temporary storage during the function execution. Since the requirement is 100 MB, it falls well within the limits of the /tmp directory.

upvoted 1 times

 **JohnPI** 1 month, 3 weeks ago

Selected Answer: C

C is the correct answer

upvoted 1 times

 **sankhagg** 2 months, 3 weeks ago

Starting March 2022, Lambda now supports increasing /tmp directory's maximum size limit up to 10,240MB. More information available.
<https://aws.amazon.com/blogs/aws/aws-lambda-now-supports-up-to-10-gb-ephemeral-storage/>

upvoted 2 times

 **Claire_KMT** 4 months, 1 week ago

C. Store the files in the /tmp directory and delete the files at the end of the Lambda function.

The /tmp directory is a dedicated temporary storage location provided by AWS Lambda for storing temporary files during the execution of the function.

It's cost-effective and efficient because it doesn't involve additional AWS services or storage costs.

AWS Lambda automatically manages the /tmp directory for you, including clearing its contents after the function execution is complete. You don't need to explicitly delete the files; Lambda takes care of it.

upvoted 3 times

 **LemonGremlin** 4 months, 1 week ago

Selected Answer: C

Option C is the best choice for efficient handling of temporary files within an AWS Lambda function.

upvoted 2 times

Question #212

Topic 1

A company uses Amazon DynamoDB as a data store for its order management system. The company frontend application stores orders in a DynamoDB table. The DynamoDB table is configured to send change events to a DynamoDB stream. The company uses an AWS Lambda function to log and process the incoming orders based on data from the DynamoDB stream.

An operational review reveals that the order quantity of incoming orders is sometimes set to 0. A developer needs to create a dashboard that will show how many unique customers this problem affects each day.

What should the developer do to implement the dashboard?

- A. Grant the Lambda function's execution role permissions to upload logs to Amazon CloudWatch Logs. Implement a CloudWatch Logs Insights query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the CloudWatch Logs Insights query to a CloudWatch dashboard.
- B. Use Amazon Athena to query AWS CloudTrail API logs for API calls. Implement an Athena query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the Athena query to an Amazon CloudWatch dashboard.
- C. Configure the Lambda function to send events to Amazon EventBridge. Create an EventBridge rule that groups the number of unique customers for orders with order quantity equal to 0 in 1-day periods. Add a CloudWatch dashboard as the target of the rule.
- D. Turn on custom Amazon CloudWatch metrics for the DynamoDB stream of the DynamoDB table. Create a CloudWatch alarm that groups the number of unique customers for orders with order quantity equal to 0 in 1-day periods. Add the CloudWatch alarm to a CloudWatch dashboard.

Correct Answer: D

Community vote distribution

A (70%)

D (30%)

 **konieczny69** 4 weeks ago

Selected Answer: A

D is invalid. There are no such custom metrics:
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/metrics-dimensions.html>

A is the right choice
 upvoted 2 times

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

This approach involves enhancing the existing Lambda function to log relevant information about orders (especially those with order quantity 0) to CloudWatch Logs. The developer can then use CloudWatch Logs Insights to query these logs for unique customer counts and visualize this data on a CloudWatch dashboard. This solution is feasible and effective, as it leverages the existing Lambda function and CloudWatch capabilities.
 upvoted 1 times

 **Certified101** 2 months, 2 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/96212-exam-aws-certified-developer-associate-topic-1-question-402/>
 upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: D

Choose D
 Option A is more suitable for log analysis, but in this case, the issue is related to DynamoDB data, and CloudWatch Logs may not be the most efficient way to track it.
 upvoted 1 times

 **chris_777** 3 months, 1 week ago

Selected Answer: A

I choose A
 upvoted 2 times

 **bhanupriya07** 3 months, 2 weeks ago

<https://www.examtopics.com/discussions/amazon/view/96212-exam-aws-certified-developer-associate-topic-1-question-402/>
 upvoted 3 times

 **PrakashM14** 4 months ago

Selected Answer: D

Option A suggests using CloudWatch Logs Insights, which is typically used for analyzing log data. However, in this scenario, the issue is related to metrics (order quantity), and using CloudWatch Metrics and Alarms is a more suitable approach.

I'd go with option D. It seems like a more direct and efficient approach. By using custom CloudWatch metrics for the DynamoDB stream, you can specifically track the relevant data without the need for additional CloudWatch Logs Insights queries. The alarm will then allow you to easily visualize and monitor the number of unique customers affected by the issue each day on the CloudWatch dashboard.

upvoted 2 times

 **AngelinaWatson** 4 months ago

i Passed The Exam By by This Website Thankyou et lots of lov

<https://www.passexam4sure.com/>

upvoted 1 times

 **Claire_KMT** 4 months, 1 week ago

A. Grant the Lambda function's execution role permissions to upload logs to Amazon CloudWatch Logs. Implement a CloudWatch Logs Insights query that selects the number of unique customers for orders with order quantity equal to 0 and groups the results in 1-day periods. Add the CloudWatch Logs Insights query to a CloudWatch dashboard.

Here's why this option is the best choice:

CloudWatch Logs Insights is designed for querying and analyzing log data, making it well-suited for this task.

By configuring the Lambda function's execution role to upload logs to CloudWatch Logs, you ensure that the log data is available for analysis.

You can use a CloudWatch Logs Insights query to identify unique customers for orders with a quantity of 0 and group the results by day, providing the desired daily count of affected customers.

The results of the query can be added to a CloudWatch dashboard, making it easily accessible for monitoring.

upvoted 3 times

Question #213

Topic 1

A developer needs to troubleshoot an AWS Lambda function in a development environment. The Lambda function is configured in VPC mode and needs to connect to an existing Amazon RDS for SQL Server DB instance. The DB instance is deployed in a private subnet and accepts connections by using port 1433.

When the developer tests the function, the function reports an error when it tries to connect to the database.

Which combination of steps should the developer take to diagnose this issue? (Choose two.)

- A. Check that the function's security group has outbound access on port 1433 to the DB instance's security group. Check that the DB instance's security group has inbound access on port 1433 from the function's security group.
- B. Check that the function's security group has inbound access on port 1433 from the DB instance's security group. Check that the DB instance's security group has outbound access on port 1433 to the function's security group.
- C. Check that the VPC is set up for a NAT gateway. Check that the DB instance has the public access option turned on.
- D. Check that the function's execution role permissions include rds:DescribeDBInstances, rds:ModifyDBInstance, and rds:DescribeDBSecurityGroups for the DB instance.
- E. Check that the function's execution role permissions include ec2:CreateNetworkInterface, ec2:DescribeNetworkInterfaces, and ec2:DeleteNetworkInterface.

Correct Answer: AC
Community vote distribution


kaes Highly Voted 3 months, 1 week ago

Selected Answer: AE

- A: The function needs outbound access to DB and the DB needs to allow inbound access from the function
- E: The function needs AWSLambdaVPCAccessExecutionRole role to work correctly in the VPC
(<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-permissions>)

D is incorrect as the function's execution role does not need to make any of those DB actions: Describe Modify and DescribeDB security groups!
upvoted 7 times

mitch151 Highly Voted 4 months ago

I believe It's A and D. Unsure on A, but D seems to be confirmed by this link: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/lambda-rds-connect.html>
upvoted 7 times

konieczny69 Most Recent 4 weeks ago

Selected Answer: AE

AE

This is a network issue, not a governance issue, hence D is invalid.

Between A and B its an obvious choice.

C is invalid - DB is in a private subnet

upvoted 1 times

_YaWeb 1 month, 1 week ago

ChatGPT goes with A and D

upvoted 1 times

Snape 1 month, 3 weeks ago

Selected Answer: AB

inbound and outbound connection between Lambda and the RDS should be set properly.

upvoted 1 times

rrshah83 2 months ago

Selected Answer: AE

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-permissions>

upvoted 2 times

Certified101 2 months, 2 weeks ago

Selected Answer: AE

Agree with Kae

- A: The function needs outbound access to DB and the DB needs to allow inbound access from the function
- E: The function needs AWSLambdaVPCAccessExecutionRole role to work correctly in the VPC
(<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-permissions>)

D is incorrect as the function's execution role does not need to make any of those DB actions: Describe Modify and DescribeDB security groups!
upvoted 2 times

 **joshnort** 4 weeks ago

This is excellent. Thanks for the link. Makes it very clear.

upvoted 1 times

 **fimlajirki** 2 months, 2 weeks ago

itexamstest.com

no discussion ad :)

upvoted 1 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: AD

We need connection between lambda and RDS, not to VPC. So, option E is unsuitable. We can choose the related remain option like D
About option A, it's already correct.

upvoted 2 times

 **Jing2023** 4 months ago

Selected Answer: AD

A and D

upvoted 5 times

 **Claire_KMT** 4 months ago

A and B

upvoted 1 times

Question #214

Topic 1

A developer needs to launch a new Amazon EC2 instance by using the AWS CLI.

Which AWS CLI command should the developer use to meet this requirement?

- A. aws ec2 bundle-instance
- B. aws ec2 start-instances
- C. aws ec2 confirm-product-instance
- D. aws ec2 run-instances

Correct Answer: D

Community vote distribution

D (100%)

 **chris_777** Highly Voted 3 months, 1 week ago

Selected Answer: D

D. aws ec2 run-instances

Note: B aws ec2 start-instances is used to "start an instance that you've previously stopped"

upvoted 5 times

 **Claire_KMT** Highly Voted 4 months ago

D. aws ec2 run-instances

So, to create a new EC2 instance using the AWS CLI, you would typically use the aws ec2 run-instances command, providing the necessary parameters such as the AMI ID, instance type, security groups, and key pair, among others.

upvoted 5 times

Question #215

Topic 1

A developer needs to manage AWS infrastructure as code and must be able to deploy multiple identical copies of the infrastructure, stage changes, and revert to previous versions.

Which approach addresses these requirements?

- A. Use cost allocation reports and AWS OpsWorks to deploy and manage the infrastructure.
- B. Use Amazon CloudWatch metrics and alerts along with resource tagging to deploy and manage the infrastructure.
- C. Use AWS Elastic Beanstalk and AWS CodeCommit to deploy and manage the infrastructure.
- D. Use AWS CloudFormation and AWS CodeCommit to deploy and manage the infrastructure.

Correct Answer: D

Community vote distribution

D (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: D

Here's why this option is the most suitable:

AWS CloudFormation: This service allows you to model your entire infrastructure in a text file (either JSON or YAML). This infrastructure as code approach enables you to create and manage AWS resources efficiently, consistently, and repeatably. It's ideal for deploying multiple identical copies of the same infrastructure (like staging, production environments), and the text file can be version-controlled, allowing you to stage changes and revert to previous versions.

AWS CodeCommit: This is a managed source control service that hosts private Git repositories. Integrating AWS CodeCommit with CloudFormation enables version control of your infrastructure templates. This supports staging changes and reverting to previous versions, enhancing collaboration among team members.

upvoted 2 times

 **Jing2023** 4 months ago

Selected Answer: D

this is the only option mentioning infra as code.

upvoted 4 times

 **Claire_KMT** 4 months ago

D. Use AWS CloudFormation and AWS CodeCommit to deploy and manage the infrastructure.

Here's why this is the most appropriate choice:

AWS CloudFormation: It allows you to define your infrastructure as code using templates, which can be version-controlled. You can create, update, and delete stacks of AWS resources in a controlled and predictable manner. This aligns with the requirement to deploy multiple identical copies of the infrastructure, stage changes, and revert to previous versions.

AWS CodeCommit: It provides a fully managed source control service, allowing you to store and version-control your CloudFormation templates. This ensures that you can manage and track changes to your infrastructure configurations.

upvoted 4 times

Question #216

Topic 1

A developer is working on an AWS Lambda function that accesses Amazon DynamoDB. The Lambda function must retrieve an item and update some of its attributes, or create the item if it does not exist. The Lambda function has access to the primary key.

Which IAM permissions should the developer request for the Lambda function to achieve this functionality?

- A. dynamodb:DeleteItem
dynamodb:GetItem
dynamodb:PutItem
- B. dynamodb:UpdateItem
dynamodb:GetItem
dynamodb:DescribeTable
- C. dynamodb:GetRecords
dynamodb:PutItem
dynamodb:UpdateTable
- D. dynamodb:UpdateItem
dynamodb:GetItem
dynamodb:PutItem

Correct Answer: D

Community vote distribution



Claire_KMT Highly Voted 4 months ago

D. dynamodb:UpdateItem, dynamodb:GetItem, and dynamodb:PutItem

Here's why:

dynamodb:.GetItem: This permission allows the Lambda function to retrieve an item from DynamoDB.

dynamodb:UpdateItem: This permission allows the Lambda function to update the attributes of an item in DynamoDB.

dynamodb:PutItem: This permission allows the Lambda function to create a new item if it doesn't already exist in the DynamoDB table.
upvoted 5 times

Snape Most Recent 1 month, 3 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

rrshah83 2 months ago

Selected Answer: B

x A: as delete is not required. Plus Put item is not required, update lets you create a new item if it doesn't already exist

B: meets requirements. DescribeTable helps provide a list of attributes that can be used to update.

x C: put not required; getrecords does not exist

x D: put not required.

upvoted 1 times

fimlajirki 2 months, 2 weeks ago

Selected Answer: D

itexamstest.com

no dissussion D :)

upvoted 1 times

TanTran04 2 months, 2 weeks ago

Selected Answer: D

UpdateItem: Edits an existing item's attributes

https://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_UpdateItem.html

GetItem: retrieves attributes from the Thread table

https://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_GetItem.html#API_GetItem_Examples

PutItem: Creates a new item, or replaces an old item with a new item.

https://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_PutItem.html

upvoted 2 times

 **didorins** 4 months ago

Selected Answer: D

PutItem is to CREATE new item or replace old item with new item
GetItem is to retrieve an item
UpdateItem so to update the attributes

Hence answer D
upvoted 4 times

Question #217

Topic 1

A developer has built a market application that stores pricing data in Amazon DynamoDB with Amazon ElastiCache in front. The prices of items in the market change frequently. Sellers have begun complaining that, after they update the price of an item, the price does not actually change in the product listing.

What could be causing this issue?

- A. The cache is not being invalidated when the price of the item is changed.
- B. The price of the item is being retrieved using a write-through ElastiCache cluster.
- C. The DynamoDB table was provisioned with insufficient read capacity.
- D. The DynamoDB table was provisioned with insufficient write capacity.

Correct Answer: A

Community vote distribution

A (100%)

 **Certified101** 2 months, 2 weeks ago

Selected Answer: A

A is correct
upvoted 2 times

 **kaes** 3 months, 1 week ago

Selected Answer: A

ANS: A
The cache needs to be invalidated. The write-through approach could be helpful here
upvoted 2 times

 **Claire_KMT** 4 months ago

A. The cache is not being invalidated when the price of the item is changed.

In a caching setup using Amazon ElastiCache in front of Amazon DynamoDB, if the cache is not being invalidated or updated when data in DynamoDB is changed, it can result in stale data being served from the cache, leading to the observed behavior.

To resolve this issue, you should implement a mechanism to invalidate or update the cache whenever the price of an item is changed in DynamoDB to ensure that the most up-to-date data is retrieved from the cache or DynamoDB.

upvoted 4 times

Question #218

Topic 1

A company requires that all applications running on Amazon EC2 use IAM roles to gain access to AWS services. A developer is modifying an application that currently relies on IAM user access keys stored in environment variables to access Amazon DynamoDB tables using boto, the AWS SDK for Python.

The developer associated a role with the same permissions as the IAM user to the EC2 instance, then deleted the IAM user. When the application was restarted, the AWS AccessDeniedException messages started appearing in the application logs. The developer was able to use their personal account on the server to run DynamoDB API commands using the AWS CLI.

What is the MOST likely cause of the exception?

- A. IAM policies might take a few minutes to propagate to resources.
- B. Disabled environment variable credentials are still being used by the application.
- C. The AWS SDK does not support credentials obtained using an instance role.
- D. The instance's security group does not allow access to http://169.254.169.254.

Correct Answer: B

Community vote distribution

B (100%)

 **Claire_KMT** 4 months ago

B. Disabled environment variable credentials are still being used by the application.
upvoted 3 times

 **didorins** 4 months ago

Selected Answer: B
B is the only viable answer.
upvoted 4 times

Question #219

Topic 1

A company has an existing application that has hardcoded database credentials. A developer needs to modify the existing application. The application is deployed in two AWS Regions with an active-passive failover configuration to meet company's disaster recovery strategy.

The developer needs a solution to store the credentials outside the code. The solution must comply with the company's disaster recovery strategy.

Which solution will meet these requirements in the MOST secure way?

- A. Store the credentials in AWS Secrets Manager in the primary Region. Enable secret replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.
- B. Store credentials in AWS Systems Manager Parameter Store in the primary Region. Enable parameter replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.
- C. Store credentials in a config file. Upload the config file to an S3 bucket in the primary Region. Enable Cross-Region Replication (CRR) to an S3 bucket in the secondary region. Update the application to access the config file from the S3 bucket, based on the Region.
- D. Store credentials in a config file. Upload the config file to an Amazon Elastic File System (Amazon EFS) file system. Update the application to use the Amazon EFS file system Regional endpoints to access the config file in the primary and secondary Regions.

Correct Answer: A

Community vote distribution

A (100%)

 **didorins**  4 months ago

Selected Answer: A

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/create-manage-multi-region-secrets.html>

upvoted 9 times

 **kaes**  3 months, 1 week ago

Selected Answer: A

Must be A. The Secret Manager supports region replication out-of-the-box in contrast to the Parameter Store which doesn't support it.

upvoted 3 times

 **Claire_KMT** 4 months ago

B. Store credentials in AWS Systems Manager Parameter Store in the primary Region. Enable parameter replication to the secondary Region. Update the application to use the Amazon Resource Name (ARN) based on the Region.

upvoted 2 times

Question #220

Topic 1

A developer is receiving HTTP 400: ThrottlingException errors intermittently when calling the Amazon CloudWatch API. When a call fails, no data is retrieved.

What best practice should first be applied to address this issue?

- A. Contact AWS Support for a limit increase.
- B. Use the AWS CLI to get the metrics.
- C. Analyze the applications and remove the API call.
- D. Retry the call with exponential backoff.

Correct Answer: D

Community vote distribution



✉ **didorins** 4 months ago

Selected Answer: D

Because examtopic won't allow me to modify my previous answer to use the correct option. Exponential Backoff is D
upvoted 5 times

✉ **SerialiDr** 1 month, 1 week ago

Selected Answer: D

D. Retry the call with exponential backoff is the recommended best practice in this scenario. Exponential backoff is a standard error-handling strategy for network applications in which the client progressively increases the wait time between retries, up to a maximum number of retries, when a request fails due to server-side throttling. This approach helps to smooth out the rate of API calls, reducing the likelihood of hitting the rate limit.

upvoted 2 times

✉ **vruizrob** 4 months ago

D. Retries with exponential backoff; operation with an exponentially increasing wait time
upvoted 4 times

✉ **Claire_KMT** 4 months ago

D. Retry the call with exponential backoff.
upvoted 4 times

✉ **didorins** 4 months ago

Selected Answer: A

You are doing too many requests. Try less frequent with exponential backoff.
upvoted 1 times

Question #221

Topic 1

An application needs to use the IP address of the client in its processing. The application has been moved into AWS and has been placed behind an Application Load Balancer (ALB). However, all the client IP addresses now appear to be the same. The application must maintain the ability to scale horizontally.

Based on this scenario, what is the MOST cost-effective solution to this problem?

- A. Remove the application from the ALB. Delete the ALB and change Amazon Route 53 to direct traffic to the instance running the application.
- B. Remove the application from the ALB and create a Classic Load Balancer in its place. Direct traffic to the application using the HTTP protocol.
- C. Alter the application code to inspect the X-Forwarded-For header. Ensure that the code can work properly if a list of IP addresses is passed in the header.
- D. Alter the application code to inspect a custom header. Alter the client code to pass the IP address in the custom header.

Correct Answer: C

Community vote distribution


 C (100%)

✉️  **SerialiDr** 1 month, 1 week ago

Selected Answer: C

Use a Classic Load Balancer with HTTP protocol: While a Classic Load Balancer would also add the X-Forwarded-For header, there's no significant benefit in switching from an Application Load Balancer (ALB) to a Classic Load Balancer for this purpose. ALBs are generally preferred for application layer (HTTP/HTTPS) load balancing due to their advanced routing capabilities and other features.

upvoted 1 times

✉️  **SerialiDr** 1 month, 1 week ago

C. Inspect the X-Forwarded-For header: This is the most appropriate solution. The X-Forwarded-For header is added by ALBs (and other types of load balancers) to HTTP requests and contains the original IP address of the client. Modifying the application to use this header allows it to obtain the client's IP address without removing the benefits of load balancing.

upvoted 1 times

✉️  **Claire_KMT** 4 months ago

C. Alter the application code to inspect the X-Forwarded-For header. Ensure that the code can work properly if a list of IP addresses is passed in the header.

upvoted 1 times

✉️  **didorins** 4 months ago

Selected Answer: C

If you need to see external IP address and your app is behind ALB, always use x-forwarded-for
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/x-forwarded-headers.html>

upvoted 3 times

Question #222

Topic 1

A developer is designing a serverless application that customers use to select seats for a concert venue. Customers send the ticket requests to an Amazon API Gateway API with an AWS Lambda function that acknowledges the order and generates an order ID. The application includes two additional Lambda functions: one for inventory management and one for payment processing. These two Lambda functions run in parallel and write the order to an Amazon Dynamo DB table.

The application must provide seats to customers according to the following requirements. If a seat is accidentally sold more than once, the first order that the application received must get the seat. In these cases, the application must process the payment for only the first order. However, if the first order is rejected during payment processing, the second order must get the seat. In these cases, the application must process the payment for the second order.

Which solution will meet these requirements?

- A. Send the order ID to an Amazon Simple Notification Service (Amazon SNS) FIFO topic that fans out to one Amazon Simple Queue Service (Amazon SQS) FIFO queue for inventory management and another SQS FIFO queue for payment processing.
- B. Change the Lambda function that generates the order ID to initiate the Lambda function for inventory management. Then initiate the Lambda function for payment processing.
- C. Send the order ID to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the Lambda functions for inventory management and payment processing to the topic.
- D. Deliver the order ID to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda functions for inventory management and payment processing to poll the queue.

Correct Answer: A
Community vote distribution


MarkTpTTT55 Highly Voted 4 months ago

Selected Answer: A

- A. The only viable solution
upvoted 7 times

SerialiDr Most Recent 1 month, 1 week ago

Selected Answer: A

Here's why this solution is most appropriate:

SNS FIFO Topic: A First-In-First-Out (FIFO) SNS topic ensures that messages are delivered in the exact order they are sent. This is critical for maintaining the order of ticket requests.

SQS FIFO Queues: By having two separate FIFO queues for inventory management and payment processing, the application can process these aspects in parallel while still maintaining the order integrity. The FIFO nature of the queues ensures that if a seat is sold more than once, the first order received is processed first.

Order Processing Logic: With this setup, if the first order is rejected during payment processing, the second order can be processed next. The sequential processing inherent in FIFO queues ensures that this logic can be correctly implemented.

upvoted 2 times

Claire_KMT 4 months ago

Selected Answer: D

- D. Deliver the order ID to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda functions for inventory management and payment processing to poll the queue.
upvoted 2 times

Claire_KMT 4 months ago

- D. Deliver the order ID to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda functions for inventory management and payment processing to poll the queue.
upvoted 1 times

Question #223

Topic 1

An application uses AWS X-Ray to generate a large amount of trace data on an hourly basis. A developer wants to use filter expressions to limit the returned results through user-specified custom attributes.

How should the developer use filter expressions to filter the results in X-Ray?

- A. Add custom attributes as annotations in the segment document.
- B. Add custom attributes as metadata in the segment document.
- C. Add custom attributes as new segment fields in the segment document.
- D. Create new sampling rules that are based on custom attributes.

Correct Answer: A

Community vote distribution

A (73%)

B (27%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

Annotations in AWS X-Ray are key-value pairs that are indexed for use with filter expressions. This means that you can use annotations to add custom attributes to your trace data, which can then be queried using X-Ray filter expressions. Annotations are used for values that you want to use for searching, filtering, or creating groups. By adding these custom attributes as annotations, the developer can effectively use filter expressions to limit the returned results based on these attributes.

upvoted 1 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-java-segment.html>
filter expressions => annotations

upvoted 1 times

 **Jeff1719** 3 months ago

Selected Answer: A

Annotations are indexed, used for filtering, unlike metadata
upvoted 3 times

 **jingle4944** 3 months, 3 weeks ago

Selected Answer: A

If you add annotations with the X-Ray SDK, you can also filter based on the presence of an annotation key or the value of a key.
<https://docs.aws.amazon.com/xray/latest/devguide/xray-console-filters.html>
upvoted 2 times

 **PrakashM14** 4 months ago

Selected Answer: A

To filter the results in AWS X-Ray using custom attributes, the developer should add custom attributes as annotations in the segment document.
upvoted 1 times

 **Claire_KMT** 4 months ago

Selected Answer: B

B. Add custom attributes as metadata in the segment document.

Custom attributes are best added as metadata in the segment document because X-Ray filter expressions can use metadata to filter traces. Annotations and new segment fields are not typically used for filtering traces in this context.
upvoted 3 times

 **Claire_KMT** 4 months ago

B. Add custom attributes as metadata in the segment document.

Custom attributes are best added as metadata in the segment document because X-Ray filter expressions can use metadata to filter traces. Annotations and new segment fields are not typically used for filtering traces in this context.
upvoted 1 times

Question #224

Topic 1

A web application is using Amazon Kinesis Data Streams for clickstream data that may not be consumed for up to 12 hours.

How can the developer implement encryption at rest for data within the Kinesis Data Streams?

- A. Enable SSL connections to Kinesis.
- B. Use Amazon Kinesis Consumer Library.
- C. Encrypt the data once it is at rest with a Lambda function.
- D. Enable server-side encryption in Kinesis Data Streams.

Correct Answer: D

Community vote distribution

D (100%)

 **didorins**  4 months ago

Selected Answer: D

<https://docs.aws.amazon.com/streams/latest/dev/server-side-encryption.html>

upvoted 5 times

 **Claire_KMT**  4 months ago

Selected Answer: D

D. Enable server-side encryption in Kinesis Data Streams.

Amazon Kinesis Data Streams allows you to enable server-side encryption, which encrypts data at rest. This ensures that data stored within the Kinesis Data Streams is protected with encryption.

upvoted 4 times

 **Claire_KMT** 4 months ago

D. Enable server-side encryption in Kinesis Data Streams.

Amazon Kinesis Data Streams allows you to enable server-side encryption, which encrypts data at rest. This ensures that data stored within the Kinesis Data Streams is protected with encryption.

upvoted 3 times

Question #225

Topic 1

An application is real-time processing millions of events that are received through an API.

What service could be used to allow multiple consumers to process the data concurrently and MOST cost-effectively?

- A. Amazon SNS with fanout to an SQS queue for each application
- B. Amazon SNS with fanout to an SQS FIFO (first-in, first-out) queue for each application
- C. Amazon Kinesis Firehose
- D. Amazon Kinesis Data Streams

Correct Answer: D

Community vote distribution

D (100%)

✉️  **SerialiDr** 1 month, 1 week ago

Selected Answer: D

This service is specifically designed for real-time processing of large-scale streaming data. Kinesis Data Streams allows multiple consumers to process the same stream concurrently, making it highly suitable for scenarios where you have high-volume data streams that need to be processed in real-time by various applications. It offers high throughput, scalability, and durability for streaming data, and enables multiple applications to process the same stream concurrently, making it the most cost-effective and efficient choice for this scenario.

upvoted 2 times

✉️  **Claire_KMT** 4 months ago

D. Amazon Kinesis Data Streams.

Amazon Kinesis Data Streams is designed for real-time data streaming and allows multiple consumers to process data concurrently and in real-time. It can handle millions of events and provides a scalable and cost-effective solution for handling high-throughput data streams.

upvoted 2 times

✉️  **didorins** 4 months ago

Selected Answer: D

Real-time data processing is KDS

upvoted 4 times

Question #226

Topic 1

Given the following AWS CloudFormation template:

Description: Creates a new Amazon S3 bucket for shared content. Uses a random bucket name to avoid conflicts.

Resources:

```
ContentBucket:
  Type: AWS::S3::Bucket
```

Outputs:

```
ContentBucketName:
  Value: !Ref ContentBucket
```

What is the MOST efficient way to reference the new Amazon S3 bucket from another AWS CloudFormation template?

- A. Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.
- B. Add Exported: true to the Content.Bucket in the original template and use ImportResource in other templates.
- C. Create a custom AWS CloudFormation resource that gets the bucket name from the ContentBucket resource of the first stack.
- D. Use Fn::Include to include the existing template in other templates and use the ContentBucket resource directly.

Correct Answer: A

Community vote distribution



A (100%)

 **bhanupriya07** 3 months, 2 weeks ago

Selected Answer: A

- A. Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.
upvoted 3 times

 **Claire_KMT** 4 months ago

- A. Add an Export declaration to the Outputs section of the original template and use ImportValue in other templates.
upvoted 2 times

 **papason** 4 months ago

By adding an Export declaration to the Outputs section of the original CloudFormation template, you can make the bucket name available for other templates to import and use. This allows you to reference the bucket name directly in other templates without the need for additional resources or custom logic.

upvoted 2 times

Question #227

Topic 1

A developer has built an application that inserts data into an Amazon DynamoDB table. The table is configured to use provisioned capacity. The application is deployed on a burstable nano Amazon EC2 instance. The application logs show that the application has been failing because of a ProvisionedThroughputExceededException error.

Which actions should the developer take to resolve this issue? (Choose two.)

- A. Move the application to a larger EC2 instance.
- B. Increase the number of read capacity units (RCUs) that are provisioned for the DynamoDB table.
- C. Reduce the frequency of requests to DynamoDB by implementing exponential backoff.
- D. Increase the frequency of requests to DynamoDB by decreasing the retry delay.
- E. Change the capacity mode of the DynamoDB table from provisioned to on-demand.

Correct Answer: CE

Community vote distribution



✉️ **SerialiDr** 1 month, 1 week ago

Selected Answer: BC

B. This error indicates that the application's request rate is exceeding the throughput that has been provisioned for the table. Increasing the provisioned read capacity units (RCUs) and/or write capacity units (WCUs) for the DynamoDB table will allow it to handle a higher request rate, thereby reducing the likelihood of encountering this error. However, this approach requires careful capacity planning and may increase costs.

C. Exponential backoff is a standard error retry strategy that involves progressively increasing the delay between retries when there is a ProvisionedThroughputExceededException. This approach helps to smooth out the rate of requests, giving the table time to accommodate bursts of read or write requests. Implementing exponential backoff in the application will help to effectively manage request retries and reduce the chance of continually hitting the provisioned throughput limit.

upvoted 2 times

✉️ **Certified101** 2 months, 2 weeks ago

Selected Answer: CE

C & E correct

upvoted 2 times

✉️ **tqiu654** 2 months, 3 weeks ago

Selected Answer: BC

Based on ChatGPT: BC

upvoted 1 times

✉️ **bhanupriya07** 3 months, 2 weeks ago

Selected Answer: CE

C. Reduce the frequency of requests to DynamoDB by implementing exponential backoff.

E. Change the capacity mode of the DynamoDB table from provisioned to on-demand.

upvoted 4 times

✉️ **Claire_KMT** 4 months ago

B. Increase the number of read capacity units (RCUs) that are provisioned for the DynamoDB table.

OR

E. Change the capacity mode of the DynamoDB table from provisioned to on-demand.

C. Reduce the frequency of requests to DynamoDB by implementing exponential backoff.

upvoted 1 times

✉️ **tapan666** 4 months ago

It 'inserts' data, so it needs WCUs and not RCUs. So option B is invalid too. C and E are the correct options.

upvoted 5 times

Question #228

Topic 1

A company is hosting a workshop for external users and wants to share the reference documents with the external users for 7 days. The company stores the reference documents in an Amazon S3 bucket that the company owns.

What is the MOST secure way to share the documents with the external users?

- A. Use S3 presigned URLs to share the documents with the external users. Set an expiration time of 7 days.
- B. Move the documents to an Amazon WorkDocs folder. Share the links of the WorkDocs folder with the external users.
- C. Create temporary IAM users that have read-only access to the S3 bucket. Share the access keys with the external users. Expire the credentials after 7 days.
- D. Create a role that has read-only access to the S3 bucket. Share the Amazon Resource Name (ARN) of this role with the external users.

Correct Answer: A

Community vote distribution

A (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: A

Presigned URLs are a secure way to provide temporary access to specific objects in an S3 bucket. By generating a presigned URL, you grant time-limited access to the files without having to alter the underlying permissions of the S3 bucket or objects. You can set an expiration time for the URL, ensuring that access to the document is automatically revoked after 7 days. This method is straightforward and does not require the management of user identities or permissions beyond the scope of the shared objects.

upvoted 2 times

 **Claire_KMT** 4 months ago

A. Use S3 presigned URLs to share the documents with the external users. Set an expiration time of 7 days.

upvoted 2 times

 **didorins** 4 months ago

Selected Answer: A

Temporary access to S3 object to external users is Pre-signed URL

upvoted 4 times

Question #229

Topic 1

A developer is planning to use an Amazon API Gateway and AWS Lambda to provide a REST API. The developer will have three distinct environments to manage: development, test, and production.

How should the application be deployed while minimizing the number of resources to manage?

- A. Create a separate API Gateway and separate Lambda function for each environment in the same Region.
- B. Assign a Region for each environment and deploy API Gateway and Lambda to each Region.
- C. Create one API Gateway with multiple stages with one Lambda function with multiple aliases.
- D. Create one API Gateway and one Lambda function, and use a REST parameter to identify the environment.

Correct Answer: C

Community vote distribution

C (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

This approach involves creating a single API Gateway and a single Lambda function. Within the API Gateway, you can create multiple stages, each corresponding to a different environment (development, test, production). Similarly, for the Lambda function, you can create multiple aliases, each pointing to a different version of the Lambda function that corresponds to each environment. This setup allows for clear separation of environments within the same set of resources. It simplifies deployment and management by reducing the number of resources and also provides an easy way to promote changes from one environment to another.

upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: C

API Gateway

A stage in API Gateway represents a deployment of your API. You can have separate stages for development, test, and production. Each stage can have its own settings, such as stage variables, custom domains, and caching configurations.

Lambda function

Each alias can point to a specific version of your Lambda function. This allows you to promote versions through different environments without changing the function's Amazon Resource Name (ARN) in your API Gateway.

upvoted 2 times

 **bhanupriya07** 3 months, 2 weeks ago

Selected Answer: C

C. Create one API Gateway with multiple stages with one Lambda function with multiple aliases.

upvoted 4 times

 **Claire_KMT** 4 months ago

C. Create one API Gateway with multiple stages with one Lambda function with multiple aliases.

upvoted 3 times

Question #230

Topic 1

A developer registered an AWS Lambda function as a target for an Application Load Balancer (ALB) using a CLI command. However, the Lambda function is not being invoked when the client sends requests through the ALB.

Why is the Lambda function not being invoked?

- A. A Lambda function cannot be registered as a target for an ALB.
- B. A Lambda function can be registered with an ALB using AWS Management Console only.
- C. The permissions to invoke the Lambda function are missing.
- D. Cross-zone is not enabled on the ALB.

Correct Answer: C

Community vote distribution

C (100%)

 **SerialiDr** 1 month, 1 week ago

Selected Answer: C

To allow an ALB to invoke a Lambda function, you need to grant the ALB permission to invoke the Lambda. This is typically done by adding a resource-based policy to the Lambda function, granting invoke permission to the ALB. If this permission is not set, the ALB will not be able to trigger the Lambda function in response to incoming requests.

upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: C

The Lambda function must have the lambda:InvokeFunction permission for the ALB to successfully invoke it.

upvoted 3 times

 **kaes** 3 months, 1 week ago

Selected Answer: C

ANS: C

upvoted 3 times

 **Claire_KMT** 4 months ago

C. The permissions to invoke the Lambda function are missing.

upvoted 3 times

Question #231

Topic 1

A developer is creating an AWS Lambda function that will connect to an Amazon RDS for MySQL instance. The developer wants to store the database credentials. The database credentials need to be encrypted and the database password needs to be automatically rotated.

Which solution will meet these requirements?

- A. Store the database credentials as environment variables for the Lambda function. Set the environment variables to rotate automatically.
- B. Store the database credentials in AWS Secrets Manager. Set up managed rotation on the database credentials.
- C. Store the database credentials in AWS Systems Manager Parameter Store as secure string parameters. Set up managed rotation on the parameters.
- D. Store the database credentials in the X-Amz-Security-Token parameter. Set up managed rotation on the parameter.

Correct Answer: B

Community vote distribution

B (100%)

 **Claire_KMT**  4 months ago

B. Store the database credentials in AWS Secrets Manager. Set up managed rotation on the database credentials.
upvoted 5 times

 **Certified101**  2 months, 2 weeks ago

Selected Answer: B
BBBBBBBBBBB
upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

Selected Answer: B
automatically rotated => AWS Secrets Manager
upvoted 2 times

Question #232

Topic 1

A developer wants to reduce risk when deploying a new version of an existing AWS Lambda function. To test the Lambda function, the developer needs to split the traffic between the existing version and the new version of the Lambda function.

Which solution will meet these requirements?

- A. Configure a weighted routing policy in Amazon Route 53. Associate the versions of the Lambda function with the weighted routing policy.
- B. Create a function alias. Configure the alias to split the traffic between the two versions of the Lambda function.
- C. Create an Application Load Balancer (ALB) that uses the Lambda function as a target. Configure the ALB to split the traffic between the two versions of the Lambda function.
- D. Create the new version of the Lambda function as a Lambda layer on the existing version. Configure the function to split the traffic between the two layers.

Correct Answer: B

Community vote distribution

B (100%)

 **Snape** 1 month, 3 weeks ago

Selected Answer: B

This approach is more efficient and cost-effective than other options such as configuring a weighted routing policy in Amazon Route 53, creating an Application Load Balancer (ALB) that uses the Lambda function as a target, or creating the new version of the Lambda function as a Lambda layer on the existing version

upvoted 2 times

 **BronJames** 3 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/88419-exam-aws-certified-developer-associate-topic-1-question-350/>

upvoted 3 times

 **Claire_KMT** 4 months ago

B. Create a function alias. Configure the alias to split the traffic between the two versions of the Lambda function.

upvoted 2 times

Question #233

Topic 1

A developer has created a large AWS Lambda function. Deployment of the function is failing because of an `InvalidParameterValueException` error. The error message indicates that the unzipped size of the function exceeds the maximum supported value.

Which actions can the developer take to resolve this error? (Choose two.)

- A. Submit a quota increase request to AWS Support to increase the function to the required size.
- B. Use a compression algorithm that is more efficient than ZIP.
- C. Break up the function into multiple smaller functions.
- D. Zip the .zip file twice to compress the file more.
- E. Move common libraries, function dependencies, and custom runtimes into Lambda layers.

Correct Answer: CE

Community vote distribution

CE (67%) AD (17%) AE (17%)

✉️  **SerialiDr** 1 month ago

Selected Answer: CE

C. Break up the function into multiple smaller functions.

If the size of the Lambda function is too large, breaking it into smaller, more modular functions can help. Each function can be responsible for a specific part of the application's logic. This approach not only helps with deployment but also aligns with microservices best practices, potentially improving the maintainability and scalability of the application.

E. Move common libraries, function dependencies, and custom runtimes into Lambda layers.

Lambda layers are a way to manage and share common components across multiple Lambda functions. By moving libraries, dependencies, and runtimes into layers, you reduce the size of the Lambda function's deployment package. Layers can be shared across multiple functions, leading to more efficient use of storage and easier management of common code.

upvoted 2 times

✉️  **Snape** 1 month, 3 weeks ago

Selected Answer: CE

C and E

upvoted 2 times

✉️  **nickqq** 1 month, 3 weeks ago

A E no discussion

upvoted 2 times

✉️  **kipr** 2 months ago

C and E

<https://www.examtopics.com/discussions/amazon/view/5330-exam-aws-certified-developer-associate-topic-1-question-17/>

upvoted 2 times

✉️  **Certified101** 2 months, 2 weeks ago

Selected Answer: AD

A & E is correct

upvoted 1 times

✉️  **TanTran04** 2 months, 2 weeks ago

Selected Answer: AE

Following anasbakla document, we can see the default storage of Quota is 75 GB for uploaded functions (.zip file archives) and layers.

upvoted 1 times

✉️  **anasbakla** 3 months, 2 weeks ago

A and E

<https://docs.aws.amazon.com/lambda/latest/dg/gettingstarted-limits.html>

upvoted 2 times

Question #234

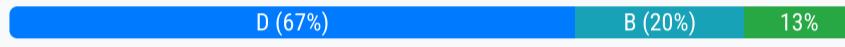
Topic 1

A developer is troubleshooting an application in an integration environment. In the application, an Amazon Simple Queue Service (Amazon SQS) queue consumes messages and then an AWS Lambda function processes the messages. The Lambda function transforms the messages and makes an API call to a third-party service.

There has been an increase in application usage. The third-party API frequently returns an HTTP 429 Too Many Requests error message. The error message prevents a significant number of messages from being processed successfully.

How can the developer resolve this issue?

- A. Increase the SQS event source's batch size setting.
- B. Configure provisioned concurrency for the Lambda function based on the third-party API's documented rate limits.
- C. Increase the retry attempts and maximum event age in the Lambda function's asynchronous configuration.
- D. Configure maximum concurrency on the SQS event source based on the third-party service's documented rate limits.

Correct Answer: A*Community vote distribution*

nickolaj Highly Voted 3 months, 1 week ago

Selected Answer: D

<https://aws.amazon.com/about-aws/whats-new/2023/01/aws-lambda-maximum-concurrency-amazon-sqs-event-source/>
upvoted 8 times

SerialiDr Most Recent 1 month ago

Selected Answer: D

By setting the maximum concurrency on the SQS event source, the developer can control the number of Lambda functions executing concurrently. This approach ensures that the rate of API calls does not exceed the rate limits set by the third-party service, thereby reducing the likelihood of encountering the HTTP 429 error. Adjusting the concurrency settings allows for better control of the throughput to match the API's capacity.
upvoted 2 times

Snape 1 month, 3 weeks ago

Selected Answer: B

The developer can configure provisioned concurrency for the Lambda function based on the third-party API's documented rate limits. This can help to ensure that the function has sufficient concurrency to handle the incoming messages and make API calls without exceeding the rate limits of the third-party service

upvoted 1 times

AMEJack 3 months, 3 weeks ago

Selected Answer: C

Provisioned concurrency will not solve the problem as the number of instances can increase till it reaches the max number of unreserved limit (this is not reserved concurrency).

upvoted 1 times

PrakashM14 4 months ago

Selected Answer: B

Option B addresses the issue by configuring provisioned concurrency for the Lambda function. Provisioned concurrency ensures that a specified number of concurrent executions of the Lambda function are always available. This can help in managing the third-party API rate limits by controlling the number of simultaneous requests made to the API. By setting the provisioned concurrency to a value that aligns with the third-party API's rate limits, you can avoid exceeding those limits and reduce the occurrence of HTTP 429 errors.

upvoted 2 times

Jing2023 4 months ago

Selected Answer: C

A. increase the batch size does not change how many items being processed.

C is from

Configuring error handling for asynchronous invocation — You can set it up when creating the lambda.

Maximum age of event — The maximum amount of time Lambda retains an event in the asynchronous event queue, up to 6 hours.

Retry attempts — The number of times Lambda retries when the function returns an error, between 0 and 2.

upvoted 1 times

Claire_KMT 4 months ago

- B. Configure provisioned concurrency for the Lambda function based on the third-party API's documented rate limits.
upvoted 2 times

Question #235

Topic 1

A company has a three-tier application that is deployed in Amazon Elastic Container Service (Amazon ECS). The application is using an Amazon RDS for MySQL DB instance. The application performs more database reads than writes.

During times of peak usage, the application's performance degrades. When this performance degradation occurs, the DB instance's ReadLatency metric in Amazon CloudWatch increases suddenly.

How should a developer modify the application to improve performance?

- A. Use Amazon ElastiCache to cache query results.
- B. Scale the ECS cluster to contain more ECS instances.
- C. Add read capacity units (RCUs) to the DB instance.
- D. Modify the ECS task definition to increase the task memory.

Correct Answer: A

Community vote distribution

A (100%)

SerialiDr 1 month ago

Selected Answer: A

Amazon ElastiCache can significantly enhance the read performance of the application by caching frequently accessed data. This reduces the load on the RDS database by serving repeated read requests from the cache rather than querying the database each time. This is particularly effective for applications with a high read-to-write ratio and can lead to a substantial reduction in the ReadLatency metric of the database.

upvoted 2 times

kaes 3 months, 1 week ago

Selected Answer: A

ANS: A

upvoted 2 times

Claire_KMT 4 months ago

A. Use Amazon ElastiCache to cache query results.

upvoted 2 times

Question #236

Topic 1

A company has an online web application that includes a product catalog. The catalog is stored in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The application must be able to list the objects in the S3 bucket and must be able to download objects through an IAM policy.

Which policy allows MINIMUM access to meet these requirements?

- A.
- ```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Allow",
 "Action": [
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```
- B.
- ```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:)"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    }
  ]
}
```
- C.
- ```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "s3:GetObject",
 "s3:PutObject",
 "s3:DeleteObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "s3>ListBucket",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
 },
 {
 "Effect": "Deny",
 "Action": [
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
 }
]
}
```

**Correct Answer: A***Community vote distribution* A (100%)

 **Certified101** 2 months, 2 weeks ago

**Selected Answer: A**

A is the correct answer

upvoted 2 times

 **kaes** 3 months, 1 week ago

**Selected Answer: A**

ANS: A

upvoted 2 times

 **Claire\_KMT** 4 months ago

A is the correct answer.

upvoted 3 times

## Question #237

## Topic 1

A developer is writing an application to encrypt files outside of AWS before uploading the files to an Amazon S3 bucket. The encryption must be symmetric and must be performed inside the application.

How can the developer implement the encryption in the application to meet these requirements?

- A. Create a data key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.
- B. Create a Hash-Based Message Authentication Code (HMAC) key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.
- C. Create a data key pair in AWS Key Management Service (AWS KMS). Use the AWS CLI to encrypt the files.
- D. Create a data key in AWS Key Management Service (AWS KMS). Use the AWS CLI to encrypt the files.

**Correct Answer: A***Community vote distribution*A (100%)

SerialiDr 1 month ago

**Selected Answer: A**

This option aligns with the requirements. AWS KMS allows the creation of symmetric data keys which can be used for encryption outside of AWS. The AWS Encryption SDK is designed to simplify encryption and decryption operations, making it a suitable choice for implementing encryption within the application. The developer can use the data key obtained from AWS KMS for the encryption process.

upvoted 2 times

Certified101 2 months, 2 weeks ago

**Selected Answer: A**

AAAAAA

upvoted 2 times

Jing2023 4 months ago

**Selected Answer: A**

C and D cannot make it within the application.

upvoted 3 times

Claire\_KMT 4 months ago

A. Create a data key in AWS Key Management Service (AWS KMS). Use the AWS Encryption SDK to encrypt the files.

upvoted 3 times

## Question #238

## Topic 1

A developer is working on an application that is deployed on an Amazon EC2 instance. The developer needs a solution that will securely transfer files from the application to an Amazon S3 bucket.

What should the developer do to meet these requirements in the MOST secure way?

- A. Create an IAM user. Create an access key for the IAM user. Store the access key in the application's environment variables.
- B. Create an IAM role. Create an access key for the IAM role. Store the access key in the application's environment variables.
- C. Create an IAM role. Configure the IAM role to access the specific Amazon S3 API calls the application requires. Associate the IAM role with the EC2 instance.
- D. Configure an S3 bucket policy for the S3 bucket. Configure the S3 bucket policy to allow access for the EC2 instance ID.

**Correct Answer: B**

*Community vote distribution*



C (100%)

 **Claire\_KMT** Highly Voted 4 months ago

C. Create an IAM role. Configure the IAM role to access the specific Amazon S3 API calls the application requires. Associate the IAM role with the EC2 instance.

upvoted 6 times

 **SerialiDr** Most Recent 1 month ago

**Selected Answer: C**

This approach follows AWS best practices. An IAM role can be created with the necessary permissions to access the S3 bucket. Then, this role can be associated with the EC2 instance. Applications running on the instance can then use the role's permissions to access S3 securely, without needing to manage access keys. This method leverages AWS's built-in security mechanisms and avoids the risks associated with managing static credentials.

upvoted 2 times

 **doubleh9324** 4 months ago

**Selected Answer: C**

c!!!!!!!!!!!!

upvoted 3 times

 **bammy** 4 months ago

C is the correct answer

upvoted 4 times

 **didorins** 4 months ago

**Selected Answer: C**

Create role with required permissions. Attach it to IAM as instance profile.

upvoted 4 times

## Question #239

## Topic 1

A developer created a web API that receives requests by using an internet-facing Application Load Balancer (ALB) with an HTTPS listener. The developer configures an Amazon Cognito user pool and wants to ensure that every request to the API is authenticated through Amazon Cognito.

What should the developer do to meet this requirement?

- A. Add a listener rule to the listener to return a fixed response if the Authorization header is missing. Set the fixed response to 401 Unauthorized.
- B. Create an authentication action for the listener rules of the ALB. Set the rule action type to authenticate-cognito. Set the OnUnauthenticatedRequest field to "deny."
- C. Create an Amazon API Gateway API. Configure all API methods to be forwarded to the ALB endpoint. Create an authorizer of the COGNITO\_USER\_POOLS type. Configure every API method to use that authorizer.
- D. Create a new target group that includes an AWS Lambda function target that validates the Authorization header by using Amazon Cognito. Associate the target group with the listener.

**Correct Answer: B**

*Community vote distribution*

B (67%)

C (33%)

 **SerialiDr** 1 month ago

**Selected Answer: B**

This approach uses the built-in capabilities of the ALB to authenticate requests with Amazon Cognito. By configuring a rule action to authenticate with a Cognito user pool, the ALB can handle authentication before the request is forwarded to the target group. The OnUnauthenticatedRequest setting of "deny" ensures that unauthenticated requests are not allowed access, which aligns with the requirement to authenticate every request.

upvoted 2 times

 **dostonbekabdullaev** 1 month, 1 week ago

**Selected Answer: B**

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html#configure-user-authentication>  
upvoted 2 times

 **JohnPI** 1 month, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-enable-cognito-user-pool.html>  
upvoted 1 times

 **rrshah83** 2 months ago

**Selected Answer: B**

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html#configure-user-authentication>  
upvoted 2 times

 **c9ebec2** 2 months, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>  
upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/amazon/view/88889-exam-aws-certified-developer-associate-topic-1-question-332/>  
upvoted 2 times

 **Certified101** 2 months, 2 weeks ago

**Selected Answer: C**

I think its C - API G would work better ?  
upvoted 1 times

 **Claire\_KMT** 4 months ago

B. Create an authentication action for the listener rules of the ALB. Set the rule action type to authenticate-cognito. Set the OnUnauthenticatedRequest field to "deny."  
upvoted 2 times

## Question #240

## Topic 1

A company recently deployed an AWS Lambda function. A developer notices an increase in the function throttle metrics in Amazon CloudWatch.

What are the MOST operationally efficient solutions to reduce the function throttling? (Choose two.)

- A. Migrate the function to Amazon Elastic Kubernetes Service (Amazon EKS).
- B. Increase the maximum age of events in Lambda.
- C. Increase the function's reserved concurrency.
- D. Add the lambda:GetFunctionConcurrency action to the execution role.
- E. Request a service quota change for increased concurrency.

**Correct Answer:** CE

*Community vote distribution*

CE (100%)

✉  **SerialiDr** 1 month ago

**Selected Answer:** CE

C. Increase the function's reserved concurrency.

Reserved concurrency is a feature in AWS Lambda that allows you to allocate a specific amount of concurrency to a particular function. This ensures that the function has a dedicated amount of concurrency and is not affected by throttling due to high usage of other functions in your account. Increasing the reserved concurrency can help mitigate throttling issues, especially if the throttling is due to reaching account-level concurrency limits.

E. Request a service quota change for increased concurrency.

AWS Lambda has default service quotas (formerly known as limits) for the maximum number of concurrent executions across all functions in your account. If your Lambda function is experiencing throttling due to reaching these account-level concurrency limits, requesting an increase in the service quota for Lambda concurrency can provide a solution.

upvoted 2 times

✉  **TanTran04** 2 months, 2 weeks ago

**Selected Answer:** CE

Following issue throttling.

C and E is suitable

upvoted 2 times

✉  **oussa\_ama** 4 months ago

The correct answer is C&E.

upvoted 3 times

✉  **Claire\_KMT** 4 months ago

C. Increase the function's reserved concurrency: Reserved concurrency ensures that a specific number of concurrent executions are always available for your function.

E. Request a service quota change for increased concurrency: If your application is experiencing throttling and the reserved concurrency isn't sufficient, you can request a service quota increase for additional concurrency.

upvoted 3 times

## Question #241

## Topic 1

A company is creating a REST service using an Amazon API Gateway with AWS Lambda integration. The service must run different versions for testing purposes.

What would be the BEST way to accomplish this?

- A. Use an X-Version header to denote which version is being called and pass that header to the Lambda function(s).
- B. Create an API Gateway Lambda authorizer to route API clients to the correct API version.
- C. Create an API Gateway resource policy to isolate versions and provide context to the Lambda function(s).
- D. Deploy the API versions as unique stages with unique endpoints and use stage variables to provide further context.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **SerialiDr** 1 month ago

**Selected Answer: D**

API Gateway allows you to create different stages for your API, each with its own configuration. These stages can represent different versions of your API (like development, test, and production). You can deploy your API to these stages and have different configurations for each stage, such as different Lambda functions, stage variables, or settings. This approach is straightforward and aligns with best practices for managing different environments in API Gateway.

upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

**Selected Answer: D**

Creating unique stages for different versions is a common practice for managing and deploying different versions of REST APIs. => D

upvoted 4 times

 **Claire\_KMT** 4 months ago

D. Deploy the API versions as unique stages with unique endpoints and use stage variables to provide further context.

upvoted 3 times

## Question #242

## Topic 1

A company is using AWS CodePipeline to deliver one of its applications. The delivery pipeline is triggered by changes to the main branch of an AWS CodeCommit repository and uses AWS CodeBuild to implement the test and build stages of the process and AWS CodeDeploy to deploy the application.

The pipeline has been operating successfully for several months and there have been no modifications. Following a recent change to the application's source code, AWS CodeDeploy has not deployed the updated application as expected.

What are the possible causes? (Choose two.)

- A. The change was not made in the main branch of the AWS CodeCommit repository.
- B. One of the earlier stages in the pipeline failed and the pipeline has terminated.
- C. One of the Amazon EC2 instances in the company's AWS CodePipeline cluster is inactive.
- D. The AWS CodePipeline is incorrectly configured and is not invoking AWS CodeDeploy.
- E. AWS CodePipeline does not have permissions to access AWS CodeCommit.

**Correct Answer:** AB

*Community vote distribution*



✉ **tapan666** 4 months ago

**Selected Answer: AB**

- A. The change was not made in the main branch of the AWS CodeCommit repository: In this pipeline setup, if the change was made in a branch other than the main branch, it would not trigger the pipeline, and therefore, AWS CodeDeploy wouldn't deploy the updated application.
- B. One of the earlier stages in the pipeline failed and the pipeline has terminated: If one of the preceding stages in the pipeline failed, it would prevent the subsequent stages, including AWS CodeDeploy, from being executed.

upvoted 6 times

✉ **SerialiDr** 1 month ago

**Selected Answer: AB**

- A. The change was not made in the main branch of the AWS CodeCommit repository.  
If the change to the application's source code was not made in the main branch (or the branch that triggers the pipeline), AWS CodePipeline would not detect the change and therefore would not initiate the deployment process. It's crucial that changes are made in the correct branch that is configured to trigger the pipeline.
- B. One of the earlier stages in the pipeline failed and the pipeline has terminated.  
If any stage in AWS CodePipeline fails (such as a failure in the test or build stages in AWS CodeBuild), the pipeline stops and does not proceed to the deployment stage. It is common for pipelines to be configured to halt on failure to prevent the deployment of potentially faulty code.

upvoted 2 times

✉ **Certified101** 2 months, 2 weeks ago

**Selected Answer: AB**

AB is correct - there have been no changes, so someone either merged code into the wrong branch (not triggering the pipeline) or it failed at an earlier stage.

Other options don't make sense given the scenario

upvoted 2 times

✉ **LR2023** 2 months, 3 weeks ago

**Selected Answer: BC**

The delivery pipeline is triggered by changes to the main branch - so new code change should have triggered this but this caused errors for some reasons and option C

upvoted 1 times

✉ **ShawnWon** 3 months, 2 weeks ago

AB

the key word is "The pipeline has been operating successfully for several months and there have been no modifications." So the "D. The codePipeline is incorrectly configured" is incorrect, because if the configuration is incorrect, it won't have been operating successfully for several months.

upvoted 3 times

✉ **PrakashM14** 3 months, 3 weeks ago

**Selected Answer: BD**

- B. One of the earlier stages in the pipeline failed and the pipeline has terminated.
- D. The AWS CodePipeline is incorrectly configured and is not invoking AWS CodeDeploy.

upvoted 1 times

 **Claire\_KMT** 4 months ago

- B. One of the earlier stages in the pipeline failed and the pipeline has terminated.
- D. The AWS CodePipeline is incorrectly configured and is not invoking AWS CodeDeploy.

upvoted 1 times

## Question #243

## Topic 1

A developer is building a serverless application by using AWS Serverless Application Model (AWS SAM) on multiple AWS Lambda functions. When the application is deployed, the developer wants to shift 10% of the traffic to the new deployment of the application for the first 10 minutes after deployment. If there are no issues, all traffic must switch over to the new version.

Which change to the AWS SAM template will meet these requirements?

- A. Set the Deployment Preference Type to Canary10Percent10Minutes. Set the AutoPublishAlias property to the Lambda alias.
- B. Set the Deployment Preference Type to Linear10PercentEvery10Minutes. Set AutoPublishAlias property to the Lambda alias.
- C. Set the Deployment Preference Type to Canary10Percent10Minutes. Set the PreTraffic and PostTraffic properties to the Lambda alias.
- D. Set the Deployment Preference Type to Linear10PercentEvery10Minutes. Set PreTraffic and PostTraffic properties to the Lambda alias.

**Correct Answer: B**

*Community vote distribution*



✉ **didorins** 4 months ago

**Selected Answer: C**

C should be it.

Shift traffic in two batches is Canary  
Validation is done with hooks

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html>  
upvoted 8 times

✉ **Jisking** 3 days, 19 hours ago

**Selected Answer: A**

I go with A!  
upvoted 1 times

✉ **konieczny69** 4 weeks ago

**Selected Answer: A**

AutoPublishAlias is a requirement.  
Pre and Post traffic handlers are nice to have  
upvoted 1 times

✉ **SerialiDr** 1 month ago

**Selected Answer: A**

This configuration will ensure that during deployment, 10% of the traffic is shifted to the new version for 10 minutes as a "canary" release. If no issues are detected during this period, AWS SAM will automatically shift the rest of the traffic to the new version. The AutoPublishAlias property is used to specify the alias that the AWS SAM deployment process will update to point to the new version of the function.  
upvoted 1 times

✉ **Snapie** 1 month, 3 weeks ago

**Selected Answer: A**

set the Deployment Preference Type to Canary10Percent10Minutes and set the AutoPublishAlias property to the Lambda alias.  
upvoted 1 times

✉ **rrshah83** 2 months ago

**Selected Answer: A**

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html>  
upvoted 1 times

✉ **Mimi666** 2 months, 2 weeks ago

**Selected Answer: A**

Hooks as post y pre are not obligatory required  
upvoted 1 times

✉ **tqiu654** 2 months, 3 weeks ago

**Selected Answer: A**

Based on ChatGPT: A. PostTraffic properties are not necessary.  
upvoted 1 times

nickolaj 3 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/sam-resource-function.html>

property to the Lambda alias.

upvoted 2 times

NinjaCloud 3 months, 4 weeks ago

Answer: A!

Option B, which uses the "Linear" deployment type, gradually shifts traffic, and doesn't fully meet the requirement of immediately switching all traffic if there are no issues within the first 10 minutes.

upvoted 3 times

Claire\_KMT 4 months ago

A. Set the Deployment Preference Type to Canary10Percent10Minutes. Set the AutoPublishAlias property to the Lambda alias.

upvoted 3 times

LemonGremlin 4 months, 1 week ago

Option C is the best choice for a canary deployment with the specific requirements mentioned in the scenario.

upvoted 2 times

## Question #244

## Topic 1

An AWS Lambda function is running in a company's shared AWS account. The function needs to perform an additional ec2:DescribeInstances action that is directed at the company's development accounts. A developer must configure the required permissions across the accounts.

How should the developer configure the permissions to adhere to the principle of least privilege?

- A. Create an IAM role in the shared account. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship between the development accounts for this role. Update the Lambda function IAM role in the shared account by adding the ec2:DescribeInstances permission to the role.
- B. Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.
- C. Create an IAM role in the shared account. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship between the development accounts for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.
- D. Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the ec2:DescribeInstances permission to the role.

**Correct Answer: B**

*Community vote distribution*

**B (73%)**    **C (18%)**    **9%**

 **PrakashM14**  4 months ago

**Selected Answer: B**

Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.

upvoted 6 times

 **SerialiDr**  1 month ago

**Selected Answer: B**

Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.

upvoted 1 times

 **Snape** 1 month, 3 weeks ago

**Selected Answer: B**

Classic case of cross account access (CAA)

upvoted 1 times

 **Kowsik\_shashi** 4 months ago

**Selected Answer: C**

By using iam:AssumeRole, AWS allows you to implement the principle of least privilege, which means entities have only the permissions they require to perform specific tasks and nothing more.

upvoted 2 times

 **Ibaker12** 4 months ago

**Selected Answer: A**

iam:AssumeRole doesn't exist it is sts:AssumeRole & creating IAM roles within development accounts is unnecessary work

upvoted 1 times

 **Claire\_KMT** 4 months ago

B. Create an IAM role in the development accounts. Add the ec2:DescribeInstances permission to the role. Establish a trust relationship with the shared account for this role. Update the Lambda function IAM role in the shared account by adding the iam:AssumeRole permissions.

upvoted 1 times

 **didorins** 4 months ago

B

To enable cross account AWS service actions, create role with required permissions in account which holds the resource. Enable trust relationship with account that will access the resource. Allow accessing account to assume the role.

upvoted 1 times

## Question #245

## Topic 1

A developer is building a new application that will be deployed on AWS. The developer has created an AWS CodeCommit repository for the application. The developer has initialized a new project for the application by invoking the AWS Cloud Development Kit (AWS CDK) cdk init command.

The developer must write unit tests for the infrastructure as code (IaC) templates that the AWS CDK generates. The developer also must run a validation tool across all constructs in the CDK application to ensure that critical security configurations are activated.

Which combination of actions will meet these requirements with the LEAST development overhead? (Choose two.)

- A. Use a unit testing framework to write custom unit tests against the cdk.out file that the AWS CDK generates. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository.
- B. Use the CDK assertions module to integrate unit tests with the application. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository.
- C. Use the CDK runtime context to set key-value pairs that must be present in the cdk.out file that the AWS CDK generates. Fail the stack synthesis if any violations are present.
- D. Write a script that searches the application for specific key configuration strings. Configure the script to produce a report of any security violations.
- E. Use the CDK Aspects class to create custom rules to apply to the CDK application. Fail the stack synthesis if any violations are present.

**Correct Answer:** BE

*Community vote distribution*

BE (100%)

 **SerialiDr** 1 month ago

**Selected Answer: BE**

B. The AWS CDK assertions library provides a convenient way to write unit tests for CDK applications. It allows developers to assert various aspects of the CDK constructs, such as properties and resource counts. Integrating these unit tests into the CI/CD pipeline ensures that they are automatically run after any commit, providing continuous validation of the infrastructure code.  
 E. Aspects in AWS CDK are a way to apply operations to all constructs in a CDK app or a part of the app. By using the Aspects class, the developer can create custom rules (like security configuration checks) and apply them across all constructs in the CDK application. If these rules find any violations, the stack synthesis can be set to fail, ensuring that the application adheres to critical security configurations.

upvoted 2 times

 **c9ebec2** 2 months, 2 weeks ago

**Selected Answer: BE**

B: <https://docs.aws.amazon.com/cdk/v2/guide/testing.html> fine-grained assertions

E: <https://docs.aws.amazon.com/cdk/v2/guide/aspects.html>

upvoted 2 times

 **TanTran04** 2 months, 2 weeks ago

**Selected Answer: BE**

Option B:  
 The standard approach to testing AWS CDK apps uses the AWS CDK's assertions module  
<https://docs.aws.amazon.com/cdk/v2/guide/testing.html>

Option E: By using the CDK Aspects class to create custom rules, you can enforce specific conditions or checks on your CDK application, including security configurations. Failing the stack synthesis if any violations are present ensures that deployments do not proceed if critical security configurations are not met.

CHATGPT 3.5

upvoted 1 times

 **deepak547** 3 months ago

Option B allows writing unit tests for the infrastructure code using the built-in CDK assertions. Running them in a CI/CD pipeline on commits provides automated testing.

Option E lets you define security validation rules as Aspects, which run on synth to catch issues early.

upvoted 1 times

 **Claire\_KMT** 4 months ago

B. Use the CDK assertions module to integrate unit tests with the application. Run the unit tests in a continuous integration and continuous delivery (CI/CD) pipeline that is invoked after any commit to the repository.

- E. Use the CDK Aspects class to create custom rules to apply to the CDK application. Fail the stack synthesis if any violations are present.  
upvoted 3 times

## Question #246

## Topic 1

An online sales company is developing a serverless application that runs on AWS. The application uses an AWS Lambda function that calculates order success rates and stores the data in an Amazon DynamoDB table. A developer wants an efficient way to invoke the Lambda function every 15 minutes.

Which solution will meet this requirement with the LEAST development effort?

- A. Create an Amazon EventBridge rule that has a rate expression that will run the rule every 15 minutes. Add the Lambda function as the target of the EventBridge rule.
- B. Create an AWS Systems Manager document that has a script that will invoke the Lambda function on Amazon EC2. Use a Systems Manager Run Command task to run the shell script every 15 minutes.
- C. Create an AWS Step Functions state machine. Configure the state machine to invoke the Lambda function execution role at a specified interval by using a Wait state. Set the interval to 15 minutes.
- D. Provision a small Amazon EC2 instance. Set up a cron job that invokes the Lambda function every 15 minutes.

**Correct Answer: B**

*Community vote distribution*



A (100%)

 **SerialiDr** 1 month ago

**Selected Answer: A**

Amazon EventBridge (formerly known as CloudWatch Events) allows you to set up a rule with a specific schedule using cron or rate expressions. In this case, a rate expression of rate(15 minutes) can be used. EventBridge rules can directly target a Lambda function, making this a straightforward and low-effort solution to execute the function at regular intervals.

upvoted 2 times

 **Claire\_KMT** 4 months ago

A. Create an Amazon EventBridge rule that has a rate expression that will run the rule every 15 minutes. Add the Lambda function as the target of the EventBridge rule.

upvoted 3 times

 **didorins** 4 months ago

**Selected Answer: A**

Run Lambda as cron = Event Bridge

upvoted 4 times

 **LemonGremlin** 4 months, 1 week ago

**Selected Answer: A**

option A is the most efficient and least development effort option for invoking the Lambda function every 15 minutes, as it leverages Amazon EventBridge's built-in scheduling capabilities and is fully serverless.

upvoted 4 times

## Question #247

## Topic 1

A company deploys a photo-processing application to an Amazon EC2 instance. The application needs to process each photo in less than 5 seconds. If processing takes longer than 5 seconds, the company's development team must receive a notification.

How can a developer implement the required time measurement and notification with the LEAST operational overhead?

- A. Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that is based on a static threshold of 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Each time a photo is processed, publish the processing time to the queue. Create an application to consume from the queue and to determine whether any values are more than 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that enters ALARM state if the average of values is greater than 5 seconds. Notify the development team by sending an Amazon Simple Email Service (Amazon SES) message.
- D. Create an Amazon Kinesis data stream. Each time a photo is processed, publish the processing time to the data stream. Create an Amazon CloudWatch alarm that enters ALARM state if any values are more than 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.

**Correct Answer: A**

Community vote distribution

A (100%)

 **tapan666**  4 months ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/amazon/view/88805-exam-aws-certified-developer-associate-topic-1-question-263/>  
upvoted 5 times

 **SerialiDr**  1 month ago

**Selected Answer: A**

This approach directly leverages AWS services for monitoring and notification with minimal setup and maintenance. CloudWatch custom metrics can be used to track the processing time for each photo. A CloudWatch alarm can then be configured to trigger when any metric value exceeds the threshold of 5 seconds, sending a notification to the development team via an SNS topic.  
upvoted 2 times

 **Claire\_KMT** 4 months ago

A. Create an Amazon CloudWatch custom metric. Each time a photo is processed, publish the processing time as a metric value. Create a CloudWatch alarm that is based on a static threshold of 5 seconds. Notify the development team by using an Amazon Simple Notification Service (Amazon SNS) topic.  
upvoted 2 times

## Question #248

## Topic 1

A company is using AWS Elastic Beanstalk to manage web applications that are running on Amazon EC2 instances. A developer needs to make configuration changes. The developer must deploy the changes to new instances only.

Which types of deployment can the developer use to meet this requirement? (Choose two.)

- A. All at once
- B. Immutable
- C. Rolling
- D. Blue/green
- E. Rolling with additional batch

**Correct Answer:** BD

*Community vote distribution*

BD (100%)

✉  **tapan666**  4 months ago

**Selected Answer: BD**

<https://www.examtopics.com/discussions/amazon/view/88855-exam-aws-certified-developer-associate-topic-1-question-289/>  
upvoted 6 times

✉  **SerialiDr**  1 month ago

**Selected Answer: BD**

B. Immutable: In an immutable deployment, AWS Elastic Beanstalk deploys the application version to a fresh group of instances in a new Auto Scaling group. Once the new instances pass health checks, they are moved to the existing Auto Scaling group, and the old instances are terminated. This approach ensures that new instances are used for the deployment, minimizing the impact on the existing environment.

D. Blue/Green: Blue/green deployment involves deploying the new version of the application to a separate environment (the "green" environment). Once the new environment is ready and tested, the traffic is switched from the old environment (the "blue" environment) to the new one. This type of deployment is effective for ensuring that the new version is deployed on new instances and provides a straightforward way to rollback if needed.  
upvoted 2 times

✉  **Certified101** 2 months, 2 weeks ago

**Selected Answer: BD**

BD - <https://www.examtopics.com/discussions/amazon/view/88855-exam-aws-certified-developer-associate-topic-1-question-289/>  
upvoted 2 times

✉  **Claire\_KMT** 4 months ago

B. Immutable  
D. Blue/green  
upvoted 2 times

## Question #249

## Topic 1

A developer needs to use Amazon DynamoDB to store customer orders. The developer's company requires all customer data to be encrypted at rest with a key that the company generates.

What should the developer do to meet these requirements?

- A. Create the DynamoDB table with encryption set to None. Code the application to use the key to decrypt the data when the application reads from the table. Code the application to use the key to encrypt the data when the application writes to the table.
- B. Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS customer managed key during creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.
- C. Store the key by using AWS Key Management Service (AWS KMS). Create the DynamoDB table with default encryption. Include the kms:Encrypt parameter with the Amazon Resource Name (ARN) of the AWS KMS key when using the DynamoDB software development kit (SDK).
- D. Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS AWS managed key during creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **joshnort** 3 weeks, 5 days ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/database/bring-your-own-encryption-keys-to-amazon-dynamodb/>  
upvoted 1 times

 **SerialiDr** 1 month ago

**Selected Answer: B**

This option allows the developer to use a customer-managed key in AWS KMS for encryption at rest in DynamoDB. The customer-managed key offers more flexibility and control over the key management compared to AWS managed keys. When creating the DynamoDB table, the developer can specify the KMS key to be used for encryption.

upvoted 2 times

 **tapan666** 4 months ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/amazon/view/78943-exam-aws-certified-developer-associate-topic-1-question-23/>  
upvoted 3 times

 **Claire\_KMT** 4 months ago

B. Store the key by using AWS Key Management Service (AWS KMS). Choose an AWS KMS customer managed key during the creation of the DynamoDB table. Provide the Amazon Resource Name (ARN) of the AWS KMS key.

upvoted 3 times

## Question #250

## Topic 1

A company uses AWS CloudFormation to deploy an application that uses an Amazon API Gateway REST API with AWS Lambda function integration. The application uses Amazon DynamoDB for data persistence. The application has three stages: development, testing, and production. Each stage uses its own DynamoDB table.

The company has encountered unexpected issues when promoting changes to the production stage. The changes were successful in the development and testing stages. A developer needs to route 20% of the traffic to the new production stage API with the next production release. The developer needs to route the remaining 80% of the traffic to the existing production stage. The solution must minimize the number of errors that any single customer experiences.

Which approach should the developer take to meet these requirements?

- A. Update 20% of the planned changes to the production stage. Deploy the new production stage. Monitor the results. Repeat this process five times to test all planned changes.
- B. Update the Amazon Route 53 DNS record entry for the production stage API to use a weighted routing policy. Set the weight to a value of 80. Add a second record for the production domain name. Change the second routing policy to a weighted routing policy. Set the weight of the second policy to a value of 20. Change the alias of the second policy to use the testing stage API.
- C. Deploy an Application Load Balancer (ALB) in front of the REST API. Change the production API Amazon Route 53 record to point traffic to the ALB. Register the production and testing stages as targets of the ALB with weights of 80% and 20%, respectively.
- D. Configure canary settings for the production stage API. Change the percentage of traffic directed to canary deployment to 20%. Make the planned updates to the production stage. Deploy the changes

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **SerialiDr** 1 month ago

**Selected Answer: D**

Amazon API Gateway supports canary release deployments, which are specifically designed for this type of scenario. By configuring canary settings, the developer can gradually roll out changes to a small percentage of users (20% in this case) while still serving the majority of users (80%) with the current production stage. This approach helps in minimizing the impact of potential issues with new deployments.

upvoted 2 times

 **ansobimat** 3 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **Claire\_KMT** 4 months ago

D. Configure canary settings for the production stage API. Change the percentage of traffic directed to canary deployment to 20%. Make the planned updates to the production stage. Deploy the changes

upvoted 2 times

## Question #251

## Topic 1

A developer has created a data collection application that uses Amazon API Gateway, AWS Lambda, and Amazon S3. The application's users periodically upload data files and wait for the validation status to be reflected on a processing dashboard. The validation process is complex and time-consuming for large files.

Some users are uploading dozens of large files and have to wait and refresh the processing dashboard to see if the files have been validated. The developer must refactor the application to immediately update the validation result on the user's dashboard without reloading the full dashboard.

What is the MOST operationally efficient solution that meets these requirements?

- A. Integrate the client with an API Gateway WebSocket API. Save the user-uploaded files with the WebSocket connection ID. Push the validation status to the connection ID when the processing is complete to initiate an update of the user interface.
- B. Launch an Amazon EC2 micro instance, and set up a WebSocket server. Send the user-uploaded file and user detail to the EC2 instance after the user uploads the file. Use the WebSocket server to send updates to the user interface when the uploaded file is processed.
- C. Save the user's email address along with the user-uploaded file. When the validation process is complete, send an email notification through Amazon Simple Notification Service (Amazon SNS) to the user who uploaded the file.
- D. Save the user-uploaded file and user detail to Amazon DynamoDB. Use Amazon DynamoDB Streams with Amazon Simple Notification Service (Amazon SNS) push notifications to send updates to the browser to update the user interface.

**Correct Answer: A**

*Community vote distribution*



✉️ PrakashM14 4 months ago

**Selected Answer: A**

Option B involves setting up a WebSocket server on an EC2 instance, which is more manual and may require additional management overhead. Option C relies on email notifications, which might introduce delays and may not provide the desired real-time updates. Option D involves DynamoDB and SNS, which may add complexity without the direct support for real-time updates that WebSocket provides.

So, Option A

upvoted 5 times

✉️ SerialiDr 1 month ago

**Selected Answer: A**

This approach leverages the real-time capabilities of WebSocket connections managed by Amazon API Gateway. When a user uploads a file, the application can associate the file with the user's WebSocket connection ID. Once the file validation process completes, the application can send the status directly to the connected client, allowing immediate updates to the dashboard without the need for manual refreshes.

upvoted 2 times

✉️ tqi654 2 months, 3 weeks ago

**Selected Answer: D**

Based on ChatGPT: D.

upvoted 1 times

✉️ ansobimat 3 months, 1 week ago

**Selected Answer: A**

A. Integrate the client with an API Gateway WebSocket API. Save the user-uploaded files with the WebSocket connection ID. Push the validation status to the connection ID when the processing is complete to initiate an update of the user interface.

upvoted 3 times

✉️ tapan666 4 months ago

**Selected Answer: D**

Option C could work for notifying users, it doesn't provide immediate updates on the user's dashboard. Users would need to check their email to see the validation status, which may not be as user-friendly as real-time updates on the dashboard.

It adds complexity with email notifications and may result in longer delays before users see the validation results.

Option D (using DynamoDB Streams and Amazon SNS) is preferred because it offers a more operationally efficient and real-time solution without the need for WebSocket management, email notifications, or a constantly running EC2 instance. It provides immediate updates on the user's dashboard while keeping operational complexity and costs to a minimum.

upvoted 2 times

✉️ Claire\_KMT 4 months ago

B. Launch an Amazon EC2 micro instance, and set up a WebSocket server. Send the user-uploaded file and user detail to the EC2 instance after the user uploads the file. Use the WebSocket server to send updates to the user interface when the uploaded file is processed.

OR

D. Save the user-uploaded file and user detail to Amazon DynamoDB. Use Amazon DynamoDB Streams with Amazon Simple Notification Service (Amazon SNS) push notifications to send updates to the browser to update the user interface.

upvoted 1 times

## Question #252

## Topic 1

A company's developer is creating an application that uses Amazon API Gateway. The company wants to ensure that only users in the Sales department can use the application. The users authenticate to the application by using federated credentials from a third-party identity provider (IdP) through Amazon Cognito. The developer has set up an attribute mapping to map an attribute that is named Department and to pass the attribute to a custom AWS Lambda authorizer.

To test the access limitation, the developer sets their department to Engineering in the IdP and attempts to log in to the application. The developer is denied access. The developer then updates their department to Sales in the IdP and attempts to log in. Again, the developer is denied access. The developer checks the logs and discovers that access is being denied because the developer's access token has a department value of Engineering.

Which of the following is a possible reason that the developer's department is still being reported as Engineering instead of Sales?

- A. Authorization caching is enabled in the custom Lambda authorizer.
- B. Authorization caching is enabled on the Amazon Cognito user pool.
- C. The IAM role for the custom Lambda authorizer does not have a Department tag.
- D. The IAM role for the Amazon Cognito user pool does not have a Department tag.

**Correct Answer: A***Community vote distribution*

 A horizontal progress bar with a blue segment representing 86% of the total length, followed by a teal segment representing the remaining 14%.

7%

 **tapan666**  4 months ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/amazon/view/88914-exam-aws-certified-developer-associate-topic-1-question-294/>  
upvoted 5 times

 **joshnort**  3 weeks, 5 days ago

**Selected Answer: A**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/configure-api-gateway-lambda-authorization-with-console.html>  
upvoted 1 times

 **SerialiDr** 1 month ago

**Selected Answer: A**

When authorization caching is enabled in a custom Lambda authorizer, the authorizer can cache the policy associated with an access token. This caching is designed to improve performance by reducing the number of calls to the Lambda function. However, it can also lead to outdated authorization information being used if the user's attributes change in the identity provider (IdP) but the cached policy in the Lambda authorizer is still based on the old attributes.

In this case, when the developer initially logged in with the department set to Engineering, the custom Lambda authorizer created and cached a policy based on this information. Subsequently, even after the developer updated their department to Sales in the IdP, the cached policy (which still reflects the Engineering department) was used, leading to the access denial.

upvoted 2 times

 **SerialiDr** 1 month ago

**Selected Answer: A**

This approach leverages the real-time capabilities of WebSocket connections managed by Amazon API Gateway. When a user uploads a file, the application can associate the file with the user's WebSocket connection ID. Once the file validation process completes, the application can send the status directly to the connected client, allowing immediate updates to the dashboard without the need for manual refreshes.

upvoted 1 times

 **SerialiDr** 1 month ago

wrongly added here, please delete

upvoted 1 times

 **tqiu654** 2 months, 3 weeks ago

**Selected Answer: D**

Based on ChatGPT:D  
upvoted 1 times

 **anasbakla** 3 months, 2 weeks ago

**Selected Answer: A**

A is Correct

upvoted 3 times

 **PrakashM14** 4 months ago

**Selected Answer: B**

Options A, C, and D do not directly address the caching of user attributes in the context of Amazon Cognito. Option A refers to caching in the custom Lambda authorizer, but the issue seems more likely to be related to the Cognito user pool's caching mechanism. Options C and D mention IAM roles and tags, which may be relevant for other aspects of access control but are not the primary cause of the reported department value in this scenario.

upvoted 1 times

 **Claire\_KMT** 4 months ago

B. Authorization caching is enabled on the Amazon Cognito user pool.

upvoted 1 times

## Question #253

## Topic 1

A company has migrated an application to Amazon EC2 instances. Automatic scaling is working well for the application user interface. However, the process to deliver shipping requests to the company's warehouse staff is encountering issues. Duplicate shipping requests are arriving, and some requests are lost or arrive out of order.

The company must avoid duplicate shipping requests and must process the requests in the order that the requests arrive. Requests are never more than 250 KB in size and take 5-10 minutes to process. A developer needs to rearchitect the application to improve the reliability of the delivery and processing of the requests.

What should the developer do to meet these requirements?

- A. Create an Amazon Kinesis Data Firehose delivery stream to process the requests. Create an Amazon Kinesis data stream. Modify the application to write the requests to the Kinesis data stream.
- B. Create an AWS Lambda function to process the requests. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the Lambda function to the SNS topic. Modify the application to write the requests to the SNS topic.
- C. Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) standard queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.
- D. Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.

**Correct Answer: D**

*Community vote distribution*



D (100%)

✉  **joshnort** 2 weeks, 4 days ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-exactly-once-processing.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-message-order.html>  
upvoted 1 times

✉  **SerialiDr** 1 month ago

**Selected Answer: D**

Amazon SQS FIFO (First-In-First-Out) queues are designed to ensure that messages are processed exactly once and in the exact order that they are sent. This characteristic makes FIFO queues suitable for scenarios where order and uniqueness are critical. By integrating the FIFO queue with an AWS Lambda function, the developer can automate the processing of the shipping requests as they arrive in the queue.

upvoted 2 times

✉  **tapan666** 4 months ago

**Selected Answer: D**

<https://www.examtopics.com/discussions/amazon/view/88667-exam-aws-certified-developer-associate-topic-1-question-209/>  
upvoted 3 times

✉  **Claire\_KMT** 4 months ago

D. Create an AWS Lambda function to process the requests. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the SQS queue as an event source for the Lambda function. Modify the application to write the requests to the SQS queue.  
upvoted 3 times

## Question #254

## Topic 1

A developer is creating a machine learning (ML) pipeline in AWS Step Functions that contains AWS Lambda functions. The developer has configured an Amazon Simple Queue Service (Amazon SQS) queue to deliver ML model parameters to the ML pipeline to train ML models. The developer uploads the trained models are uploaded to an Amazon S3 bucket.

The developer needs a solution that can locally test the ML pipeline without making service integration calls to Amazon SQS and Amazon S3.

Which solution will meet these requirements?

- A. Use the Amazon CodeGuru Profiler to analyze the Lambda functions used in the AWS Step Functions pipeline.
- B. Use the AWS Step Functions Local Docker Image to run and locally test the Lambda functions.
- C. Use the AWS Serverless Application Model (AWS SAM) CLI to run and locally test the Lambda functions.
- D. Use AWS Step Functions Local with mocked service integrations.

**Correct Answer:** D

*Community vote distribution*

D (100%)

SerialiDr 1 month ago

**Selected Answer: D**

AWS Step Functions Local allows developers to test Step Functions workflows on their local machines, without the need to deploy them to AWS. By using Step Functions Local, developers can simulate Step Functions and mock the integration with AWS services such as Amazon SQS and Amazon S3. This approach is ideal for testing the flow of the ML pipeline, including the interaction of Lambda functions, without actually triggering external AWS services.

upvoted 2 times

deepak547 3 months ago

Step Functions Local, specifically allows mocking AWS services like SQS and S3. This enables end-to-end local testing of the state machine while simulating external calls.

Therefore, AWS Step Functions Local with mocked integrations meets the requirements to test the pipeline offline without relying on live AWS services. This is the simplest way to achieve local testing.

upvoted 2 times

tapan666 4 months ago

**Selected Answer: D**

D. Use AWS Step Functions Local with mocked service integrations.

Hide Solution

upvoted 3 times

Claire\_KMT 4 months ago

D. Use AWS Step Functions Local with mocked service integrations.

upvoted 2 times

## Question #255

## Topic 1

A company runs a batch processing application by using AWS Lambda functions and Amazon API Gateway APIs with deployment stages for development, user acceptance testing, and production. A development team needs to configure the APIs in the deployment stages to connect to third-party service endpoints.

Which solution will meet this requirement?

- A. Store the third-party service endpoints in Lambda layers that correspond to the stage.
- B. Store the third-party service endpoints in API Gateway stage variables that correspond to the stage.
- C. Encode the third-party service endpoints as query parameters in the API Gateway request URL.
- D. Store the third-party service endpoint for each environment in AWS AppConfig.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **ANDRES715** 4 days, 5 hours ago

**Selected Answer: B**

You.com y chatGpt  
upvoted 1 times

 **ANDRES715** 4 days, 5 hours ago

You.com y chatGpt  
upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: B**

D: additional complex  
C: this is typically used to send data to the end point. Not to configure the endpoint itself. Less secure.  
upvoted 1 times

## Question #256

## Topic 1

A developer is building a serverless application that runs on AWS. The developer wants to create an accelerated development workflow that deploys incremental changes to AWS for testing. The developer wants to deploy the incremental changes but does not want to fully deploy the entire application to AWS for every code commit.

What should the developer do to meet these requirements?

- A. Use the AWS Serverless Application Model (AWS SAM) to build the application. Use the `sam sync` command to deploy the incremental changes.
- B. Use the AWS Serverless Application Model (AWS SAM) to build the application. Use the `sam init` command to deploy the incremental changes.
- C. Use the AWS Cloud Development Kit (AWS CDK) to build the application. Use the `cdk synth` command to deploy the incremental changes.
- D. Use the AWS Cloud Development Kit (AWS CDK) to build the application. Use the `cdk bootstrap` command to deploy the incremental changes.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **ANDRES715** 4 days, 5 hours ago

**Selected Answer: A**

You.com

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

Serverless

`cdk synth` command is not used for deploying changes. Instead, `cdk synth` generates an AWS CloudFormation template from the CDK app's code, which describes the cloud resources that need to be created or updated. It does not actually deploy those changes to AWS.

upvoted 1 times

 **tgv** 2 weeks ago

**Selected Answer: A**

Here the answer is A - `sam sync`.

According to my research:

- `cdk synth`: only constructs your CloudFormation template. It does not deploy (create actual resources) it to AWS. You can take the template constructed, deploy it manually in CFN console, edit or inspect.
- `sam init`: used to initialize a new serverless application
- `cdk bootstrap`: the main purpose of `cdk bootstrap` is to provision a set of resources required to support the deployment of AWS CDK applications

upvoted 3 times

## Question #257

## Topic 1

A developer is building an application that will use an Amazon API Gateway API with an AWS Lambda backend. The team that will develop the frontend requires immediate access to the API endpoints to build the UI. To prepare the backend application for integration, the developer needs to set up endpoints. The endpoints need to return predefined HTTP status codes and JSON responses for the frontend team. The developer creates a method for an API resource.

Which solution will meet these requirements?

- A. Set the integration type to AWS\_PROXY. Provision Lambda functions to return hardcoded JSON data.
- B. Set the integration type to MOCK. Configure the method's integration request and integration response to associate a JSON responses with specific HTTP status codes.
- C. Set the integration type to HTTP\_PROXY. Configure API Gateway to pass all requests to an external placeholder API, which the team will build.
- D. Set the integration type to MOCK. Use a method request to define HTTP status codes. Use an integration request to define JSON responses.

**Correct Answer: B**

*Community vote distribution*

 B (100%)

 **ANDRES715** 4 days, 5 hours ago

**Selected Answer: B**

You.com

upvoted 1 times

 **tgv** 2 weeks ago

**Selected Answer: B**

the correct answer is B

upvoted 4 times

## Question #258

## Topic 1

A developer is migrating an application to Amazon Elastic Kubernetes Service (Amazon EKS). The developer migrates the application to Amazon Elastic Container Registry (Amazon ECR) with an EKS cluster. As part of the application migration to a new backend, the developer creates a new AWS account. The developer makes configuration changes to the application to point the application to the new AWS account and to use new backend resources. The developer successfully tests the changes within the application by deploying the pipeline.

The Docker image build and the pipeline deployment are successful, but the application is still connecting to the old backend. The developer finds that the application's configuration is still referencing the original EKS cluster and not referencing the new backend resources.

Which reason can explain why the application is not connecting to the new resources?

- A. The developer did not successfully create the new AWS account.
- B. The developer added a new tag to the Docker image.
- C. The developer did not update the Docker image tag to a new version.
- D. The developer pushed the changes to a new Docker image tag.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: C**

B probably intended to say 'a wrong tag' but not as clear as C.  
upvoted 2 times

## Question #259

## Topic 1

A developer is creating an application that reads and writes to multiple Amazon S3 buckets. The application will be deployed to an Amazon EC2 instance. The developer wants to make secure API requests from the EC2 instances without the need to manage the security credentials for the application. The developer needs to apply the principle of least privilege.

Which solution will meet these requirements?

- A. Create an IAM user. Create access keys and secret keys for the user. Associate the user with an IAM policy that allows s3:\* permissions.
- B. Associate the EC2 instance with an IAM role that has an IAM policy that allows s3>ListBucket and s3:\*Object permissions for specific S3 buckets.
- C. Associate the EC2 instance with an IAM role that has an AmazonS3FullAccess AWS managed policy.
- D. Create a bucket policy on the S3 bucket that allows s3>ListBucket and s3:\*Object permissions to the EC2 instance.

**Correct Answer: B**

*Community vote distribution*

 B (100%)

 **ANDRES715** 4 days, 5 hours ago

Habla de varios depositos S3 por eso la opcion correcta es la B ya que C no especifica cada deposito, habla de solo uno.  
upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: B**

B is correct.  
upvoted 2 times

## Question #260

## Topic 1

A developer is writing an application that will retrieve sensitive data from a third-party system. The application will format the data into a PDF file. The PDF file could be more than 1 MB. The application will encrypt the data to disk by using AWS Key Management Service (AWS KMS). The application will decrypt the file when a user requests to download it. The retrieval and formatting portions of the application are complete.

The developer needs to use the GenerateDataKey API to encrypt the PDF file so that the PDF file can be decrypted later. The developer needs to use an AWS KMS symmetric customer managed key for encryption.

Which solutions will meet these requirements?

- A. Write the encrypted key from the GenerateDataKey API to disk for later use. Use the plaintext key from the GenerateDataKey API and a symmetric encryption algorithm to encrypt the file.
- B. Write the plain text key from the GenerateDataKey API to disk for later use. Use the encrypted key from the GenerateDataKey API and a symmetric encryption algorithm to encrypt the file.
- C. Write the encrypted key from the GenerateDataKey API to disk for later use. Use the plaintext key from the GenerateDataKey API to encrypt the file by using the KMS Encrypt API.
- D. Write the plain text key from the GenerateDataKey API to disk for later use. Use the encrypted key from the GenerateDataKey API to encrypt the file by using the KMS Encrypt API.

**Correct Answer: A**

*Community vote distribution*

A (67%)

D (33%)

ANDRES715 4 days, 4 hours ago

**Selected Answer: D**

Según la documentación de AWS, cuando se utiliza la API GenerateDataKey, se obtiene una clave de texto sin formato y una clave cifrada. La clave de texto sin formato se puede escribir en el disco para su uso posterior, mientras que la clave cifrada se utiliza para cifrar los datos. En este caso, el desarrollador debe escribir la clave de texto sin formato en el disco para su uso posterior y utilizar la clave cifrada para cifrar el archivo PDF mediante la API de cifrado KMS.

upvoted 1 times

CrescentShared 1 week, 4 days ago

**Selected Answer: A**

Using the KMS Encrypt API to encrypt large amounts of data, such as a PDF file that could be more than 1 MB, is not efficient and can be costly. AWS KMS is designed for encrypting small amounts of data, such as encryption keys or short strings. For larger data, it's recommended to use a client-side encryption library with a data key generated by KMS.

upvoted 2 times

## Question #261

## Topic 1

A company runs an application on Amazon EC2 instances. The EC2 instances open connections to an Amazon RDS for SQL Server database. A developer needs to store and access the credentials and wants to automatically rotate the credentials. The developer does not want to store the credentials for the database in the code.

Which solution will meet these requirements in the MOST secure way?

- A. Create an IAM role that has permissions to access the database. Attach the IAM role to the EC2 instances.
- B. Store the credentials as secrets in AWS Secrets Manager. Create an AWS Lambda function to update the secrets and the database. Retrieve the credentials from Secrets Manager as needed.
- C. Store the credentials in an encrypted text file in an Amazon S3 bucket. Configure the EC2 instance launch template to download the credentials from Amazon S3 as the instance launches. Create an AWS Lambda function to update the secrets and the database.
- D. Store the credentials in an Amazon DynamoDB table. Configure an Amazon CloudWatch Events rule to invoke an AWS Lambda function to periodically update the secrets and database.

**Correct Answer: B**

*Community vote distribution*

 B (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **tgv** 2 weeks ago

rotation --> Secrets Manager

upvoted 2 times

 **VKG0507** 3 weeks, 4 days ago

The ans is B

upvoted 3 times

## Question #262

## Topic 1

A company wants to test its web application more frequently. The company deploys the application by using a separate AWS CloudFormation stack for each environment. The company deploys the same CloudFormation template to each stack as the application progresses through the development lifecycle.

A developer needs to build in notifications for the quality assurance (QA) team. The developer wants the notifications to occur for new deployments in the final preproduction environment.

Which solution will meet these requirements?

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the QA team to the Amazon SNS topic. Update the CloudFormation stack options to point to the SNS topic in the pre-production environment.
- B. Create an AWS Lambda function that notifies the QA team. Create an Amazon EventBridge rule to invoke the Lambda function on the default event bus. Filter the events on the CloudFormation service and on the CloudFormation stack Amazon Resource Name (ARN).
- C. Create an Amazon CloudWatch alarm that monitors the metrics from CloudFormation. Filter the metrics on the stack name and the stack status. Configure the CloudWatch alarm to notify the QA team.
- D. Create an AWS Lambda function that notifies the QA team. Configure the event source mapping to receive events from CloudFormation. Specify the filtering values to limit invocations to the desired CloudFormation stack.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

A is correct.

upvoted 2 times

## Question #263

## Topic 1

A developer manages three AWS accounts. Each account contains an Amazon RDS DB instance in a private subnet. The developer needs to define users in each database in a consistent way. The developer must ensure that the same users are created and updated later in all three accounts.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an AWS CloudFormation template. Declare the users in the template. Attach the users to the database. Deploy the template in each account.
- B. Create an AWS CloudFormation template that contains a custom resource to create the users in the database. Deploy the template in each account.
- C. Write a script that creates the users. Deploy an Amazon EC2 instance in each account to run the script on the databases. Run the script in each account.
- D. Implement an AWS Lambda function that creates the users in the database. Provide the function with the details of all three accounts.

**Correct Answer: B***Community vote distribution* B (100%) **CrescentShared** 1 week, 4 days ago**Selected Answer: B**

CloudFormation itself does not natively manage database users within RDS. You would need a custom resource or some additional automation to create users within the RDS instance.

upvoted 2 times

## Question #264

## Topic 1

A company is building a new application that runs on AWS and uses Amazon API Gateway to expose APIs. Teams of developers are working on separate components of the application in parallel. The company wants to publish an API without an integrated backend so that teams that depend on the application backend can continue the development work before the API backend development is complete.

Which solution will meet these requirements?

- A. Create API Gateway resources and set the integration type value to MOCK. Configure the method integration request and integration response to associate a response with an HTTP status code. Create an API Gateway stage and deploy the API.
- B. Create an AWS Lambda function that returns mocked responses and various HTTP status codes. Create API Gateway resources and set the integration type value to AWS\_PROXY. Deploy the API.
- C. Create an EC2 application that returns mocked HTTP responses. Create API Gateway resources and set the integration type value to AWS. Create an API Gateway stage and deploy the API.
- D. Create API Gateway resources and set the integration type value set to HTTP\_PROXY. Add mapping templates and deploy the API. Create an AWS Lambda layer that returns various HTTP status codes. Associate the Lambda layer with the API deployment.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 ANDRES715 4 days, 4 hours ago

**Selected Answer: A**

Al crear recursos de API Gateway y establecer el tipo de integración en MOCK, se puede simular la respuesta de la API sin necesidad de un backend real. Esto permite que los equipos de desarrollo trabajen en paralelo en componentes separados de la aplicación y continúen el trabajo de desarrollo antes de que se complete el backend de la API.

upvoted 1 times

 CrescentShared 1 week, 4 days ago

**Selected Answer: A**

Duplicated question.

upvoted 1 times

## Question #265

## Topic 1

An application that runs on AWS receives messages from an Amazon Simple Queue Service (Amazon SQS) queue and processes the messages in batches. The application sends the data to another SQS queue to be consumed by another legacy application. The legacy system can take up to 5 minutes to process some transaction data.

A developer wants to ensure that there are no out-of-order updates in the legacy system. The developer cannot alter the behavior of the legacy system.

Which solution will meet these requirements?

- A. Use an SQS FIFO queue. Configure the visibility timeout value.
- B. Use an SQS standard queue with a SendMessageBatchRequestEntry data type. Configure the DelaySeconds values.
- C. Use an SQS standard queue with a SendMessageBatchRequestEntry data type. Configure the visibility timeout value.
- D. Use an SQS FIFO queue. Configure the DelaySeconds value.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 ANDRES715 4 days, 4 hours ago

**Selected Answer: A**

Al utilizar una cola SQS FIFO, se garantiza que los mensajes se procesen en el orden en que se reciben. Esto evita actualizaciones desordenadas en el sistema heredado y asegura la coherencia en el procesamiento de los datos de transacciones.

Además, al configurar el valor del tiempo de espera de visibilidad, se puede controlar el tiempo durante el cual un mensaje permanece invisible para otros consumidores después de que un consumidor lo recibe. Esto permite que el sistema heredado tenga hasta 5 minutos para procesar algunos datos de transacciones antes de que estén disponibles para otros consumidores.

upvoted 1 times

 CrescentShared 1 week, 4 days ago

**Selected Answer: A**

A is correct

upvoted 1 times

## Question #266

## Topic 1

A company is building a compute-intensive application that will run on a fleet of Amazon EC2 instances. The application uses attached Amazon Elastic Block Store (Amazon EBS) volumes for storing data. The Amazon EBS volumes will be created at time of initial deployment. The application will process sensitive information. All of the data must be encrypted. The solution should not impact the application's performance.

Which solution will meet these requirements?

- A. Configure the fleet of EC2 instances to use encrypted EBS volumes to store data.
- B. Configure the application to write all data to an encrypted Amazon S3 bucket.
- C. Configure a custom encryption algorithm for the application that will encrypt and decrypt all data.
- D. Configure an Amazon Machine Image (AMI) that has an encrypted root volume and store the data to ephemeral disks.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

Option B is not ideal because writing all data to an S3 bucket would introduce network latency and might impact performance. By default, Amazon EBS volumes can only be attached to one EC2 instance at a time, and they cannot be mounted to multiple instances simultaneously. However, AWS does offer a feature called Amazon EBS Multi-Attach, which allows you to attach a Provisioned IOPS SSD (io1 or io2) EBS volume to up to 16 Nitro-based EC2 instances within the same Availability Zone. This feature is designed for applications that require concurrent access to the same data from multiple instances, such as clustered databases or parallel file systems.

upvoted 2 times

## Question #267

## Topic 1

A developer is updating the production version of an AWS Lambda function to fix a defect. The developer has tested the updated code in a test environment. The developer wants to slowly roll out the updates to a small subset of production users before rolling out the changes to all users. Only 10% of the users should be initially exposed to the new code in production.

Which solution will meet these requirements?

- A. Update the Lambda code and create a new version of the Lambda function. Create a Lambda function trigger. Configure the traffic weights in the trigger between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.
- B. Create a new Lambda function that uses the updated code. Create a Lambda alias for the production Lambda function. Configure the Lambda alias to send 90% of the traffic to the production Lambda function, and send 10% of the traffic to the test Lambda function.
- C. Update the Lambda code and create a new version of the Lambda function. Create a Lambda proxy integration. Configure the Lambda proxy to split traffic between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.
- D. Update the Lambda code and create a new version of the Lambda function. Create a Lambda function alias. Configure the traffic weights in the Lambda alias between the two Lambda function versions. Send 90% of the traffic to the production version, and send 10% of the traffic to the new version.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: D**

D is correct.

upvoted 1 times

## Question #268

## Topic 1

A developer is creating an AWS Lambda function that consumes messages from an Amazon Simple Queue Service (Amazon SQS) standard queue. The developer notices that the Lambda function processes some messages multiple times.

How should developer resolve this issue MOST cost-effectively?

- A. Change the Amazon SQS standard queue to an Amazon SQS FIFO queue by using the Amazon SQS message deduplication ID.
- B. Set up a dead-letter queue.
- C. Set the maximum concurrency limit of the AWS Lambda function to 1.
- D. Change the message processing to use Amazon Kinesis Data Streams instead of Amazon SQS.

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

A is correct.

upvoted 2 times

## Question #269

## Topic 1

A developer is optimizing an AWS Lambda function and wants to test the changes in production on a small percentage of all traffic. The Lambda function serves requests to a REST API in Amazon API Gateway. The developer needs to deploy their changes and perform a test in production without changing the API Gateway URL.

Which solution will meet these requirements?

- A. Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. On the production API Gateway stage, define a canary release and set the percentage of traffic to direct to the canary release. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Publish the API to the canary stage.
- B. Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Deploy a new API Gateway stage.
- C. Define an alias on the \$LATEST version of the Lambda function. Update the API Gateway endpoint to reference the new Lambda function alias. Upload and publish the optimized Lambda function code. On the production API Gateway stage, define a canary release and set the percentage of traffic to direct to the canary release. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Publish to the canary stage.
- D. Define a function version for the currently deployed production Lambda function. Update the API Gateway endpoint to reference the new Lambda function version. Upload and publish the optimized Lambda function code. Update the API Gateway endpoint to use the \$LATEST version of the Lambda function. Deploy the API to the production API Gateway stage.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **ANDRES715** 4 days, 4 hours ago

**Selected Answer: C**

Al definir un alias en la versión \$LATEST de la función Lambda, el desarrollador puede referenciar este alias en el punto final de API Gateway. Luego, al cargar y publicar el código de función Lambda optimizado, se asegura de que la API Gateway haga referencia al nuevo alias de la función Lambda.

Después, en la etapa de producción de API Gateway, se puede definir una versión canary y establecer el porcentaje de tráfico que se dirigirá a la versión canary. Esto permite probar los cambios en producción en un pequeño porcentaje del tráfico sin cambiar la URL de API Gateway.

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: C**

A also looks good, C has an alias created and more like a practical way.

upvoted 1 times

## Question #270

## Topic 1

A company notices that credentials that the company uses to connect to an external software as a service (SaaS) vendor are stored in a configuration file as plaintext.

The developer needs to secure the API credentials and enforce automatic credentials rotation on a quarterly basis.

Which solution will meet these requirements MOST securely?

- A. Use AWS Key Management Service (AWS KMS) to encrypt the configuration file. Decrypt the configuration file when users make API calls to the SaaS vendor. Enable rotation.
- B. Retrieve temporary credentials from AWS Security Token Service (AWS STS) every 15 minutes. Use the temporary credentials when users make API calls to the SaaS vendor.
- C. Store the credentials in AWS Secrets Manager and enable rotation. Configure the API to have Secrets Manager access.
- D. Store the credentials in AWS Systems Manager Parameter Store and enable rotation. Retrieve the credentials when users make API calls to the SaaS vendor.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: C**

A too much effort.  
upvoted 2 times

## Question #271

## Topic 1

A company has an application that is hosted on Amazon EC2 instances. The application stores objects in an Amazon S3 bucket and allows users to download objects from the S3 bucket. A developer turns on S3 Block Public Access for the S3 bucket. After this change, users report errors when they attempt to download objects. The developer needs to implement a solution so that only users who are signed in to the application can access objects in the S3 bucket.

Which combination of steps will meet these requirements in the MOST secure way? (Choose two.)

- A. Create an EC2 instance profile and role with an appropriate policy. Associate the role with the EC2 instances.
- B. Create an IAM user with an appropriate policy. Store the access key ID and secret access key on the EC2 instances.
- C. Modify the application to use the S3 GeneratePresignedUrl API call.
- D. Modify the application to use the S3 GetObject API call and to return the object handle to the user.
- E. Modify the application to delegate requests to the S3 bucket.

**Correct Answer: A E**

*Community vote distribution*



ANDRES715 4 days, 4 hours ago

**Selected Answer: BC**

Cree un usuario de IAM con una política adecuada (opción B): El desarrollador debe crear un usuario de IAM en AWS con una política que permita el acceso a los objetos del depósito S3 solo a los usuarios autenticados en la aplicación. Esta política debe tener permisos adecuados para acceder y descargar objetos del depósito S3.

Modifique la aplicación para utilizar la llamada API S3 GeneratePresignedUrl (opción C): El desarrollador debe modificar la aplicación para utilizar la llamada API S3 GeneratePresignedUrl. Esta llamada generará una URL prefirmada que contiene una firma de seguridad y un tiempo de expiración. Solo los usuarios autenticados que tengan acceso a esta URL prefirmada podrán descargar los objetos del depósito S3.

upvoted 1 times

CrescentShared 1 week, 4 days ago

**Selected Answer: AC**

Option E: Modifying the application to delegate requests to the S3 bucket is less secure than using pre-signed URLs. If the application acts as a proxy for S3 requests, it would need to handle the data transfer from S3 to the user, which can increase the load on the application and potentially expose the application to additional security risks.

upvoted 1 times

## Question #272

## Topic 1

An Amazon Simple Queue Service (Amazon SQS) queue serves as an event source for an AWS Lambda function. In the SQS queue, each item corresponds to a video file that the Lambda function must convert to a smaller resolution. The Lambda function is timing out on longer video files, but the Lambda function's timeout is already configured to its maximum value.

What should a developer do to avoid the timeouts without additional code changes?

- A. Increase the memory configuration of the Lambda function.
- B. Increase the visibility timeout on the SQS queue.
- C. Increase the instance size of the host that runs the Lambda function.
- D. Use multi-threading for the conversion.

**Correct Answer:** D

*Community vote distribution*

A (100%)

✉️  **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

Increasing memory will also increase CPU, thereby optimizing performance of Lambda function  
upvoted 1 times

✉️  **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

"Without any additional code changes."  
upvoted 4 times

## Question #273

## Topic 1

A company is building an application on AWS. The application's backend includes an Amazon API Gateway REST API. The company's frontend application developers cannot continue work until the backend API is ready for integration. The company needs a solution that will allow the frontend application developers to continue their work.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Configure mock integrations for API Gateway API methods.
- B. Integrate a Lambda function with API Gateway and return a mocked response.
- C. Add new API endpoints to the API Gateway stage and returns a mocked response.
- D. Configure a proxy resource for API Gateway API methods.

**Correct Answer:** D

*Community vote distribution*

A (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

mock integration

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

Duplicated questions.

upvoted 1 times

## Question #274

## Topic 1

A company is preparing to migrate an application to the company's first AWS environment. Before this migration, a developer is creating a proof-of-concept application to validate a model for building and deploying container-based applications on AWS.

Which combination of steps should the developer take to deploy the containerized proof-of-concept application with the LEAST operational effort? (Choose two.)

- A. Package the application into a .zip file by using a command line tool. Upload the package to Amazon S3.
- B. Package the application into a container image by using the Docker CLI. Upload the image to Amazon Elastic Container Registry (Amazon ECR).
- C. Deploy the application to an Amazon EC2 instance by using AWS CodeDeploy.
- D. Deploy the application to Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.
- E. Deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

**Correct Answer:** BD

*Community vote distribution*

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证  
微信添加 hello231119

BE (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: BE**

E corresponds to actions in B  
upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: BE**

Why D? Is EKS necessary?  
upvoted 2 times

## Question #275

## Topic 1

A developer supports an application that accesses data in an Amazon DynamoDB table. One of the item attributes is expirationDate in the timestamp format. The application uses this attribute to find items, archive them, and remove them from the table based on the timestamp value.

The application will be decommissioned soon, and the developer must find another way to implement this functionality. The developer needs a solution that will require the least amount of code to write.

Which solution will meet these requirements?

- A. Enable TTL on the expirationDate attribute in the table. Create a DynamoDB stream. Create an AWS Lambda function to process the deleted items. Create a DynamoDB trigger for the Lambda function.
- B. Create two AWS Lambda functions: one to delete the items and one to process the items. Create a DynamoDB stream. Use the DeleteItem API operation to delete the items based on the expirationDate attribute. Use the GetRecords API operation to get the items from the DynamoDB stream and process them.
- C. Create two AWS Lambda functions: one to delete the items and one to process the items. Create an Amazon EventBridge scheduled rule to invoke the Lambda functions. Use the DeleteItem API operation to delete the items based on the expirationDate attribute. Use the GetRecords API operation to get the items from the DynamoDB table and process them.
- D. Enable TTL on the expirationDate attribute in the table. Specify an Amazon Simple Queue Service (Amazon SQS) dead-letter queue as the target to delete the items. Create an AWS Lambda function to process the items.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

Not sure why C. A can totally handle this.

upvoted 3 times

## Question #276

## Topic 1

A developer needs to implement a custom machine learning (ML) library in an application. The size of the library is 15 GB. The size of the library is increasing. The application uses AWS Lambda functions. All the Lambda functions must have access to the library.

Which solution will meet these requirements?

- A. Save the library in Lambda layers. Attach the layers to all Lambda functions.
- B. Save the library in Amazon S3. Download the library from Amazon S3 inside the Lambda function.
- C. Save the library as a Lambda container image. Redeploy the Lambda functions with the new image.
- D. Save the library in an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all the Lambda functions.

**Correct Answer:** D

*Community vote distribution*

D (50%) A (50%)

 **ANDRES715** 3 days, 4 hours ago

**Selected Answer: A**

La solución recomendada para este caso es guardar la biblioteca en capas Lambda y adjuntar esas capas a todas las funciones Lambda. Esto permitirá que todas las funciones Lambda tengan acceso a la biblioteca sin necesidad de duplicarla en cada función.

Las capas Lambda son una forma de compartir código y bibliotecas comunes entre varias funciones Lambda. Puedes crear una capa Lambda que contenga la biblioteca de aprendizaje automático y luego adjuntar esa capa a todas las funciones Lambda que necesiten acceder a ella.

Al utilizar capas Lambda, puedes reducir el tamaño de las funciones Lambda y simplificar su mantenimiento. Además, si el tamaño de la biblioteca está aumentando, puedes actualizar la capa Lambda sin tener que modificar y volver a implementar todas las funciones Lambda.

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: D**

S3 takes too long.

upvoted 1 times

## Question #277

## Topic 1

A developer is designing a serverless application for a game in which users register and log in through a web browser. The application makes requests on behalf of users to a set of AWS Lambda functions that run behind an Amazon API Gateway HTTP API.

The developer needs to implement a solution to register and log in users on the application's sign-in page. The solution must minimize operational overhead and must minimize ongoing management of user identities.

Which solution will meet these requirements?

- A. Create Amazon Cognito user pools for external social identity providers. Configure IAM roles for the identity pools.
- B. Program the sign-in page to create users' IAM groups with the IAM roles attached to the groups.
- C. Create an Amazon RDS for SQL Server DB instance to store the users and manage the permissions to the backend resources in AWS.
- D. Configure the sign-in page to register and store the users and their passwords in an Amazon DynamoDB table with an attached IAM policy.

**Correct Answer:** C

*Community vote distribution*

A (100%)

✉️ ANDRES715 3 days, 4 hours ago

**Selected Answer: A**

Amazon Cognito es un servicio de AWS que permite agregar fácilmente la funcionalidad de registro e inicio de sesión a las aplicaciones. Puedes utilizar proveedores de identidades sociales externos, como Google, Facebook o Amazon, para permitir que los usuarios se registren e inicien sesión en tu aplicación.

Al crear grupos de usuarios en Amazon Cognito y asignar roles de IAM a esos grupos, puedes gestionar de manera eficiente los permisos y accesos de los usuarios a los recursos backend en AWS. Esto te permite minimizar los gastos operativos y la gestión continua de las identidades de los usuarios.

upvoted 1 times

✉️ monishvster 3 days, 5 hours ago

**Selected Answer: A**

Cognito is the answer

upvoted 1 times

✉️ CrescentShared 1 week, 4 days ago

**Selected Answer: A**

Anybody has an idea why it is C?

upvoted 1 times

## Question #278

## Topic 1

A company has a web application that is hosted on Amazon EC2 instances. The EC2 instances are configured to stream logs to Amazon CloudWatch Logs. The company needs to receive an Amazon Simple Notification Service (Amazon SNS) notification when the number of application error messages exceeds a defined threshold within a 5-minute period.

Which solution will meet these requirements?

- A. Rewrite the application code to stream application logs to Amazon SNS. Configure an SNS topic to send a notification when the number of errors exceeds the defined threshold within a 5-minute period.
- B. Configure a subscription filter on the CloudWatch Logs log group. Configure the filter to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.
- C. Install and configure the Amazon Inspector agent on the EC2 instances to monitor for errors. Configure Amazon Inspector to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.
- D. Create a CloudWatch metric filter to match the application error pattern in the log data. Set up a CloudWatch alarm based on the new custom metric. Configure the alarm to send an SNS notification when the number of errors exceeds the defined threshold within a 5-minute period.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **Moumita** Highly Voted 3 weeks, 2 days ago

Correct Answer is D

upvoted 6 times

 **monishvster** Most Recent 3 days, 5 hours ago

Selected Answer: D

Should be D

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

Selected Answer: D

Should be D

upvoted 3 times

## Question #279

## Topic 1

A photo sharing application uses Amazon S3 to store image files. All user images are manually audited for inappropriate content by a third-party company. The audits are completed 1-24 hours after user upload and the results are written to an Amazon DynamoDB table, which uses the S3 object key as a primary key. The database items can be queried by using a REST API created by the third-party company.

An application developer needs to implement an automated process to tag all S3 objects with the results of the content audit.

What should the developer do to meet these requirements in the MOST operationally efficient way?

- A. Create an AWS Lambda function to run in response to the s3:ObjectCreated event type. Write the S3 key to an Amazon Simple Queue Service (Amazon SQS) queue with a visibility timeout of 24 hours. Create and configure a second Lambda function to read items from the queue. Retrieve the results for each item from the DynamoDB table. Tag each S3 object accordingly.
- B. Create an AWS Lambda function to run in response to the s3:ObjectCreated event type. Integrate the function into an AWS Step Functions standard workflow. Define an AWS Step Functions Wait state and set the value to 24 hours. Create and configure a second Lambda function to retrieve the audit results and tag the S3 objects accordingly after the Wait state is over.
- C. Create an AWS Lambda function to load all untagged S3 objects. Retrieve the results for each item from the REST API and tag each S3 object accordingly. Create and configure an Amazon EventBridge rule to run at regular intervals. Set the Lambda function as a target for the EventBridge rule.
- D. Launch an Amazon EC2 instance. Deploy a script to the EC2 instance to use the external database results to tag the S3 objects accordingly. Configure a crontab file to run the script at regular intervals.

**Correct Answer: A***Community vote distribution*

✉️ **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

Should be A

upvoted 1 times

✉️ **Jisking** 3 days, 17 hours ago

**Selected Answer: B**

I may choose B.

upvoted 1 times

✉️ **CrescentShared** 1 week, 4 days ago

**Selected Answer: C**

A does not make any sense.

upvoted 1 times

## Question #280

## Topic 1

A company has built an AWS Lambda function to convert large image files into output files that can be used in a third-party viewer application. The company recently added a new module to the function to improve the output of the generated files. However, the new module has increased the bundle size and has increased the time that is needed to deploy changes to the function code.

How can a developer increase the speed of the Lambda function deployment?

- A. Use AWS CodeDeploy to deploy the function code.
- B. Use Lambda layers to package and load dependencies.
- C. Increase the memory size of the function.
- D. Use Amazon S3 to host the function dependencies.

**Correct Answer:** D

*Community vote distribution*

 B (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: B**

Must be B

upvoted 3 times

## Question #281

## Topic 1

A developer creates a static website for their department. The developer deploys the static assets for the website to an Amazon S3 bucket and serves the assets with Amazon CloudFront. The developer uses origin access control (OAC) on the CloudFront distribution to access the S3 bucket.

The developer notices users can access the root URL and specific pages but cannot access directories without specifying a file name. For example, /products/index.html works, but /products/ returns an error. The developer needs to enable accessing directories without specifying a file name without exposing the S3 bucket publicly.

Which solution will meet these requirements?

- A. Update the CloudFront distribution's settings to index.html as the default root object is set.
- B. Update the Amazon S3 bucket settings and enable static website hosting. Specify index.html as the Index document. Update the S3 bucket policy to enable access. Update the CloudFront distribution's origin to use the S3 website endpoint.
- C. Create a CloudFront function that examines the request URL and appends index.html when directories are being accessed. Add the function as a viewer request CloudFront function to the CloudFront distribution's behavior.
- D. Create a custom error response on the CloudFront distribution with the HTTP error code set to the HTTP 404 Not Found response code and the response page path to /index.html. Set the HTTP response code to the HTTP 200 OK response code.

**Correct Answer: B**

*Community vote distribution*

C (67%)

B (33%)

 **HD98** 1 day, 20 hours ago

C is the right option

upvoted 1 times

 **ANDRES715** 3 days, 4 hours ago

**Selected Answer: B**

Al habilitar el alojamiento de sitios web estáticos en el depósito de Amazon S3 y especificar index.html como documento de índice, se permite el acceso a los directorios sin especificar un nombre de archivo. Al mismo tiempo, al actualizar la política del depósito S3 para habilitar el acceso y el origen de la distribución de CloudFront para utilizar el punto final del sitio web de S3, se garantiza que el acceso se gestione de manera segura sin exponer públicamente el depósito de S3.

upvoted 1 times

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: C**

When you enable static website hosting on an S3 bucket, you can specify an index document, which S3 automatically returns when a user requests a directory. However, changing the CloudFront origin to the S3 website endpoint would expose the S3 bucket publicly, which contradicts the requirement to keep the S3 bucket private.

upvoted 2 times

 **HD98** 1 day, 20 hours ago

C correct

upvoted 1 times

## Question #282

## Topic 1

A developer is testing a RESTful application that is deployed by using Amazon API Gateway and AWS Lambda. When the developer tests the user login by using credentials that are not valid, the developer receives an HTTP 405: METHOD\_NOT\_ALLOWED error. The developer has verified that the test is sending the correct request for the resource.

Which HTTP error should the application return in response to the request?

- A. HTTP 401
- B. HTTP 404
- C. HTTP 503
- D. HTTP 505

**Correct Answer: A**

*Community vote distribution*



A (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: A**

C. HTTP 503: Service Unavailable - This status code indicates that the server is not ready to handle the request. It is usually a temporary state, often due to maintenance or overloading.

D. HTTP 505: HTTP Version Not Supported - This status code means that the server does not support the HTTP protocol version used in the request. It is a rare occurrence and typically indicates that the client is using an outdated or unsupported version of HTTP.

upvoted 3 times

## Question #283

## Topic 1

A developer must use multi-factor authentication (MFA) to access data in an Amazon S3 bucket that is in another AWS account.

Which AWS Security Token Service (AWS STS) API operation should the developer use with the MFA information to meet this requirement?

- A. AssumeRoleWithWebIdentity
- B. GetFederationToken
- C. AssumeRoleWithSAML
- D. AssumeRole

**Correct Answer: B**

*Community vote distribution*



D (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: D**

answer Is D

upvoted 3 times

## Question #284

## Topic 1

A developer designed an application on an Amazon EC2 instance. The application makes API requests to objects in an Amazon S3 bucket.

Which combination of steps will ensure that the application makes the API requests in the MOST secure manner? (Choose two.)

- A. Create an IAM user that has permissions to the S3 bucket. Add the user to an IAM group.
- B. Create an IAM role that has permissions to the S3 bucket.
- C. Add the IAM role to an instance profile. Attach the instance profile to the EC2 instance.
- D. Create an IAM role that has permissions to the S3 bucket. Assign the role to an IAM group.
- E. Store the credentials of the IAM user in the environment variables on the EC2 instance.

**Correct Answer:** BC

*Community vote distribution*

BC (100%)

 **CrescentShared** 1 week, 4 days ago

**Selected Answer: BC**

BC is correct

upvoted 2 times

## Question #285

## Topic 1

An AWS Lambda function requires read access to an Amazon S3 bucket and requires read/write access to an Amazon DynamoDB table. The correct IAM policy already exists.

What is the MOST secure way to grant the Lambda function access to the S3 bucket and the DynamoDB table?

- A. Attach the existing IAM policy to the Lambda function.
- B. Create an IAM role for the Lambda function. Attach the existing IAM policy to the role. Attach the role to the Lambda function.
- C. Create an IAM user with programmatic access. Attach the existing IAM policy to the user. Add the user access key ID and secret access key as environment variables in the Lambda function.
- D. Add the AWS account root user access key ID and secret access key as encrypted environment variables in the Lambda function.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: B**

must be b

upvoted 2 times

## Question #286

## Topic 1

A developer is using AWS Step Functions to automate a workflow. The workflow defines each step as an AWS Lambda function task. The developer notices that runs of the Step Functions state machine fail in the GetResource task with either an `IllegalArgumentException` error or a `TooManyRequestsException` error.

The developer wants the state machine to stop running when the state machine encounters an `IllegalArgumentException` error. The state machine needs to retry the GetResource task one additional time after 10 seconds if the state machine encounters a `TooManyRequestsException` error. If the second attempt fails, the developer wants the state machine to stop running.

How can the developer implement the Lambda retry functionality without adding unnecessary complexity to the state machine?

- A. Add a Delay task after the GetResource task. Add a catcher to the GetResource task. Configure the catcher with an error type of `TooManyRequestsException`. Configure the next step to be the Delay task. Configure the Delay task to wait for an interval of 10 seconds. Configure the next step to be the GetResource task.
- B. Add a catcher to the GetResource task. Configure the catcher with an error type of `TooManyRequestsException`, an interval of 10 seconds, and a maximum attempts value of 1. Configure the next step to be the GetResource task.
- C. Add a retrier to the GetResource task. Configure the retrier with an error type of `TooManyRequestsException`, an interval of 10 seconds, and a maximum attempts value of 1.
- D. Duplicate the GetResource task. Rename the new GetResource task to TryAgain. Add a catcher to the original GetResource task. Configure the catcher with an error type of `TooManyRequestsException`. Configure the next step to be TryAgain.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: C**

Should be C  
upvoted 1 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: C**

Should be C  
upvoted 1 times

## Question #287

## Topic 1

A developer is creating a serverless application that uses an AWS Lambda function. The developer will use AWS CloudFormation to deploy the application. The application will write logs to Amazon CloudWatch Logs. The developer has created a log group in a CloudFormation template for the application to use. The developer needs to modify the CloudFormation template to make the name of the log group available to the application at runtime.

Which solution will meet this requirement?

- A. Use the AWS::Include transform in CloudFormation to provide the log group's name to the application.
- B. Pass the log group's name to the application in the user data section of the CloudFormation template.
- C. Use the CloudFormation template's Mappings section to specify the log group's name for the application.
- D. Pass the log group's Amazon Resource Name (ARN) as an environment variable to the Lambda function.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: D**

User data is typically used to pass startup scripts to EC2 instances, not Lambda functions. This would not be the appropriate mechanism for a serverless application using Lambda. The Mappings section in a CloudFormation template is used to define sets of key-value pairs that can be used to specify conditional parameter values based on region or other criteria. It doesn't provide a direct way to make the log group's name available to the Lambda function at runtime.

upvoted 3 times

## Question #288

## Topic 1

A developer is creating an Amazon DynamoDB table by using the AWS CLI. The DynamoDB table must use server-side encryption with an AWS owned encryption key.

How should the developer create the DynamoDB table to meet these requirements?

- A. Create an AWS Key Management Service (AWS KMS) customer managed key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- B. Create an AWS Key Management Service (AWS KMS) AWS managed key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- C. Create an AWS owned key. Provide the key's Amazon Resource Name (ARN) in the KMSMasterKeyId parameter during creation of the DynamoDB table.
- D. Create the DynamoDB table with the default encryption options.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: D**

D is good enough to meet the requirement.

upvoted 1 times

## Question #289

## Topic 1

A company has an application that runs across multiple AWS Regions. The application is experiencing performance issues at irregular intervals. A developer must use AWS X-Ray to implement distributed tracing for the application to troubleshoot the root cause of the performance issues.

What should the developer do to meet this requirement?

- A. Use the X-Ray console to add annotations for AWS services and user-defined services.
- B. Use Region annotation that X-Ray adds automatically for AWS services. Add Region annotation for user-defined services.
- C. Use the X-Ray daemon to add annotations for AWS services and user-defined services.
- D. Use Region annotation that X-Ray adds automatically for user-defined services. Configure X-Ray to add Region annotation for AWS services.

**Correct Answer: B**

*Community vote distribution*

**B (100%)**

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: B**

User defined has to be in sdk.

upvoted 2 times

## Question #290

## Topic 1

A company runs an application on AWS. The application uses an AWS Lambda function that is configured with an Amazon Simple Queue Service (Amazon SQS) queue called high priority queue as the event source. A developer is updating the Lambda function with another SQS queue called low priority queue as the event source. The Lambda function must always read up to 10 simultaneous messages from the high priority queue before processing messages from low priority queue. The Lambda function must be limited to 100 simultaneous invocations.

Which solution will meet these requirements?

- A. Set the event source mapping batch size to 10 for the high priority queue and to 90 for the low priority queue.
- B. Set the delivery delay to 0 seconds for the high priority queue and to 10 seconds for the low priority queue.
- C. Set the event source mapping maximum concurrency to 10 for the high priority queue and to 90 for the low priority queue.
- D. Set the event source mapping batch window to 10 for the high priority queue and to 90 for the low priority queue.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: C**

Should be C

upvoted 1 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: C**

None of them seems to be guarantee the requirement.

Set the reserved concurrency on the Lambda function to 100 to limit the total invocations across all triggers.

Configure the event source mapping for the high priority queue to use a maximum concurrency that ensures its messages are processed first. This could be most of the reserved concurrency (but not all, to allow for some processing of the low priority queue).

Configure the event source mapping for the low priority queue with a smaller maximum concurrency to ensure it doesn't starve the high priority queue of Lambda resources.

upvoted 2 times

## Question #291

## Topic 1

A data visualization company wants to strengthen the security of its core applications. The applications are deployed on AWS across its development, staging, pre-production, and production environments. The company needs to encrypt all of its stored sensitive credentials. The sensitive credentials need to be automatically rotated. A version of the sensitive credentials need to be stored for each environment.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Configure AWS Secrets Manager versions to store different copies of the same credentials across multiple environments.
- B. Create a new parameter version in AWS Systems Manager Parameter Store for each environment. Store the environment-specific credentials in the parameter version.
- C. Configure the environment variables in the application code. Use different names for each environment type.
- D. Configure AWS Secrets Manager to create a new secret for each environment type. Store the environment-specific credentials in the secret.

**Correct Answer: C***Community vote distribution* D (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: D**

Should be D

upvoted 1 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: D**

C does not make sense.

upvoted 2 times

## Question #292

## Topic 1

A developer is investigating an issue in part of a company's application. In the application, messages are sent to an Amazon Simple Queue Service (Amazon SQS) queue. The AWS Lambda function polls messages from the SQS queue and sends email messages by using Amazon Simple Email Service (Amazon SES). Users have been receiving duplicate email messages during periods of high traffic.

Which reasons could explain the duplicate email messages? (Choose two.)

- A. Standard SQS queues support at-least-once message delivery.
- B. Standard SQS queues support exactly-once processing, so the duplicate email messages are because of user error.
- C. Amazon SES has the DomainKeys Identified Mail (DKIM) authentication incorrectly configured.
- D. The SQS queue's visibility timeout is lower than or the same as the Lambda function's timeout.
- E. The Amazon SES bounce rate metric is too high.

**Correct Answer: AD***Community vote distribution* AD (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: AD**

AD is correct.

upvoted 3 times

## Question #293

## Topic 1

A developer is deploying a company's application to Amazon EC2 instances. The application generates gigabytes of data files each day. The files are rarely accessed, but the files must be available to the application's users within minutes of a request during the first year of storage. The company must retain the files for 7 years.

How can the developer implement the application to meet these requirements MOST cost-effectively?

- A. Store the files in an Amazon S3 bucket. Use the S3 Glacier Instant Retrieval storage class. Create an S3 Lifecycle policy to transition the files to the S3 Glacier Deep Archive storage class after 1 year.
- B. Store the files in an Amazon S3 bucket. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition the files to the S3 Glacier Flexible Retrieval storage class after 1 year.
- C. Store the files on an Amazon Elastic Block Store (Amazon EBS) volume. Use Amazon Data Lifecycle Manager (Amazon DLM) to create snapshots of the EBS volumes and to store those snapshots in Amazon S3.
- D. Store the files on an Amazon Elastic File System (Amazon EFS) mount. Configure EFS lifecycle management to transition the files to the EFS Standard- Infrequent Access (Standard-IA) storage class after 1 year.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

Should be A

upvoted 1 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: A**

Must be A

upvoted 2 times

## Question #294

## Topic 1

A company's developer has deployed an application in AWS by using AWS CloudFormation. The CloudFormation stack includes parameters in AWS Systems Manager Parameter Store that the application uses as configuration settings. The application can modify the parameter values.

When the developer updated the stack to create additional resources with tags, the developer noted that the parameter values were reset and that the values ignored the latest changes made by the application. The developer needs to change the way the company deploys the CloudFormation stack. The developer also needs to avoid resetting the parameter values outside the stack.

Which solution will meet these requirements with the LEAST development effort?

- A. Modify the CloudFormation stack to set the deletion policy to Retain for the Parameter Store parameters.
- B. Create an Amazon DynamoDB table as a resource in the CloudFormation stack to hold configuration data for the application. Migrate the parameters that the application is modifying from Parameter Store to the DynamoDB table.
- C. Create an Amazon RDS DB instance as a resource in the CloudFormation stack. Create a table in the database for parameter configuration. Migrate the parameters that the application is modifying from Parameter Store to the configuration table.
- D. Modify the CloudFormation stack policy to deny updates on Parameter Store parameters.

**Correct Answer: C**

*Community vote distribution*



**monishvster** 3 days, 5 hours ago

**Selected Answer: A**

Should be A. As the developer also needs to avoid resetting the parameter values outside the stack.

upvoted 1 times

**CrescentShared** 1 week, 3 days ago

**Selected Answer: D**

It is D

upvoted 2 times

## Question #295

## Topic 1

A company has a social media application that receives large amounts of traffic. User posts and interactions are continuously updated in an Amazon RDS database. The data changes frequently, and the data types can be complex. The application must serve read requests with minimal latency.

The application's current architecture struggles to deliver these rapid data updates efficiently. The company needs a solution to improve the application's performance.

Which solution will meet these requirements?

- A. Use Amazon DynamoDB Accelerator (DAX) in front of the RDS database to provide a caching layer for the high volume of rapidly changing data.
- B. Set up Amazon S3 Transfer Acceleration on the RDS database to enhance the speed of data transfer from the databases to the application.
- C. Add an Amazon CloudFront distribution in front of the RDS database to provide a caching layer for the high volume of rapidly changing data.
- D. Create an Amazon ElastiCache for Redis cluster. Update the application code to use a write-through caching strategy and read the data from Redis.

**Correct Answer:** C

*Community vote distribution*



✉️ ANDRES715 3 days, 3 hours ago

**Selected Answer: R**

R. Utilice Amazon DynamoDB Accelerator (DAX) frente a la base de datos RDS para proporcionar una capa de almacenamiento en caché para el gran volumen de datos que cambian rápidamente.

Al utilizar Amazon DynamoDB Accelerator (DAX) frente a la base de datos RDS, se puede proporcionar una capa de almacenamiento en caché para el gran volumen de datos que cambian rápidamente. DAX mejora el rendimiento de las consultas de lectura al almacenar en caché los resultados de las consultas más frecuentes, lo que reduce la latencia y mejora la capacidad de respuesta de la aplicación.

Es importante tener en cuenta que DynamoDB Accelerator (DAX) es una opción eficiente para mejorar el rendimiento de aplicaciones que requieren un acceso rápido a datos que cambian con frecuencia, como en el caso de una aplicación de redes sociales.

upvoted 1 times

✉️ monishvster 3 days, 5 hours ago

**Selected Answer: D**

Should be D

upvoted 1 times

✉️ CrescentShared 1 week, 3 days ago

**Selected Answer: D**

hesitate between C and D.

upvoted 1 times

## Question #296

## Topic 1

A developer created an AWS Lambda function that performs a series of operations that involve multiple AWS services. The function's duration time is higher than normal. To determine the cause of the issue, the developer must investigate traffic between the services without changing the function code.

Which solution will meet these requirements?

- A. Enable AWS X-Ray active tracing in the Lambda function. Review the logs in X-Ray.
- B. Configure AWS CloudTrail. View the trail logs that are associated with the Lambda function.
- C. Review the AWS Config logs in Amazon CloudWatch.
- D. Review the Amazon CloudWatch logs that are associated with the Lambda function.

**Correct Answer:** D

*Community vote distribution*

A (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

Should be A

upvoted 1 times

 **hungnv6\_rikkei** 1 week ago

**Selected Answer: A**

A. Enable AWS X-Ray active tracing in the Lambda function. Review the logs in X-Ray.

X-Ray provides insights into the duration and performance of each component, helping you identify the root cause of performance issues without modifying the function code.

upvoted 2 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: A**

between the services

upvoted 2 times

## Question #297

## Topic 1

A company has on-premises data centers that run an image processing service. The service consists of containerized applications that run on Kubernetes clusters. All the applications have access to the same NFS share for files and data storage.

The company is running out of NFS capacity in the data centers and needs to migrate to AWS as soon as possible. The Kubernetes clusters must be highly available on AWS.

Which combination of actions will meet these requirements? (Choose two.)

- A. Transfer the information that is in the NFS share to an Amazon Elastic Block Store (Amazon EBS) volume. Upload the container images to Amazon Elastic Container Registry (Amazon ECR).
- B. Transfer the information that is in the NFS share to an Amazon Elastic File System (Amazon EFS) volume. Upload the container images to Amazon Elastic Container Registry (Amazon ECR).
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic Block Store (Amazon EBS) volume at the required path for the container images.
- D. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic Block Store (Amazon EBS) volume at the required path for the container images.
- E. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to run the applications. Configure each node of the cluster to mount the Amazon Elastic File System (Amazon EFS) volume at the required path for the container images.

**Correct Answer: A E**

*Community vote distribution*

BE (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: BE**

EFS is the key here  
upvoted 1 times

 **hungnv6\_rikkei** 1 week ago

**Selected Answer: BE**

Amazon Elastic File System (Amazon EFS) volume and Amazon Elastic Kubernetes Service (Amazon EKS)  
upvoted 1 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: BE**

EBS cannot be multi mounted.  
upvoted 1 times

## Question #298

## Topic 1

A company has an analytics application that uses an AWS Lambda function to process transaction data asynchronously. A developer notices that asynchronous invocations of the Lambda function sometimes fail. When failed Lambda function invocations occur, the developer wants to invoke a second Lambda function to handle errors and log details.

Which solution will meet these requirements?

- A. Configure a Lambda function destination with a failure condition. Specify Lambda function as the destination type. Specify the error-handling Lambda function's Amazon Resource Name (ARN) as the resource.
- B. Enable AWS X-Ray active tracing on the initial Lambda function. Configure X-Ray to capture stack traces of the failed invocations. Invoke the error-handling Lambda function by including the stack traces in the event object.
- C. Configure a Lambda function trigger with a failure condition. Specify Lambda function as the destination type. Specify the error-handling Lambda function's Amazon Resource Name (ARN) as the resource.
- D. Create a status check alarm on the initial Lambda function. Configure the alarm to invoke the error-handling Lambda function when the alarm is initiated. Ensure that the alarm passes the stack trace in the event object.

**Correct Answer:** D

*Community vote distribution*

A (100%)

 monishvster 3 days, 5 hours ago

**Selected Answer: A**

Should be A since Trigger is before execution  
upvoted 1 times

 CrescentShared 1 week, 3 days ago

**Selected Answer: A**

is not a valid approach because Lambda does not have a direct configuration for triggers based on failure conditions in the way described. The concept of a trigger is generally used for starting an invocation, not handling failures.  
upvoted 2 times

## Question #299

## Topic 1

A company introduced a new feature that should be accessible to only a specific group of premium customers. A developer needs the ability to turn the feature on and off in response to performance and feedback. The developer needs a solution to validate and deploy these configurations quickly without causing any disruptions.

What should the developer do to meet these requirements?

- A. Use AWS AppConfig to manage the feature configuration and to validate and deploy changes. Use feature flags to turn the feature on and off.
- B. Use AWS Secrets Manager to securely manage and validate the feature configurations. Enable lifecycle rules to turn the feature on and off.
- C. Use AWS Config to manage the feature configuration and validation. Set up AWS Config rules to turn the feature on and off based on predefined conditions.
- D. Use AWS Systems Manager Parameter Store to store and validate the configuration settings for the feature. Enable lifecycle rules to turn the feature on and off.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: A**

App COnfig is the one  
upvoted 1 times

## Question #300

## Topic 1

A developer needs approval from a product owner before the developer can deploy code for an application to production. The developer uses AWS CodePipeline to deploy the application. The developer configures an Amazon Simple Notification Service (Amazon SNS) topic to send notifications to the product owner.

Which solution is the MOST operationally efficient way for the developer to receive approval from the product owner?

- A. Add a new stage to CodePipeline before the production deployment. Add a manual approval action to the new stage. Add a new notification rule in the pipeline settings. Specify manual approval as the event that initiates the notification. Specify the SNS topic's Amazon Resource Name (ARN) to notify the product owner.
- B. Develop an AWS Step Functions state machine that sends a notification to the product owner and accepts an approval. Add a new stage to CodePipeline before the production deployment. Add the state machine as a Step Functions action to the new stage.
- C. Add a manual approval action to the existing production deployment stage in CodePipeline. Specify the SNS topic's Amazon Resource Name (ARN) while configuring the new manual approval action.
- D. Edit the settings in CodePipeline. Create a new notification rule. Specify manual approval as the event that initiates the notification. Create a new notification target. Specify the SNS topic to notify the product owner. Save the notification rule.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: A**

should be A

upvoted 2 times

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: A**

Adding a manual approval action to a pipeline stage, which is necessary for halting the pipeline to wait for approval.

upvoted 2 times

## Question #301

## Topic 1

A developer is building a serverless application on AWS for a workflow that processes high volumes of data. In the workflow, an AWS Step Functions state machine invokes several AWS Lambda functions.

One of the Lambda functions occasionally fails because of timeout errors during periods of high demand. The developer must ensure that the workflow automatically retries the failed function invocation if a timeout error occurs.

Which solution will meet this requirement?

- A. Add a Retry field in the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts and the timeout error type to retry on.
- B. Add a Timeout field in the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts.
- C. Add a Fail state to the Step Functions state machine definition. Configure the state machine with the maximum number of retry attempts.
- D. Update the Step Functions state machine to pass the invocation request to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe a Lambda function to the SNS topic. Configure the Lambda function with the maximum number of retry attempts for a timeout error type.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 3 days ago

**Selected Answer: A**

A is correct.

upvoted 2 times

## Question #302

## Topic 1

A company runs a serverless application on AWS. The application includes an AWS Lambda function. The Lambda function processes data and stores the data in an Amazon RDS for PostgreSQL database. A developer created a user credentials in the database for the application.

The developer needs to use AWS Secrets Manager to manage the user credentials. The password must be rotated on a regular basis. The solution needs to ensure that there is high availability and no downtime for the application during secret rotation.

What should the developer do to meet these requirements?

- A. Configure managed rotation with the single user rotation strategy.
- B. Configure managed rotation with the alternating users rotation strategy.
- C. Configure automatic rotation with the single user rotation strategy.
- D. Configure automatic rotation with the alternating users rotation strategy.

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证  
微信添加 hello231119

**Correct Answer: D**

*Community vote distribution*

D (75%)

B (25%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: B**

Both B and D options involve using the alternating users rotation strategy, which is suitable for ensuring high availability and no downtime during secret rotation. The difference between "managed rotation" and "automatic rotation" is mostly semantic in this context, as both terms refer to the capability of AWS Secrets Manager to automatically rotate the secret. The more common terminology used in the context of AWS Secrets Manager is "managed rotation," so option B is often preferred.

upvoted 1 times

 **tgv** 1 week, 6 days ago

**Selected Answer: D**

Managed rotation vs. automatic rotation:

Managed rotation requires manual intervention to specify when a secret should be rotated. This doesn't meet the requirement of automated password rotation on a regular basis.

Automatic rotation automatically rotates secrets based on a defined schedule, meeting the requirement for regular password changes.

Single user vs. alternating users:

Single user rotation means there is only one set of credentials. Rotating this would cause downtime as the application needs to update its connection information.

Alternating users rotation uses two sets of credentials. Only one is active at a time. When it's time to rotate, the inactive set is rotated, and then the application switches to using that set, avoiding downtime

upvoted 3 times

## Question #303

## Topic 1

A company runs an application on AWS. The application consists of a static website that is hosted on Amazon S3. The application includes Amazon API Gateway APIs that invoke AWS Lambda functions. During a period of high traffic on the application, application users reported that the application was slow at irregular intervals. There were no failed requests.

A developer needs to find the slow executions across all the Lambda functions.

Which solution will meet these requirements?

- A. Perform a query across all the Lambda function log groups by using Amazon CloudWatch Logs Insights. Filter on type of report and sort descending by Lambda function execution duration.
- B. Enable AWS CloudTrail Insights on the account where the Lambda functions are running. After CloudTrail Insights has finished processing, review CloudTrail Insights to find the anomalous functions.
- C. Enable AWS X-Ray for all the Lambda functions. Configure an X-Ray insight on a new group that includes all the Lambda functions. After the X-Ray insight has finished processing, review the X-Ray logs.
- D. Set up AWS Glue to crawl through the logs in Amazon CloudWatch Logs for the Lambda functions. Configure an AWS Glue job to transform the logs into a structured format and to output the logs into Amazon S3. Use the Amazon CloudWatch dashboard to visualize the slowest functions based on the duration.

**Correct Answer: B**

Community vote distribution



✉️ monishvster 3 days, 5 hours ago

**Selected Answer: C**

X-ray will provide better insights for performance  
upvoted 2 times

✉️ CrescentShared 1 week, 2 days ago

**Selected Answer: A**

Hesitate. A or C?  
upvoted 1 times

## Question #304

## Topic 1

A company is building a serverless application on AWS. The application uses Amazon API Gateway and AWS Lambda. The company wants to deploy the application to its development, test, and production environments.

Which solution will meet these requirements with the LEAST development effort?

- A. Use API Gateway stage variables and create Lambda aliases to reference environment-specific resources.
- B. Use Amazon Elastic Container Service (Amazon ECS) to deploy the application to the environments.
- C. Duplicate the code for each environment. Deploy the code to a separate API Gateway stage.
- D. Use AWS Elastic Beanstalk to deploy the application to the environments.

**Correct Answer:** B

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: A**

D: not for serverless.

upvoted 2 times

## Question #305

## Topic 1

A developer uses AWS CloudFormation to deploy an Amazon API Gateway API and an AWS Step Functions state machine. The state machine must reference the API Gateway API after the CloudFormation template is deployed. The developer needs a solution that uses the state machine to reference the API Gateway endpoint.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the CloudFormation template to reference the API endpoint in the DefinitionSubstitutions property for the AWS::StepFunctions::StateMachine resource.
- B. Configure the CloudFormation template to store the API endpoint in an environment variable for the AWS::StepFunctions::StateMachine resource. Configure the state machine to reference the environment variable.
- C. Configure the CloudFormation template to store the API endpoint in a standard AWS::SecretsManager::Secret resource. Configure the state machine to reference the resource.
- D. Configure the CloudFormation template to store the API endpoint in a standard AWS::AppConfig::ConfigurationProfile resource. Configure the state machine to reference the resource.

**Correct Answer:** C

*Community vote distribution*

A (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: A**

The other options (B, C, and D) involve using additional resources or services that are not necessary for this requirement and would therefore be less cost-effective.

upvoted 2 times

## Question #306

## Topic 1

A developer is building an application on AWS. The application includes an AWS Lambda function that processes messages from an Amazon Simple Queue Service (Amazon SQS) queue.

The Lambda function sometimes fails or times out. The developer needs to figure out why the Lambda function fails to process some messages.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Increase the maximum timeout of the Lambda function to 15 minutes. Check the AWS CloudTrail event history for error details.
- B. Increase the visibility timeout of the SQS queue. Check logs in Amazon CloudWatch Logs for error details.
- C. Create a dead-letter queue. Configure the Lambda function to send the failed messages to the dead-letter queue.
- D. Create an Amazon DynamoDB table. Update the Lambda function to send the failed messages to the DynamoDB table.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **tgv** 1 week, 6 days ago

**Selected Answer: C**

Always DLQ for checking failed processed messaged in Lambda.

upvoted 4 times

## Question #307

## Topic 1

A developer needs to deploy an application in three AWS Regions by using AWS CloudFormation. Each Region will use an AWS Elastic Beanstalk environment with an Application Load Balancer (ALB). The developer wants to use AWS Certificate Manager (ACM) to deploy SSL certificates to each ALB.

Which solution will meet these requirements?

- A. Create a certificate in ACM in any one of the Regions. Import the certificate into the ALB that is in each Region.
- B. Create a global certificate in ACM. Update the CloudFormation template to deploy the global certificate to each ALB.
- C. Create a certificate in ACM in each Region. Import the certificate into the ALB for each Region.
- D. Create a certificate in ACM in the us-east-1 Region. Update the CloudFormation template to deploy the certificate to each ALB.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **nder** 2 days, 8 hours ago

**Selected Answer: C**

Certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region.

upvoted 1 times

 **tgv** 1 week, 6 days ago

**Selected Answer: C**

The correct solution is to create a certificate in each Region and to assign it to each ALB.

upvoted 4 times

## Question #308

## Topic 1

A company needs to deploy all its cloud resources by using AWS CloudFormation templates. A developer must create an Amazon Simple Notification Service (Amazon SNS) automatic notification to help enforce this rule. The developer creates an SNS topic and subscribes the email address of the company's security team to the SNS topic.

The security team must receive a notification immediately if an IAM role is created without the use of CloudFormation.

Which solution will meet this requirement?

- A. Create an AWS Lambda function to filter events from CloudTrail if a role was created without CloudFormation. Configure the Lambda function to publish to the SNS topic. Create an Amazon EventBridge schedule to invoke the Lambda function every 15 minutes.
- B. Create an AWS Fargate task in Amazon Elastic Container Service (Amazon ECS) to filter events from CloudTrail if a role was created without CloudFormation. Configure the Fargate task to publish to the SNS topic. Create an Amazon EventBridge schedule to run the Fargate task every 15 minutes.
- C. Launch an Amazon EC2 instance that includes a script to filter events from CloudTrail if a role was created without CloudFormation. Configure the script to publish to the SNS topic. Create a cron job to run the script on the EC2 instance every 15 minutes.
- D. Create an Amazon EventBridge rule to filter events from CloudTrail if a role was created without CloudFormation. Specify the SNS topic as the target of the EventBridge rule.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **ANDRES715** 2 days, 5 hours ago

**Selected Answer: D**

El desarrollador debe crear una regla de Amazon EventBridge para filtrar eventos de CloudTrail si se crea un rol sin el uso de CloudFormation. Luego, debe especificar el tema de SNS como destino de la regla de EventBridge. Esto permitirá que el equipo de seguridad reciba una notificación inmediata a través del tema de SNS cuando se cree una función de IAM sin el uso de CloudFormation.

upvoted 1 times

## Question #309

## Topic 1

A company is adopting serverless computing for some of its new services. A development team needs to create a serverless infrastructure by using AWS Serverless Application Model (AWS SAM). All infrastructure must be deployed by using AWS CloudFormation templates.

What should the development team do to meet these requirements?

- A. Add a Resources section to the CloudFormation templates that contains AWS::Lambda::Function resources.
- B. Add a Mappings section to the CloudFormation templates that contains AWS::Serverless::Function and AWS::Serverless::API.
- C. Add a Transform section to the CloudFormation templates. Use the AWS SAM syntax to define the resources.
- D. Add a Parameters section to the CloudFormation templates that specifies the relevant AWS SAM Globals section.

**Correct Answer:** D

*Community vote distribution*

C (100%)

 **monishvster** 3 days, 5 hours ago

**Selected Answer: C**

Should be C

upvoted 2 times

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: C**

Got this question in exam.

upvoted 2 times

 **tgv** 2 weeks, 1 day ago

the correct answer is C

upvoted 3 times

## Question #310

## Topic 1

A developer is building an application that invokes AWS Lambda functions asynchronously to process events. The developer notices that a Lambda function fails to process some events at random times. The developer needs to investigate the failed events and capture the events that the Lambda function fails to process.

Which solution will meet these requirements?

- A. Add an Amazon EventBridge rule for the Lambda function. Configure the EventBridge rule to react to failed events and to store the events in an Amazon DynamoDB table.
- B. Configure the Lambda function with a dead-letter queue based in Amazon Kinesis. Update the Lambda function's execution role with the required permissions.
- C. Configure the Lambda function with an Amazon Simple Queue Service (Amazon SQS) dead-letter queue. Update the Lambda function's execution role with the required permissions.
- D. Configure the Lambda function with an Amazon Simple Queue Service (Amazon SQS) FIFO dead-letter queue. Update the Lambda function's execution role with the required permissions.

**Correct Answer:** B

*Community vote distribution*

C (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: C**

Using an SQS queue for a DLQ is simpler than using Amazon Kinesis. Kinesis is a more complex service designed for real-time data streaming, which might be overkill for simply capturing failed Lambda events.

upvoted 2 times

 **tgv** 1 week, 6 days ago

The standard SQS dead-letter queue should capture the failed events and let the developer debug them, so C is the right solution.

B - There's no such thing as a DLQ in Kinesis.

D - SQS FIFO DLQ would be too much overkill for this task because you don't need ordering or deduplication.

A - This would involve additional costs and too much complexity to use a DynamoDB table for this.

upvoted 4 times

## Question #311

## Topic 1

A company has built a serverless application for its ecommerce website. The application includes a REST API in Amazon API Gateway that invokes an AWS Lambda function. The Lambda function processes data and stores the data in Amazon DynamoDB table. The Lambda function calls a third-party stock application API to process the order. After the order is processed, the Lambda function returns an HTTP 200 status code with no body to the client.

During peak usage when the API calls exceeds a certain threshold, the third-party stock application sometimes fails to process the data and responds with error messages. The company needs a solution that will not overwhelm the third-party stock application.

Which solution will meet these requirements?

- A. Configure the REST API in API Gateway to write the requests directly into DynamoDB. Configure a DynamoDB intrinsic function to perform the transformation. Set up a DynamoDB stream to call the third-party stock application API with each new row. Delete the Lambda function.
- B. Configure the REST API in API Gateway to write the requests directly into an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function with a reserved concurrency equal to the third-party stock application's threshold. Set Lambda function to process the messages from the SQS queue.
- C. Configure the REST API in API Gateway to write the requests directly into an Amazon Simple Notification Service (Amazon SNS) topic. Configure the Lambda function with a provisioned concurrency equal to the third-party stock application's threshold. Set the Lambda function to process the messages from the SNS topic.
- D. Configure the REST API in API Gateway to write the requests directly into Amazon Athena. Configure the transformation of the data by using SQL with multiple query result locations set up to point to the DynamoDB table and the third-party stock fulfilment application API. Delete the Lambda function.

**Correct Answer: B**

Community vote distribution

B (100%)

 **tgv** Highly Voted  1 week, 6 days ago

B should do it: API Gateway --> SQS <-- Lambda poll  
upvoted 5 times

 **CrescentShared** Most Recent  1 week, 2 days ago

Selected Answer: B  
no doubt.  
upvoted 2 times

## Question #312

## Topic 1

A company hosts its application on AWS. The application runs on an Amazon Elastic Container Service (Amazon ECS) cluster that uses AWS Fargate. The cluster runs behind an Application Load Balancer. The application stores data in an Amazon Aurora database. A developer encrypts and manages database credentials inside the application.

The company wants to use a more secure credential storage method and implement periodic credential rotation.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Migrate the secret credentials to Amazon RDS parameter groups. Encrypt the parameter by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant AWS KMS permissions to access Amazon RDS.
- B. Migrate the credentials to AWS Systems Manager Parameter Store. Encrypt the parameter by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager.
- C. Migrate the credentials to ECS Fargate environment variables. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager.
- D. Migrate the credentials to AWS Secrets Manager. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Turn on secret rotation. Use IAM policies and roles to grant Amazon ECS Fargate permissions to access to AWS Secrets Manager by using keys.

**Correct Answer:** C

*Community vote distribution*

D (100%)

 **nder** 2 days, 8 hours ago

**Selected Answer: D**

If it's secrets manager its for db  
upvoted 1 times

 **monishvster** 3 days, 5 hours ago

**Selected Answer: D**

Secrets Manager  
upvoted 2 times

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: D**

C is not correct.  
upvoted 2 times

 **tgv** 1 week, 6 days ago

the most secure + secrets rotation --> Secrets Manager  
upvoted 2 times

## Question #313

## Topic 1

A company has a mobile app. The app includes an Amazon API Gateway REST API that invokes AWS Lambda functions. The Lambda functions process data from the app.

The company needs to test updated Lambda functions that have new features. The company must conduct these tests with a subset of users before deployment. The tests must not affect other users of the app.

Which solution will meet these requirements with the LEAST amount of operational effort?

- A. Create a new version of each Lambda function with a weighted alias. Configure a weight value for each version of the Lambda function. Update the new weighted alias Amazon Resource Name (ARN) in the REST API.
- B. Create a new REST API in API Gateway. Set up a Lambda proxy integration to connect to multiple Lambda functions. Enable canary settings on the deployment stage. Specify a smaller percentage of API traffic to go to the new version of the Lambda function.
- C. Create a new version of each Lambda function. Integrate a predefined canary deployment in AWS CodeDeploy to slowly shift the traffic to the new versions automatically.
- D. Create a new REST API in API Gateway. Set up a Lambda non-proxy integration to connect to multiple Lambda functions. Specify the necessary parameters and properties in API Gateway. Enable canary settings on the deployment stage. Specify a smaller percentage of API traffic to go to the new version of the Lambda function.

**Correct Answer: C***Community vote distribution*

**ANDRES715** 2 days, 5 hours ago

**Selected Answer: D**

}

El desarrollador debe crear una nueva API REST en Amazon API Gateway y configurar una integración Lambda sin proxy para conectarse a múltiples funciones Lambda. Luego, debe especificar los parámetros y propiedades necesarios en API Gateway y habilitar la configuración canary en la etapa de implementación. Especifique un porcentaje menor de tráfico API para ir a la nueva versión de la función Lambda.

Al utilizar una nueva API REST en API Gateway con una configuración canary, el desarrollador puede probar las funciones Lambda actualizadas con nuevas características con un subconjunto de usuarios antes de la implementación completa. Esto permite realizar pruebas sin afectar a otros usuarios de la aplicación y con un menor esfuerzo operativo.

upvoted 1 times

**monishvster** 3 days, 5 hours ago

**Selected Answer: B**

Should be B

upvoted 1 times

**CrescentShared** 1 week, 2 days ago

**Selected Answer: B**

Option A involves using weighted aliases for Lambda functions, which is a valid approach but requires more effort to manage and update the aliases in the API Gateway configuration.

upvoted 1 times

**tgv** 1 week, 6 days ago

**Selected Answer: A**

Lambda with weighted alias with weight configured for each version of the function.

The canary situation is much suitable for deployments.

upvoted 2 times

**Americo32** 2 weeks, 5 days ago

Opção A

upvoted 2 times

## Question #314

## Topic 1

A developer works for a company that only has a single pre-production AWS account with an AWS CloudFormation AWS Serverless Application Model (AWS SAM) stack. The developer made changes to an existing AWS Lambda function specified in the AWS SAM template and additional Amazon Simple Notification service (Amazon SNS) topics.

The developer wants to do a one-time deploy of the changes to test if the changes are working. The developer does not want to impact the existing pre-production application that is currently being used by other team members as part of the release pipeline.

Which solution will meet these requirements?

- A. Use the AWS SAM CLI to package and deploy the SAM application to the pre-production AWS account. Specify the debug parameter.
- B. Use the AWS SAM CLI to package and create a change set against the pre-production AWS account. Execute the change set in a new AWS account designated for a development environment.
- C. Use the AWS SAM CLI to package and deploy the SAM application to a new AWS account designated for a development environment.
- D. Update the CloudFormation stack in the pre-production account. Add a separate stage that points to a new AWS account designated for a development environment.

**Correct Answer: C***Community vote distribution* C (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **tgv** 2 weeks, 1 day ago

best practice here is to sam pack and sam deploy to a new AWS account dedicated to development so in this case the developer wouldn't impact whatsoever the existing pre-prod application. option C

upvoted 2 times

## Question #315

## Topic 1

A company built an online event platform. For each event, the company organizes quizzes and generates leaderboards that are based on the quiz scores. The company stores the leaderboard data in Amazon DynamoDB and retains the data for 30 days after an event is complete. The company then uses a scheduled job to delete the old leaderboard data.

The DynamoDB table is configured with a fixed write capacity. During the months when many events occur, the DynamoDB write API requests are throttled when the scheduled delete job runs.

A developer must create a long-term solution that deletes the old leaderboard data and optimizes write throughput.

Which solution meets these requirements?

- A. Configure a TTL attribute for the leaderboard data.
- B. Use DynamoDB Streams to schedule and delete the leaderboard data.
- C. Use AWS Step Functions to schedule and delete the leaderboard data.
- D. Set a higher write capacity when the scheduled delete job runs.

**Correct Answer: D***Community vote distribution*A (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: A**

A is right

upvoted 2 times

 **tgv** 1 week, 6 days ago

**Selected Answer: A**

Always consider TTL when trying to ditch from DynamoDB.

upvoted 4 times

## Question #316

## Topic 1

A company uses an AWS Lambda function that reads messages from an Amazon Simple Queue Service (Amazon SQS) standard queue. The Lambda function makes an HTTP call to a third-party API for each message. The company wants to ensure that the Lambda function does not overwhelm the third-party API with more than two concurrent requests.

Which solution will meet these requirements?

- A. Configure a provisioned concurrency of two on the Lambda function.
- B. Configure a batch size of two on the Amazon SQS event source mapping for the Lambda function.
- C. Configure Lambda event filtering to process two messages from Amazon SQS at every invocations.
- D. Configure a maximum concurrency of two on the Amazon SQS event source mapping for the Lambda function.

**Correct Answer: B**

*Community vote distribution*



✉️ **monishvster** 3 days, 4 hours ago

**Selected Answer: D**

Should be D. Source: <https://aws.amazon.com/blogs/compute/introducing-maximum-concurrency-of-aws-lambda-functions-when-using-amazon-sqs-as-an-event-source/>  
upvoted 3 times

✉️ **CrescentShared** 1 week, 2 days ago

**Selected Answer: B**

configuring a maximum concurrency of two on the SQS event source mapping, is not a valid option. The concept of maximum concurrency is not directly applicable to SQS event source mappings. Concurrency in the context of Lambda functions and SQS is controlled by the batch size and the function's reserved concurrency settings.

upvoted 1 times

✉️ **tgv** 1 week, 6 days ago

**Selected Answer: D**

Correct answer is D. The maximum concurrency setting on the Amazon SQS event source mapping for the Lambda function controls how many messages are sent to the Lambda function concurrently. By setting it to two, you ensure that only two messages are processed concurrently, preventing the Lambda function from overwhelming the third-party API with more than two concurrent requests.

upvoted 3 times

## Question #317

## Topic 1

A company is using Amazon API Gateway to develop an API for its application on AWS. A developer needs to test and generate API responses. Other teams are required to test the API immediately.

What should the developer do to meet these requirements?

- A. Set up a mock integration request in API Gateway. Configure the method's integration request and integration response to associate a response with a given status code.
- B. Set up the request validators in the API's OpenAPI definition file. Import the OpenAPI definitions into API Gateway to test the API.
- C. Set up a gateway response for the API in API Gateway. Configure response headers with hardcoded HTTP status codes and responses.
- D. Set up a request parameter-based Lambda authorizer to control access to the API. Configure the Lambda function with the necessary mapping template.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **tgv** 1 week, 6 days ago

**Selected Answer: A**

The mock integration should do it here

upvoted 4 times

## Question #318

## Topic 1

A company is releasing a new feature. Users can request early access to the new feature by using an application form. The company expects a surge of requests when the application form becomes available. Each request will be stored as an item in an Amazon DynamoDB table.

Each item will contain the user's username, the submission date, and a validation status of UNVALIDATED, VALID, or NOT VALID. Each item also will contain the user's rating of the process on a scale of 1 to 5.

Each user can submit one request. For the DynamoDB table, the developer must choose a partition key that will give the workload well-distributed records across partitions.

Which DynamoDB attribute will meet these requirements?

- A. Username
- B. Submission date
- C. Validation status
- D. Rating of the process on a scale of 1 to 5

**Correct Answer: D***Community vote distribution*A (100%)

 **nder** 2 days, 8 hours ago

**Selected Answer: A**

Username avoids a hot partition key  
upvoted 1 times

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: A**

rest is not even distributed.  
upvoted 1 times

## Question #319

## Topic 1

A developer is creating a publicly accessible enterprise website consisting of only static assets. The developer is hosting the website in Amazon S3 and serving the website to users through an Amazon CloudFront distribution. The users of this application must not be able to access the application content directly from an S3 bucket. All content must be served through the Amazon CloudFront distribution.

Which solution will meet these requirements?

- A. Create a new origin access control (OAC) in CloudFront. Configure the CloudFront distribution's origin to use the new OAC. Update the S3 bucket policy to allow CloudFront OAC with read and write access to access Amazon S3 as the origin.
- B. Update the S3 bucket settings. Enable the block all public access setting in Amazon S3. Configure the CloudFront distribution's with Amazon S3 as the origin. Update the S3 bucket policy to allow CloudFront write access.
- C. Update the S3 bucket's static website settings. Enable static website hosting and specifying index and error documents. Update the CloudFront origin to use the S3 bucket's website endpoint.
- D. Update the CloudFront distribution's origin to send a custom header. Update the S3 bucket policy with a condition by using the aws:RequestTag/tag-key key. Configure the tag-key as the custom header name, and the value being matched is the header's value.

**Correct Answer: C**

*Community vote distribution*

A (67%)

C (33%)

 **nder** 2 days, 8 hours ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>  
upvoted 1 times

 **monishvster** 3 days, 4 hours ago

**Selected Answer: C**

We don't want to provide write access to CloudFront since it's a static website. S3 should suffice  
upvoted 1 times

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: A**

While enabling the block all public access setting in Amazon S3 is a good security practice and necessary for this scenario, simply allowing CloudFront "write access" is not relevant since the scenario involves serving static assets, not writing to the S3 bucket. This option also doesn't specify using an OAC or a similar method to ensure exclusive access through CloudFront.  
upvoted 1 times

## Question #320

## Topic 1

A developer built an application that calls an external API to obtain data, processes the data, and saves the result to Amazon S3. The developer built a container image with all of the necessary dependencies to run the application as a container.

The application runs locally and requires minimal CPU and RAM resources. The developer has created an Amazon ECS cluster. The developer needs to run the application hourly in Amazon Elastic Container Service (Amazon ECS).

Which solution will meet these requirements with the LEAST amount of infrastructure management overhead?

- A. Add a capacity provider to manage instances.
- B. Add an Amazon EC2 instance that runs the application.
- C. Define a task definition with an AWS Fargate launch type.
- D. Create an Amazon ECS cluster and add the managed node groups feature to run the application.

**Correct Answer:** D

*Community vote distribution*

C (100%)

✉️ ANDRES715 2 days, 4 hours ago

**Selected Answer: C**

El desarrollador debe definir una definición de tarea con un tipo de lanzamiento de AWS Fargate. Al utilizar AWS Fargate, el desarrollador puede ejecutar la aplicación en un clúster de Amazon ECS sin tener que administrar la infraestructura subyacente. Fargate se encarga de aprovisionar y escalar automáticamente los recursos necesarios para ejecutar la tarea de la aplicación, lo que reduce la carga operativa y los gastos generales de administración.

Al ejecutar la aplicación en AWS Fargate, el desarrollador puede aprovechar los recursos mínimos de CPU y RAM necesarios para la aplicación, lo que garantiza un uso eficiente de los recursos y minimiza los costos.

upvoted 1 times

✉️ tgv 1 week, 6 days ago

**Selected Answer: C**

Always ECS with Fargate for the least management.

upvoted 4 times

## Question #321

## Topic 1

A company runs its website on AWS. The company posts daily polls on its website and publishes the poll results next day. The website stores user responses in an Amazon DynamoDB table. After the poll results are published, the company does not need to keep the user responses.

A developer needs to implement a solution that will automatically remove old user responses from the DynamoDB table. The developer adds a new expiration\_date attribute to the DynamoDB table. The developer plans to use the expiration\_date attribute for the automation.

Which solution will meet these requirements with the LEAST development effort?

- A. Create an AWS Lambda function to delete old user responses based on the expiration\_date attribute. Create an Amazon EventBridge schedule to run the Lambda function daily.
- B. Create an AWS Fargate task in Amazon Elastic Container Service (Amazon ECS) to delete old user responses based on the expiration\_date attribute. Create an Amazon EventBridge schedule to run the Fargate task daily.
- C. Create an AWS Glue job to delete old user responses based on the expiration\_date attribute. Create an AWS Glue trigger schedule to run the job daily.
- D. Enable TTL on the DynamoDB table and specify the expiration\_date attribute. Expire old user responses by using DynamoDB TTL.

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **monishvster** 3 days, 4 hours ago

**Selected Answer: D**

Always TTL

upvoted 2 times

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: D**

It's D.

upvoted 2 times

 **Americo32** 2 weeks, 5 days ago

Opção A

upvoted 1 times

 **tgv** 2 weeks, 1 day ago

it says "the least development effort". in this case the TTL would be best practice

upvoted 4 times

## Question #322

## Topic 1

A developer is creating a simple proof-of-concept demo by using AWS CloudFormation and AWS Lambda functions. The demo will use a CloudFormation template to deploy an existing Lambda function. The Lambda function uses deployment packages and dependencies stored in Amazon S3. The developer defined an AWS::Lambda::Function resource in a CloudFormation template. The developer needs to add the S3 bucket to the CloudFormation template.

What should the developer do to meet these requirements with the LEAST development effort?

- A. Add the function code in the CloudFormation template inline as the code property.
- B. Add the function code in the CloudFormation template as the ZipFile property.
- C. Find the S3 key for the Lambda function. Add the S3 key as the ZipFile property in the CloudFormation template.
- D. Add the relevant key and bucket to the S3Bucket and S3Key properties in the CloudFormation template.

**Correct Answer: C**

*Community vote distribution*

 D (100%)

 **tgv** 1 week, 6 days ago

**Selected Answer: D**

The correct solution would be D, to add the S3Bucket and S3Key properties in the CloudFormation template.  
upvoted 4 times

## Question #323

## Topic 1

A developer is building a microservices-based application by using Python on AWS and several AWS services. The developer must use AWS X-Ray. The developer views the service map by using the console to view the service dependencies. During testing, the developer notices that some services are missing from the service map.

What can the developer do to ensure that all services appear in the X-Ray service map?

- A. Modify the X-Ray Python agent configuration in each service to increase the sampling rate.
- B. Instrument the application by using the X-Ray SDK for Python. Install the X-Ray SDK for all the services that the application uses.
- C. Enable X-Ray data aggregation in Amazon CloudWatch Logs for all the services that the application uses.
- D. Increase the X-Ray service map timeout value in the X-Ray console.

**Correct Answer: D**

*Community vote distribution*

 B (100%)

 **tgv**  1 week, 6 days ago

**Selected Answer: B**

Instrument the application by using the X-Ray SDK for Python  
upvoted 5 times

 **Americo32**  2 weeks, 5 days ago

Opção B  
upvoted 4 times

## Question #324

## Topic 1

A developer is building a containerized application on AWS. The application communicates with a third-party service by using API keys. The developer needs a secure way to store the API keys and pass the API keys to the containerized application.

Which solutions will meet these requirements? (Choose two.)

- A. Store the API keys as a SecureString parameter in AWS Systems Manager Parameter Store. Grant the application access to retrieve the value from Parameter Store.
- B. Store the API keys in AWS CloudFormation templates by using base64 encoding. Pass the API keys to the application through container definition environment variables.
- C. Add a new AWS CloudFormation parameter to the CloudFormation template. Pass the API keys to the application by using the container definition environment variables.
- D. Embed the API keys in the application. Build the container image on-premises. Upload the container image to Amazon Elastic Container Registry (Amazon ECR).
- E. Store the API keys as a SecretString parameter in AWS Secrets Manager. Grant the application access to retrieve the value from Secrets Manager.

**Correct Answer:** AC

*Community vote distribution*

AE (100%)

✉️  **monishvster** 3 days, 4 hours ago

**Selected Answer: AE**

I have used Secrets Manager to store API Key  
upvoted 2 times

✉️  **CrescentShared** 1 week, 2 days ago

**Selected Answer: AE**

C is not right.  
upvoted 2 times

✉️  **tgv** 2 weeks, 1 day ago

A and E would be correct in this case.  
upvoted 3 times

## Question #325

## Topic 1

A company runs an application on AWS. The application stores data in an Amazon DynamoDB table. Some queries are taking a long time to run. These slow queries involve an attribute that is not the table's partition key or sort key.

The amount of data that the application stores in the DynamoDB table is expected to increase significantly. A developer must increase the performance of the queries.

Which solution will meet these requirements?

- A. Increase the page size for each request by setting the Limit parameter to be higher than the default value. Configure the application to retry any request that exceeds the provisioned throughput.
- B. Create a global secondary index (GSI). Set query attribute to be the partition key of the index.
- C. Perform a parallel scan operation by issuing individual scan requests. In the parameters, specify the segment for the scan requests and the total number of segments for the parallel scan.
- D. Turn on read capacity auto scaling for the DynamoDB table. Increase the maximum read capacity units (RCUs).

**Correct Answer:** C

*Community vote distribution*

B (100%)

 tgv  1 week, 6 days ago

**Selected Answer: B**

Creating a GSI would be more cost efficient than increasing the RCU in this case.

upvoted 7 times

## Question #326

## Topic 1

A company runs a payment application on Amazon EC2 instances behind an Application Load Balance. The EC2 instances run in an Auto Scaling group across multiple Availability Zones. The application needs to retrieve application secrets during the application startup and export the secrets as environment variables. These secrets must be encrypted at rest and need to be rotated every month.

Which solution will meet these requirements with the LEAST development effort?

- A. Save the secrets in a text file and store the text file in Amazon S3. Provision a customer managed key. Use the key for secret encryption in Amazon S3. Read the contents of the text file and read the export as environment variables. Configure S3 Object Lambda to rotate the text file every month.
- B. Save the secrets as strings in AWS Systems Manager Parameter Store and use the default AWS Key Management Service (AWS KMS) key. Configure an Amazon EC2 user data script to retrieve the secrets during the startup and export as environment variables. Configure an AWS Lambda function to rotate the secrets in Parameter Store every month.
- C. Save the secrets as base64 encoded environment variables in the application properties. Retrieve the secrets during the application startup. Reference the secrets in the application code. Write a script to rotate the secrets saved as environment variables.
- D. Store the secrets in AWS Secrets Manager. Provision a new customer master key. Use the key to encrypt the secrets. Enable automatic rotation. Configure an Amazon EC2 user data script to programmatically retrieve the secrets during the startup and export as environment variables.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **CrescentShared** 1 week, 2 days ago

**Selected Answer: D**

D is right

upvoted 2 times

 **tgv** 2 weeks, 1 day ago

rotation --> AWS Secrets Manager

upvoted 2 times

## Question #327

## Topic 1

A company is using Amazon API Gateway to invoke a new AWS Lambda function. The company has Lambda function versions in its PROD and DEV environments. In each environment, there is a Lambda function alias pointing to the corresponding Lambda function version. API Gateway has one stage that is configured to point at the PROD alias.

The company wants to configure API Gateway to enable the PROD and DEV Lambda function versions to be simultaneously and distinctly available.

Which solution will meet these requirements?

- A. Enable a Lambda authorizer for the Lambda function alias in API Gateway. Republish PROD and create a new stage for DEV. Create API Gateway stage variables for the PROD and DEV stages. Point each stage variable to the PROD Lambda authorizer to the DEV Lambda authorizer.
- B. Set up a gateway response in API Gateway for the Lambda function alias. Republish PROD and create a new stage for DEV. Create gateway responses in API Gateway for PROD and DEV Lambda aliases.
- C. Use an environment variable for the Lambda function alias in API Gateway. Republish PROD and create a new stage for development. Create API gateway environment variables for PROD and DEV stages. Point each stage variable to the PROD Lambda function alias to the DEV Lambda function alias.
- D. Use an API Gateway stage variable to configure the Lambda function alias. Republish PROD and create a new stage for development. Create API Gateway stage variables for PROD and DEV stages. Point each stage variable to the PROD Lambda function alias and to the DEV Lambda function alias.

**Correct Answer: A***Community vote distribution* D (100%)  **tgv**  1 week, 6 days ago**Selected Answer: D**

Use an API Gateway stage variable to configure the Lambda function alias.  
upvoted 5 times

  **monishvster**  3 days, 4 hours ago**Selected Answer: D**

stage variable in API Gateway  
upvoted 1 times

## Question #328

## Topic 1

A developer is working on an ecommerce platform that communicates with several third-party payment processing APIs. The third-party payment services do not provide a test environment.

The developer needs to validate the ecommerce platform's integration with the third-party payment processing APIs. The developer must test the API integration code without invoking the third-party payment processing APIs.

Which solution will meet these requirements?

- A. Set up an Amazon API Gateway REST API with a gateway response configured for status code 200. Add response templates that contain sample responses captured from the real third-party API.
- B. Set up an AWS AppSync GraphQL API with a data source configured for each third-party API. Specify an integration type of Mock. Configure integration responses by using sample responses captured from the real third-party API.
- C. Create an AWS Lambda function for each third-party API. Embed responses captured from the real third-party API. Configure Amazon Route 53 Resolver with an inbound endpoint for each Lambda function's Amazon Resource Name (ARN).
- D. Set up an Amazon API Gateway REST API for each third-party API. Specify an integration request type of Mock. Configure integration responses by using sample responses captured from the real third-party API.

**Correct Answer:** C

*Community vote distribution*

D (67%)

A (33%)

 ANDRES715 2 days, 4 hours ago

**Selected Answer: A**

A. Configure una API REST de Amazon API Gateway con una respuesta de puerta de enlace configurada para el código de estado 200. Agregue plantillas de respuesta que contengan respuestas de muestra capturadas de la API real de terceros.

Al configurar una API REST de Amazon API Gateway con una respuesta de puerta de enlace configurada para el código de estado 200, el desarrollador puede simular las respuestas de las API de procesamiento de pagos de terceros sin invocar realmente las API reales. Al agregar plantillas de respuesta que contengan respuestas de muestra capturadas de la API real de terceros, el desarrollador puede validar la integración de la plataforma de comercio electrónico con las API de procesamiento de pagos de terceros sin tener que interactuar directamente con las API reales.  
upvoted 1 times

 CrescentShared 1 week, 2 days ago

**Selected Answer: D**

D is right

upvoted 2 times