API Gateway

Completed on 28-July-2021

Attempt
01

Marks Obtained
2 / 10

Your score
20%

Time Taken
00 H 09 M 14 S

Result
Failed

Domains wise Quiz Performance Report

No	1
Domain	Other
Total Question	9
Correct	2
Incorrect	7
Unattempted	0
Marked for review	0

No	2
Domain	Define Performant Architectures
Total Question	1
Correct	0
Incorrect	1
Unattempted	0
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	10
Correct	2
Incorrect	8
Unattempted	0
Marked for review	0

Review the Answers

Sorting by All

Question 1 Correct

Domain : Other

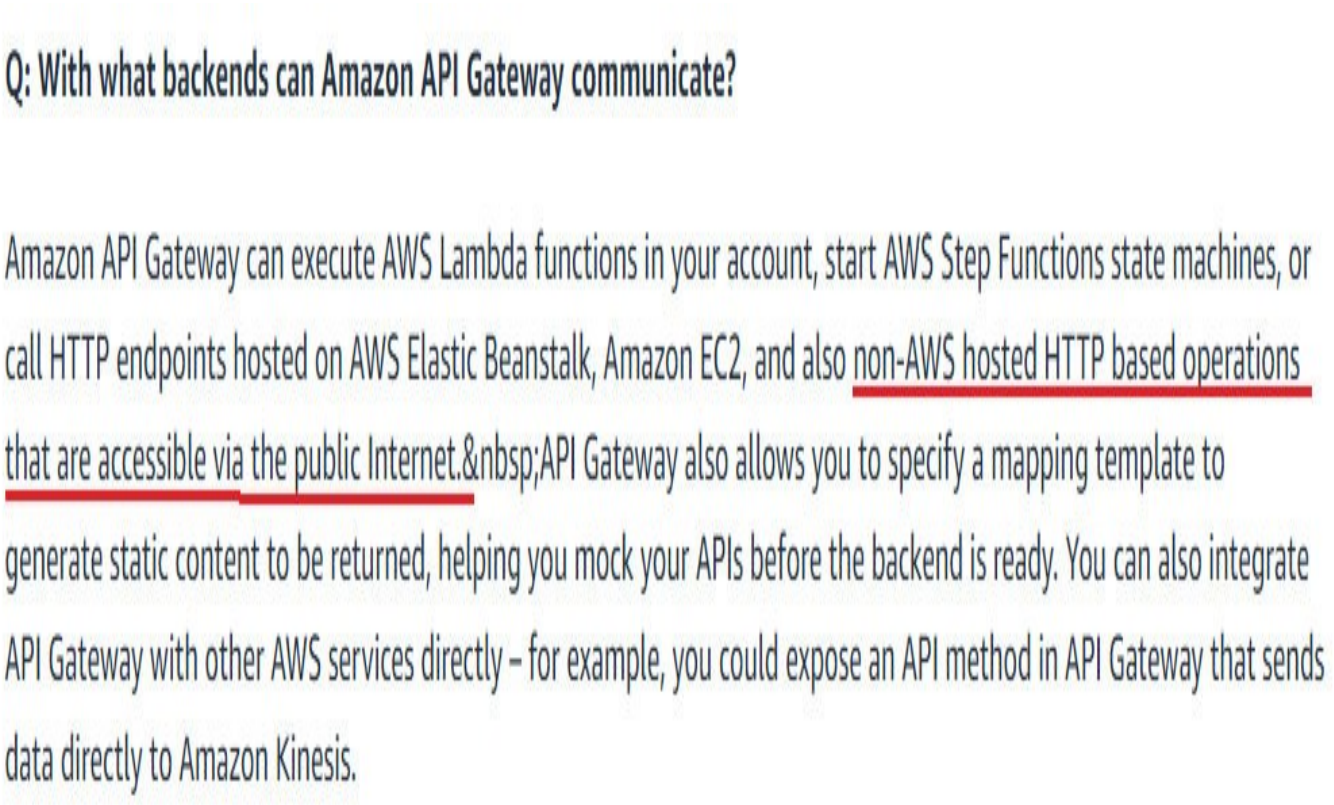
Which of the following are valid integration sources for API Gateway? (choose 3 options)

- ✓ A. Public facing HTTP-based endpoints outside AWS network.
- ✓ B. Lambda functions from another account.
- C. Database connections on internet outside AWS network.
- ✓ D. VPC Link
- E. SFTP connection

Explanation:

Answer: A, B, D

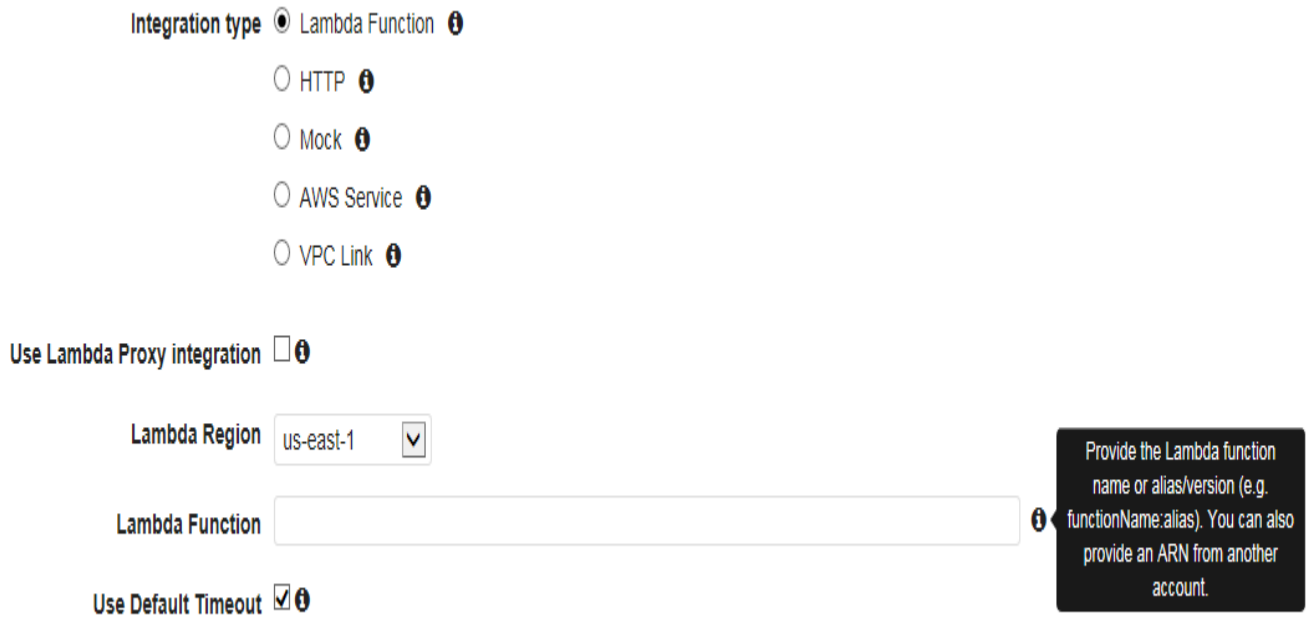
Option A is correct. AWS API Gateway can integrate with any HTTP-based endpoints available over the internet.



Q: With what backends can Amazon API Gateway communicate?

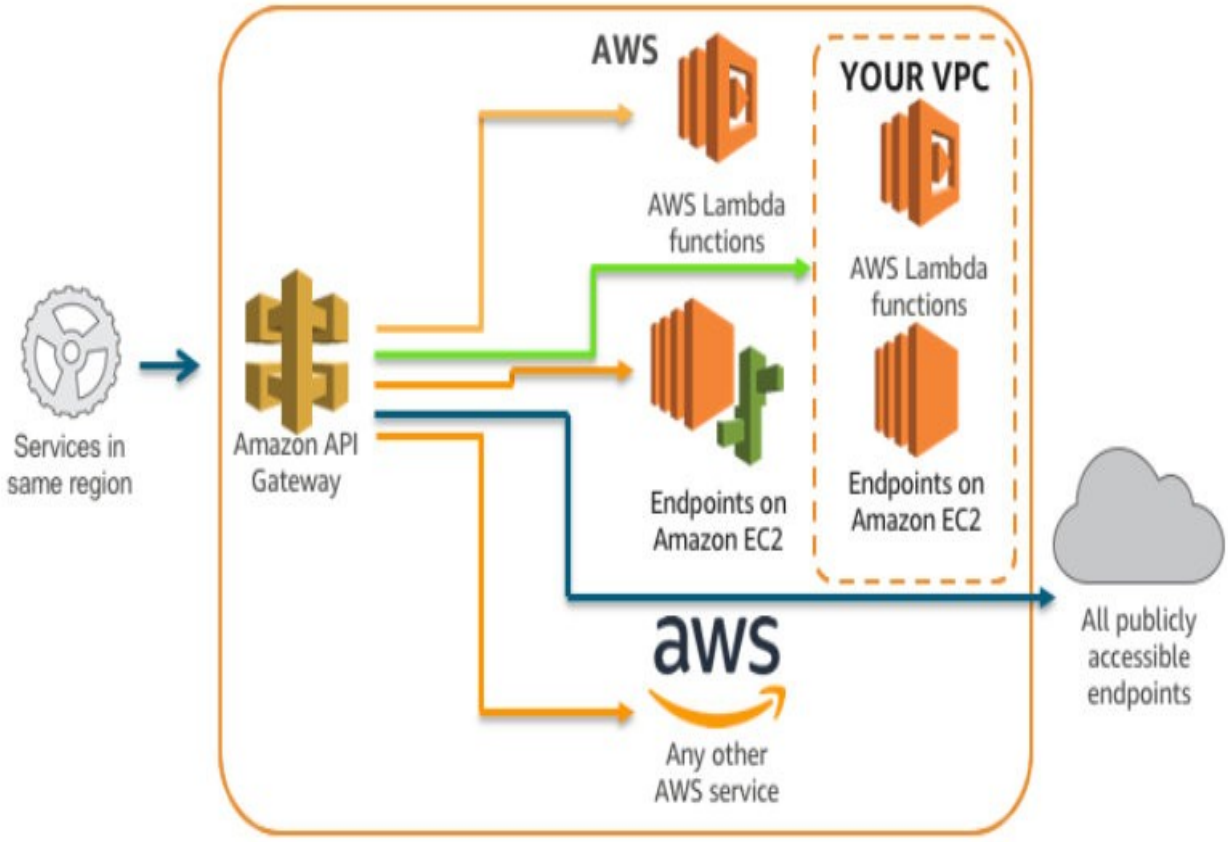
Amazon API Gateway can execute AWS Lambda functions in your account, start AWS Step Functions state machines, or call HTTP endpoints hosted on AWS Elastic Beanstalk, Amazon EC2, and also **non-AWS hosted HTTP based operations that are accessible via the public Internet.** API Gateway also allows you to specify a mapping template to generate static content to be returned, helping you mock your APIs before the backend is ready. You can also integrate API Gateway with other AWS services directly. For example, you could expose an API method in API Gateway that sends data directly to Amazon Kinesis.

Option B is correct. AWS can use Lambda function from another account as an integration type.



Option C is incorrect. AWS API gateway can connect to AWS services, making proxy calls only to their respective AWS APIs. There is no integration type for database connections directly from API Gateway. You can use the Lambda function to connect with the database and make Lambda as an integration type for API Gateway.

Option D is correct. AWS has introduced VPC Link, a way to connect to the resources within a private VPC.



Refer to the documentation here for more information on VPC Links.
https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/

Ask our Experts

Rate this Question?

View Queries open

Question 2 Incorrect

Domain : Other

A Company ABC has 100 REST APIs exposed to the Internet from their on-premise network. They have already integrated with AWS through DirectConnect. They have approached you asking for a cost-effective way of making these REST APIs available through AWS API Gateway because of the resiliency and cost reductions provided by it. What solution would you provide?

A. API Gateway cannot integrate with on-premises backend APIs which are not over the public internet. Rebuild all the backend APIs using Lambda and integrate it with API Gateway.

B. Use VPC Link to integrate on-premises backend solutions through DirectConnect and private VPC. ✓

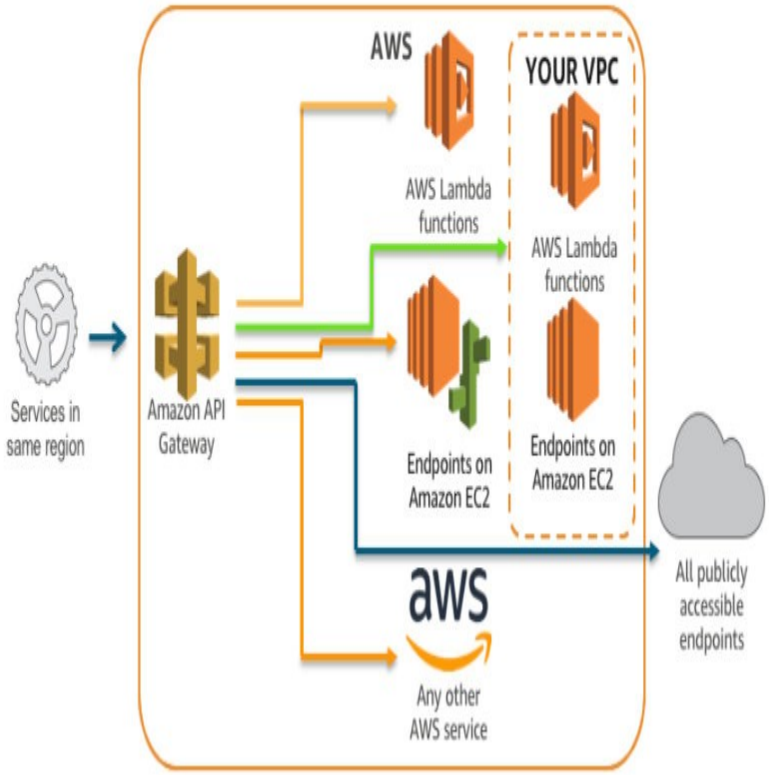
C. Build API Gateway using the existing on-premises public facing REST APIs as HTTPS endpoints integration type. ✗

D. Build API Gateway with integration type as AWS Service and select Direct Connect service.

Explanation:

Answer: B

At re:Invent 2017, we announced endpoint integrations inside a private VPC. With this capability, you can now have your backend running on EC2 be private inside your VPC without the need for a publicly accessible IP address or load balancer. Beyond that, you can also now use API Gateway to front APIs hosted by backends that exist privately in your own data centers, using AWS Direct Connect links to your VPC. Private integrations were made possible via VPC Link and Network Load Balancers, which support backends such as EC2 instances, Auto Scaling groups, and Amazon ECS using the Fargate launch type.



For more information on VPC Link, refer to the documentation here.

https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/

Option A is INCORRECT because you can use API Gateway to integrate with on-premises backend APIs. Therefore this option is invalid.

Option C is INCORRECT because you can choose the integration type as "HTTPS" if your API is integrated with an existing HTTPS endpoint. Since the question does not state any integration with any HTTPS endpoint, this option is invalid.

Option D is INCORRECT because you can choose the integration type as "AWS Service" only if your API will be integrated with an AWS service. Since the question does not state any integration with any AWS service, this option is invalid.

Please refer to page 605 on the below link:

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-dg.pdf

Ask our Experts

Rate this Question?

View Queries open

Question 3 Incorrect

Domain : Other

You have built a REST API using API gateway and distributed to your customers. However, your API is receiving large number of requests and overloading your backend system causing performance bottlenecks and eventually causing delays and failures in serving the requests for your important customers. How would you improve the API performance? (Choose 2 options)

A. Enable throttling and control the number of requests per second.

B. Create a resource policy to allow access for specific customers during specific time period.

C. Enable API caching to serve frequently requested data from API cache.

D. Enable load balancer on your backend systems.

Explanation:

Answer: A, C
Option A is correct. To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account.

For more information on throttling, refer documentation here.

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html

Option B is not correct. This is not a viable solution. Resource policies cannot have a time range based condition.

Following documentation shows the conditions supported for API Gateway resource policies.

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies-aws-condition-keys.html

Option C is correct. You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API. When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.

For details on enabling caching, refer documentation here.

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html#enable-api-gateway-caching

Option D is not correct. We can improve performance by increasing the capacity of backend systems if above settings does not help. Simply adding a load balancer does not improve any performance.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 4 Incorrect

Domain : Other

You have created a public-facing REST API using AWS API Gateway with a default throttle setting of 10000 requests per second and a burst of 5000 requests. You are getting 8000 requests in the first millisecond. Which of the following statements is true?

A. **All 8000 requests would succeed as the default throttle limit is 8000 per second.**

B. **All 8000 requests would fail as it is higher than the burst limit of 5000.**

C. **5000 requests would succeed and rest 3000 would fail.**

D. **5000 requests would succeed and throttles the rest of 3000 in the one-second period.**

Explanation:

Answer: D

To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token count for a request. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.

When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client. Upon catching such exceptions, the client can resubmit the failed requests in a rate-limiting fashion, while complying with the API Gateway throttling limits.

By default, API Gateway limits the steady-state request rate to 10,000 requests per second (rps). It limits the burst (that is, the maximum bucket size) to 5,000 requests across all APIs within an AWS account. In API Gateway, the burst limit corresponds to the maximum number of concurrent request submissions that API Gateway can fulfill at any moment without returning

429 Too Many Requests error responses.

- If the caller sends 10,000 requests in the first millisecond, API Gateway serves 5,000 of those requests and throttles the rest in the one-second period.

For more information on API Gateway throttling, refer to documentation here.

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-request-throttling-account-level-limits

NOTE:

The question says that "10000requests per **second** and burst of 5000 requests." However, "You are getting 8000 requests in one **millisecond**."

To help understand these throttling limits, here are a few examples, given the burst limit and the default account-level rate limit:

If a caller submits 10,000 requests in a one-second period evenly (for example, 10 requests every millisecond), API Gateway processes all requests without dropping any.

If the caller sends 10,000 requests in the first millisecond, API Gateway serves 5,000 of those requests and throttles the rest in the one-second period.

Please check the below link to know more about it.

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 5 Incorrect

Domain : Other

Your organization had created a REST API using AWS API Gateway and exposed it over the internet. They have noticed a consistently high number of requests per second on the GET **/users** method, approximately 9000 out of which 5000 requests are sent in 1st millisecond. This is putting more overload on backend systems. They have changed the stage's number of requests per second to 6000 and burst to 3000 requests. Now the total number of requests sent per second is reduced to 6000. However, 5000 requests being sent in 1st millisecond. What could be causing this behavior?

A. **Stage's GET /users method throttling settings might have overridden stage throttling settings with burst as 5000 requests.** ✓

B. **Account-level throttle settings are 10000 requests per second and burst 5000 requests. You cannot overwrite account-level settings.**

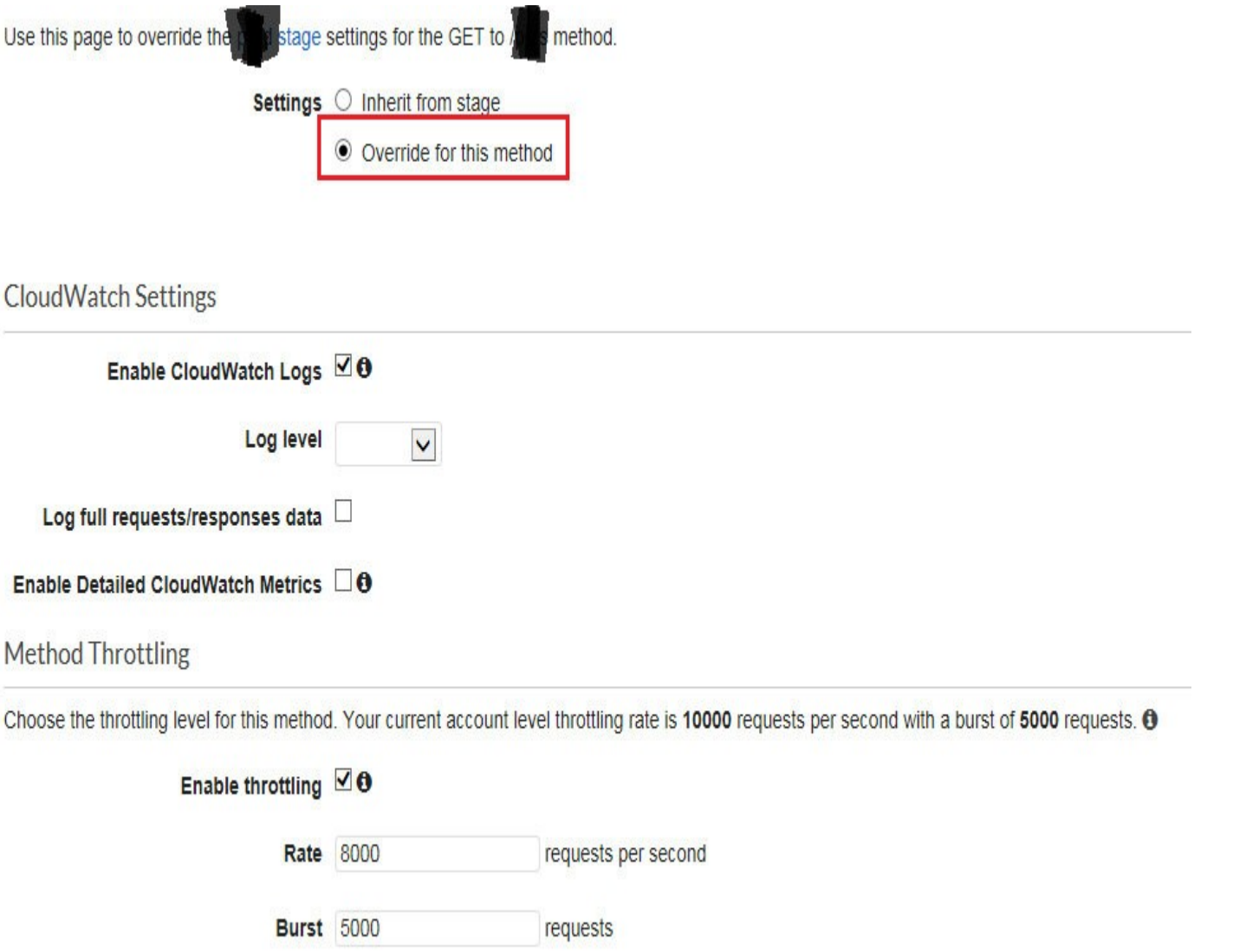
C. **Any changes made to Stage might take up to 2 hours to propagate.**

✓ D. **Requests per second are set to 6000. API can serve up to 6000 requests irrespective of how many requests sent in one millisecond.** ✗

Explanation:

Answer: A

You can override stage settings on an individual method within a stage.


Use this page to override the [redacted] stage settings for the GET to [redacted] method.
Settings
Inherit from stage
Override for this method
CloudWatch Settings
Enable CloudWatch Logs
Log level
Log full requests/responses data
Enable Detailed CloudWatch Metrics
Method Throttling
Choose the throttling level for this method. Your current account level throttling rate is 10000 requests per second with a burst of 5000 requests.
Enable throttling
Rate
8000
requests per second
Burst
5000
requests

Amazon API Gateway Usage Plans Now Support Method Level Throttling

Posted On: Jul 11, 2018

Amazon API Gateway usage plans now allow you to throttle requests for individual methods at different rates by configuring method level throttling.

Usage plans allow you to grant customers access to selected APIs at specific request rates and quotas. With method level throttling now included in usage plans, you can configure throttling (rate and burst limits) on individual client API keys for different API methods. This enables you to set more granular access controls to an API based on its use case.

You can configure method level throttling in an API's usage plan using the AWS Management Console, AWS CLI, or AWS SDKs. Visit our documentation to learn more about method level throttling in Amazon API Gateway.

Method level throttling for API Gateway is available in all regions where API Gateway is available. To see where API Gateway is available, review the AWS region table. For more information about API Gateway, visit our product page.

https://aws.amazon.com/about-aws/whats-new/2018/07/api-gateway-usage-plans-support-method-level-throttling/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 6 Incorrect

Domain : Other

Which of the following are not access control mechanisms for AWS API Gateway? (Choose 2 options)

A. Resource policies

B. Lambda authorizers

✓ C. Server-side certificates ✓

D. VPC RouteTables ✓

✓ E. Usage Plans ✗

Explanation:

Answer: C, D

Following are different ways of controlling access to your AWS API Gateway.

Controlling Access to an API in API Gateway

API Gateway supports multiple mechanisms for controlling access to your API:

- **Resource policies** let you create resource-based policies to allow or deny access to your APIs and methods from specified source IP addresses or VPC endpoints.
- **Standard AWS IAM roles and policies** offer flexible and robust access controls that can be applied to an entire API or individual methods.
- **Cross-origin resource sharing (CORS)** lets you control how your API responds to cross-domain resource requests.
- **Lambda authorizers** are Lambda functions that control access to your API methods using bearer token authentication as well as information described by headers, paths, query strings, stage variables, or context variables request parameters.
- **Amazon Cognito user pools** let you create customizable authentication and authorization solutions.
- **Client-side SSL certificates** can be used to verify that HTTP requests to your backend system are from API Gateway.
- **Usage plans** let you provide API keys to your customers — and then track and limit usage of your API stages and methods for each API key.

https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-controlling-access-to-apis.html

Option C is not an access control mechanism. API Gateway accepts the client-side certificates of your backend system.

https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html#configure-api

Option D is not an access control mechanism. RouteTables in VPCs are to control network traffic flow within a VPC.

For more information on VPC route tables, refer to documentation here:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

Ask our Experts

Rate this Question?

View Queries open

Question 7 Incorrect

Domain : Other

Your organization needs to expose certain services to your customers. You have created and deployed a REST API for your organization using AWS API Gateway over the public internet. Once deployed, you notice requests from hosts other than your customers. How would you control access in this scenario? (Choose 3 Options)

A. **Establish DirectConnect to each of your customer's networks and enable API Gateway's VPC Link through a private VPC.**

- ✓ B. Enable CORS and add required hostnames under Access-Control-Allow-Origin. ✓
- ✓ C. Configure your customer's IP address ranges in resource policy. ✓
- ✓ D. Create IAM users for your customers and enable user authentication. ✗
- E. Generate a Client Certificate to verify that HTTP requests to your backend system are from API Gateway. ✓

Explanation:

Correct Answers: B, C, and E.

Controlling Access to an API in API Gateway

API Gateway supports multiple mechanisms for controlling access to your API:

- **Resource policies** let you create resource-based policies to allow or deny access to your APIs and methods from specified source IP addresses or VPC endpoints.
- **Standard AWS IAM roles and policies** offer flexible and robust access controls that can be applied to an entire API or individual methods.
- **Cross-origin resource sharing (CORS)** lets you control how your API responds to cross-domain resource requests.
- **Lambda authorizers** are Lambda functions that control access to your API methods using bearer token authentication as well as information described by headers, paths, query strings, stage variables, or context variables request parameters.
- **Amazon Cognito user pools** let you create customizable authentication and authorization solutions.
- **Client-side SSL certificates** can be used to verify that HTTP requests to your backend system are from API Gateway.
- **Usage plans** let you provide API keys to your customers — and then track and limit usage of your API stages and methods for each API key.

Option A is not a feasible solution.

Option B is correct. You can allow a domain other than the API Gateway's domain name to access the APIs using Cross-Origin Resource Sharing.

For more information on CORS, refer documentation here:https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html

Option C is correct.

Control Access to an API with Amazon API Gateway Resource Policies

Amazon API Gateway *resource policies* are JSON policy documents that you attach to an API to control whether a specified principal (typically an IAM user or role) can invoke the API. You can use API Gateway resource policies to allow your API to be securely invoked by:

- users from a specified AWS account
- specified source IP address ranges or CIDR blocks
- specified virtual private clouds (VPCs) or VPC endpoints (in any account)

You can use resource policies for all API endpoint types in API Gateway: private, edge-optimized, and regional.

You can attach a resource policy to an API using the AWS console, AWS CLI, or AWS SDKs.

API Gateway resource policies are different from IAM policies. IAM policies are attached to IAM entities (users, groups, or roles) and define what actions those entities are capable of doing on which resources. API Gateway resource policies are attached to resources. For a more detailed discussion of the differences between identity-based (IAM) policies and resource policies, see Identity-Based Policies and Resource-Based Policies.

You can use API Gateway resource policies together with IAM policies.

Option D is incorrect. We can't exactly predict the number of users who would be using the API from the customer's side, which is why we have Option C as correct. Configuring the customer's IP range, and whoever wants to have access will be using the IP that's part of the configured range.

Option E is correct. We can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway.

NOTE: The client certificate is between API Gateway and the backend systems, not between API Gateway and the clients who make the requests.

For more information on client certificates for API gateway, refer to documentation here:

https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html

Ask our Experts

Rate this Question?

View Queries open

Question 8 Correct

Domain : Other

In AWS API Gateway, which of the following security measures is provided default by AWS to protect the backend systems?

A. **Default Cross-Origin Resource Sharing (CORS) configuration.**

B. **Default Resource Policy.**

✓ C. **Protection from distributed denial-of-service (DDoS) attacks.**

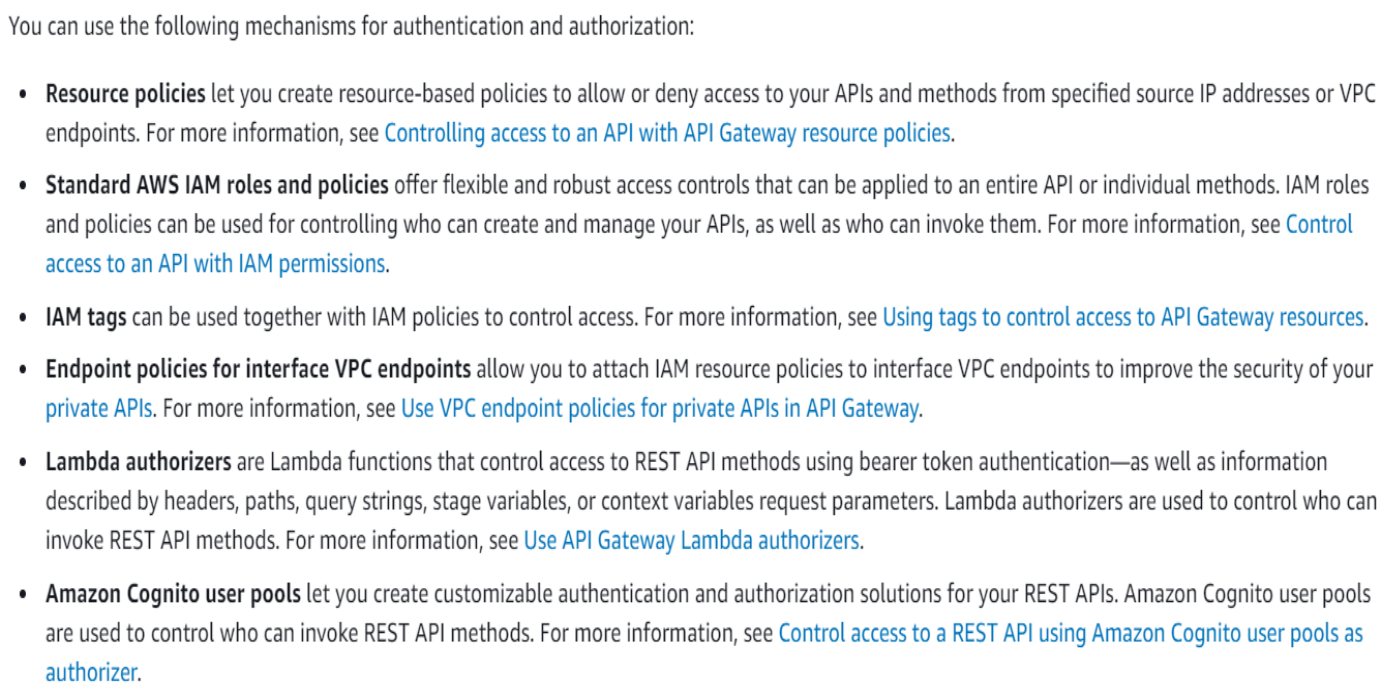
D. **Security of backend systems falls under customer responsibility. AWS provides different mechanisms to protect backend systems which are not configured by default.**

Explanation:

Answer: C

API Gateway supports throttling settings for each method or route in your APIs. You can set a standard rate limit and a burst rate limit per second for each method in your REST APIs and each route in WebSocket APIs. **Further, API Gateway automatically protects your backend systems from distributed denial-of-service (DDoS) attacks, whether attacked with counterfeit requests (Layer 7) or SYN floods (Layer 3).**

Options A and B are part of the above list and do not have any default configurations. Option C is correct.



You can use the following mechanisms for authentication and authorization:

- **Resource policies** let you create resource-based policies to allow or deny access to your APIs and methods from specified source IP addresses or VPC endpoints. For more information, see Controlling access to an API with API Gateway resource policies.
- **Standard AWS IAM roles and policies** offer flexible and robust access controls that can be applied to an entire API or individual methods. IAM roles and policies can be used for controlling who can create and manage your APIs, as well as who can invoke them. For more information, see Control access to an API with IAM permissions.
- **IAM tags** can be used together with IAM policies to control access. For more information, see Using tags to control access to API Gateway resources.
- **Endpoint policies for interface VPC endpoints** allow you to attach IAM resource policies to interface VPC endpoints to improve the security of your private APIs. For more information, see Use VPC endpoint policies for private APIs in API Gateway.
- **Lambda authorizers** are Lambda functions that control access to REST API methods using bearer token authentication—as well as information described by headers, paths, query strings, stage variables, or context variables request parameters. Lambda authorizers are used to control who can invoke REST API methods. For more information, see Use API Gateway Lambda authorizers.
- **Amazon Cognito user pools** let you create customizable authentication and authorization solutions for your REST APIs. Amazon Cognito user pools are used to control who can invoke REST API methods. For more information, see Control access to a REST API using Amazon Cognito user pools as authorizer.

Option D's statement is incorrect as it is a distractor. The above screenshot shows AWS automatically protects from DDoS attacks.

https://aws.amazon.com/api-gateway/faqs/

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 9 Incorrect

Domain :Define Performant Architectures

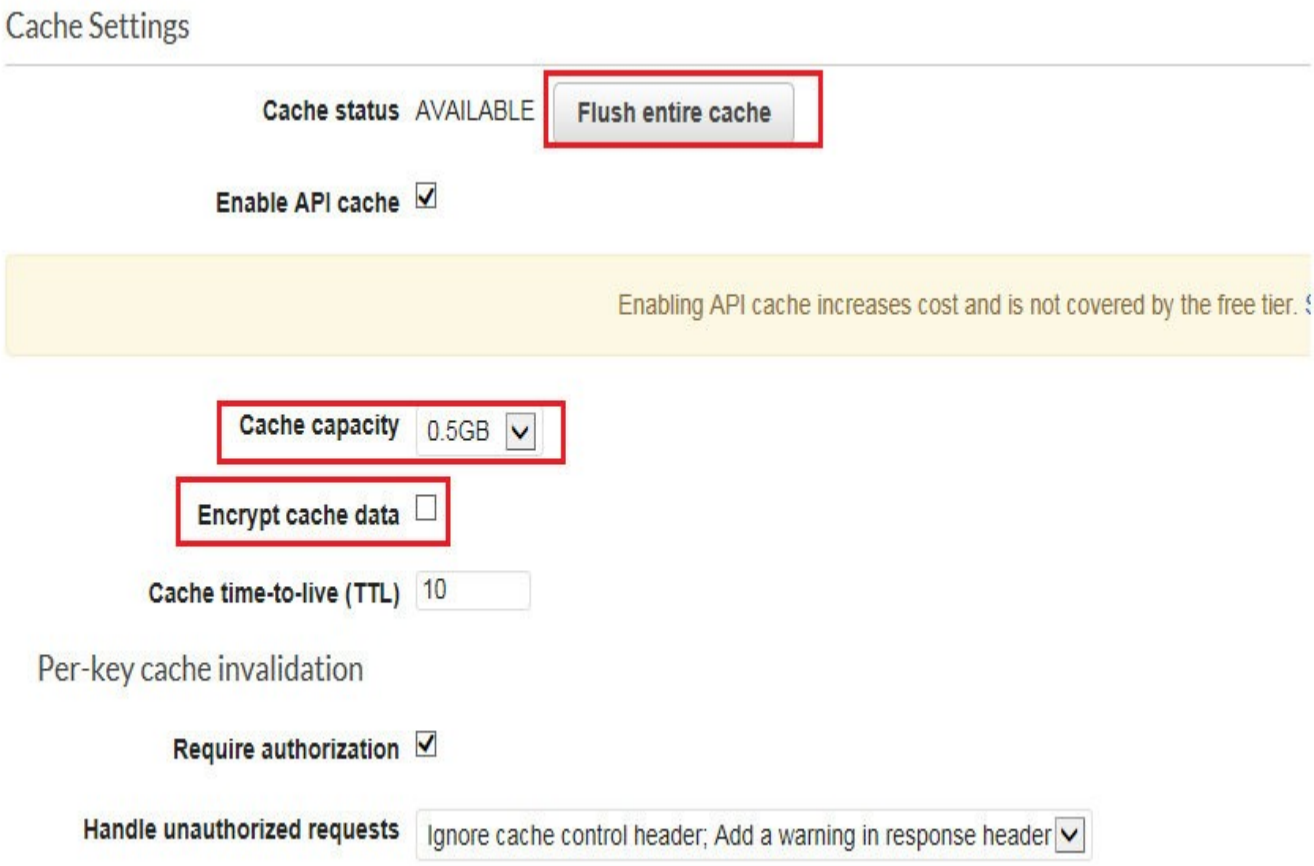
With respect to API caching for API Gateway through the console, which of the following is not a cache setting?

- A. Cache capacity ✗
- B. Encrypt cache data
- C. Refresh cache ✓
- D. Flush entire cache

Explanation:

Answer: C

Following are the settings when enabling/disabling API caching for API Gateway.



Options A, B, D are highlighted in the above screenshots. There is no action to refresh the cache on API Gateway.

For more information on API caching, refer to documentation here.

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html

Ask our Experts

Rate this Question?

View Queries open

Question 10 Incorrect

Domain : Other

You have created a REST API using AWS API Gateway and deployed it to production. Your organization requested the details regarding who is accessing the API deployed to production. How would you get the required information?

A. Enable Execution Logging in CloudWatch API logging.

B. Enable Access Logging in CloudWatch API logging.

C. CloudTrail contains the requester information for your API.

D. Enable logging in your backend system to log the requests.

Explanation:

Answer: B

Option A is incorrect because, in execution logging, API Gateway manages the CloudWatch Logs. The process includes creating log groups and log streams and reporting to the log streams any caller's requests and responses.

Option B is CORRECT because, in access logging, you, as an API developer, want to log who has accessed your API and how the caller accessed the API. You can create your own log group or choose an existing log group that could be managed by API Gateway.

https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-logging.html

Option C is incorrect. CloudTrail logs the request information on AWS API Gateway, not the APIs created through the API gateway.

https://docs.aws.amazon.com/apigateway/latest/developerguide/cloudtrail.html

Option D is incorrect. It is not effective in logging access logs as we have an option provided by AWS.

Ask our Experts

Rate this Question? 

View Queries open

Finish Review

ELB and Autoscaling

Completed on 26-July-2021

Attempt	Marks Obtained	Your score
01	0 / 10	0.0%

Time Taken	Result
00 H 04 M 34 S	Failed

Domains wise Quiz Performance Report

No	1
Domain	Other
Total Question	9
Correct	0
Incorrect	5
Unattempted	4
Marked for review	0

No	2
Domain	Design Resilient Architectures
Total Question	1
Correct	0
Incorrect	0
Unattempted	1
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	10
Correct	0
Incorrect	5
Unattempted	5
Marked for review	0

Review the Answers

Sorting by All

Question 1 Incorrect

Domain : Other

Which of the following components effectively facilitate a user to setup AutoScaling on EC2 instances for a web-based application? Choose 3 correct Options.

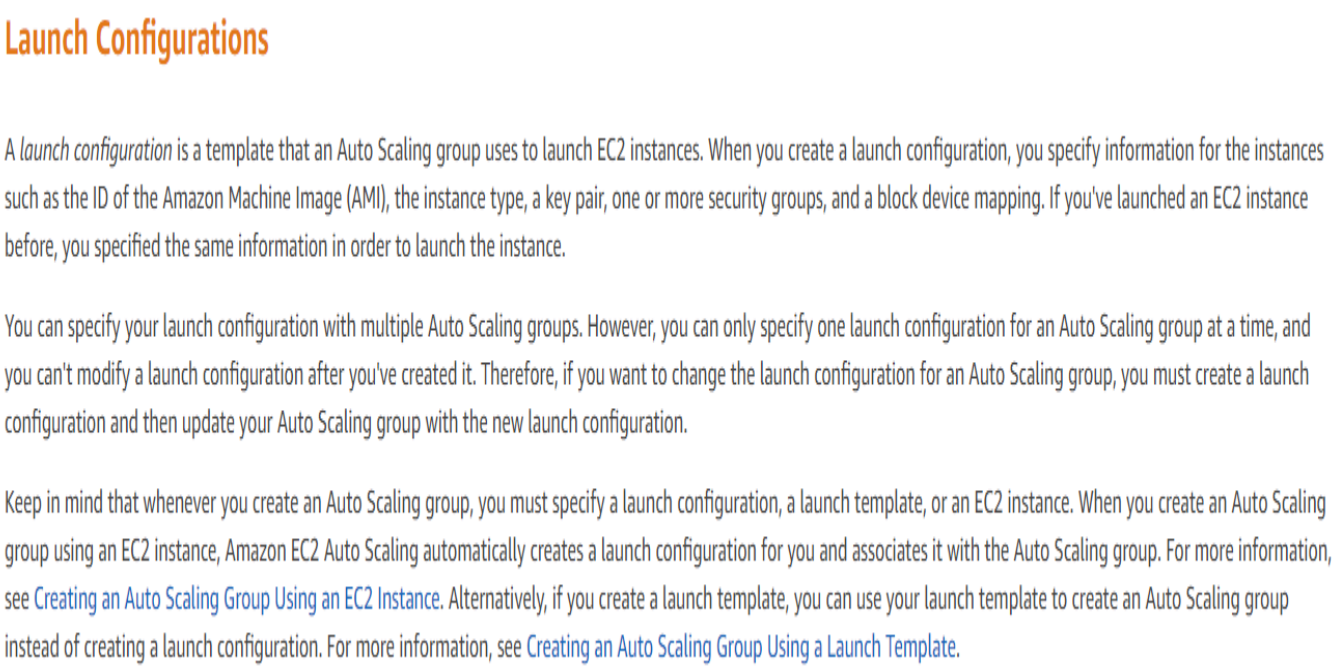
- ✓ A. Launch Configuration ✓
- B. Elastic Load Balancer ✓
- C. Lambda
- ✓ D. AutoScaling Group ✓
- ✓ E. Elastic IP ✗

Explanation:

Answer: A, B, D

Option A is correct.

A launch configuration specifies the type of EC2 instance that Amazon EC2 Auto Scaling creates for you. You create the launch configuration by including information such as the ID of the Amazon Machine Image (AMI) to use, the instance type, the key pair, security groups, and block device mapping.



Launch Configurations

A *launch configuration* is a template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance.

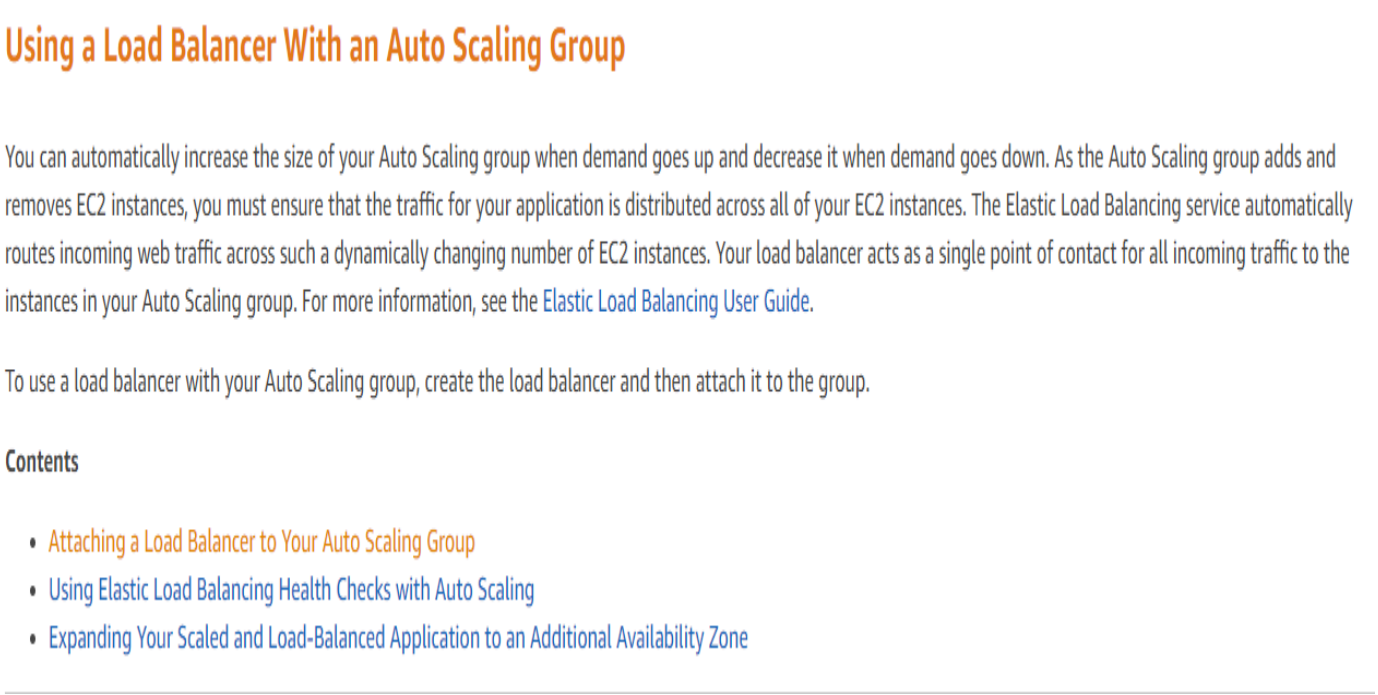
You can specify your launch configuration with multiple Auto Scaling groups. However, you can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for an Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration.

Keep in mind that whenever you create an Auto Scaling group, you must specify a launch configuration, a launch template, or an EC2 instance. When you create an Auto Scaling group using an EC2 instance, Amazon EC2 Auto Scaling automatically creates a launch configuration for you and associates it with the Auto Scaling group. For more information, see Creating an Auto Scaling Group Using an EC2 Instance. Alternatively, if you create a launch template, you can use your launch template to create an Auto Scaling group instead of creating a launch configuration. For more information, see Creating an Auto Scaling Group Using a Launch Template.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html

Option B is correct.

You can attach a load balancer to your Auto Scaling group. The load balancer automatically distributes incoming traffic across the instances in the group.



Using a Load Balancer With an Auto Scaling Group

You can automatically increase the size of your Auto Scaling group when demand goes up and decrease it when demand goes down. As the Auto Scaling group adds and removes EC2 instances, you must ensure that the traffic for your application is distributed across all of your EC2 instances. The Elastic Load Balancing service automatically routes incoming web traffic across such a dynamically changing number of EC2 instances. Your load balancer acts as a single point of contact for all incoming traffic to the instances in your Auto Scaling group. For more information, see the Elastic Load Balancing User Guide.

To use a load balancer with your Auto Scaling group, create the load balancer and then attach it to the group.

Contents

- Attaching a Load Balancer to Your Auto Scaling Group
- Using Elastic Load Balancing Health Checks with Auto Scaling
- Expanding Your Scaled and Load-Balanced Application to an Additional Availability Zone

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

Option C is not correct.

Lambda functions are not required to set up auto scaling for EC2 instances.

Option D is correct.

An Auto Scaling group is a collection of EC2 instances and the core of Amazon EC2 Auto Scaling. When you create an Auto Scaling group, you include information such as the subnets for the instances and the number of instances the group must maintain at all times.

Auto Scaling Groups

An *Auto Scaling group* contains a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management. For example, if a single application operates across multiple instances, you might want to increase the number of instances in that group to improve the performance of the application, or decrease the number of instances to reduce costs when demand is low. You can use the Auto Scaling group to scale the number of instances automatically based on criteria that you specify, or maintain a fixed number of instances even if an instance becomes unhealthy. This automatic scaling and maintaining the number of instances in an Auto Scaling group is the core functionality of the Amazon EC2 Auto Scaling service.

An Auto Scaling group starts by launching enough EC2 instances to meet its desired capacity. The Auto Scaling group maintains this number of instances by performing periodic health checks on the instances in the group. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it. For more information about health check replacements, see Maintaining the Number of Instances in Your Auto Scaling Group.

You can use scaling policies to increase or decrease the number of running EC2 instances in your group dynamically to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group and launches or terminates the instances as needed. If you manually scale or scale on a schedule, you must adjust the desired capacity of the group in order for the changes to take effect. For more information, see Scaling the Size of Your Auto Scaling Group.

Before you get started, take the time to review your application thoroughly as it runs in the AWS Cloud. Take note of the following:

- How long it takes to launch and configure a server.
- What metrics have the most relevance to your application's performance.
- How many Availability Zones you want the Auto Scaling group to span.
- Do you want to scale to increase or decrease capacity? Do you just want to ensure that a specific number of servers are always running? (Keep in mind that Amazon EC2 Auto Scaling can do both simultaneously.)
- What existing resources (such as EC2 instances or AMIs) you can use.

The better you understand your application, the more effective you can make your Auto Scaling architecture.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html

Option E is not correct.

Elastic IP is not required to set up auto scaling for EC2 instances.

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 2 Incorrect

Domain : Other

Your organization had set up Auto Scaling for an EC2 instance. They intend to launch one additional new instance with same configuration automatically when the workload increases and shut it down automatically when the workload is back to normal. However, they have applied operating system patches to the main instance for security reasons and would like this to be reflected when the Auto Scaling group launches a new EC2 instance. What actions would you take in this scenario?

A. **Auto Scaling group will launch new EC2 instance from the main instance latest snapshot. New instance will have updated patches.**

B. **Create an image out of main EC2 instance and update Auto Scaling group configuration with new image AMI ID.**

C. **Create an image out of main EC2 instance and update Launch Configuration with new image AMI ID.**

D. **Create an image out of main EC2 instance, create a new Launch Configuration with new image AMI ID, update Auto Scaling group with new Launch Configuration ID**

Explanation:

Answer: D

Option A is not correct.

Auto Scaling group launches new instances based on the configuration defined in Launch Configuration. AMI ID is one of the configuration parameter which defines the type of instance to be launched when auto-scaling logic is executed.

AMI ID is set during the creation of the launch configuration and cannot be modified.

So, the auto-scaling group will not launch a new instance based on the latest image of the main instance.

Option B is not correct.

AMI ID is a configuration on Launch Configuration, not Auto Scaling Group.

Launch Configuration:

Details

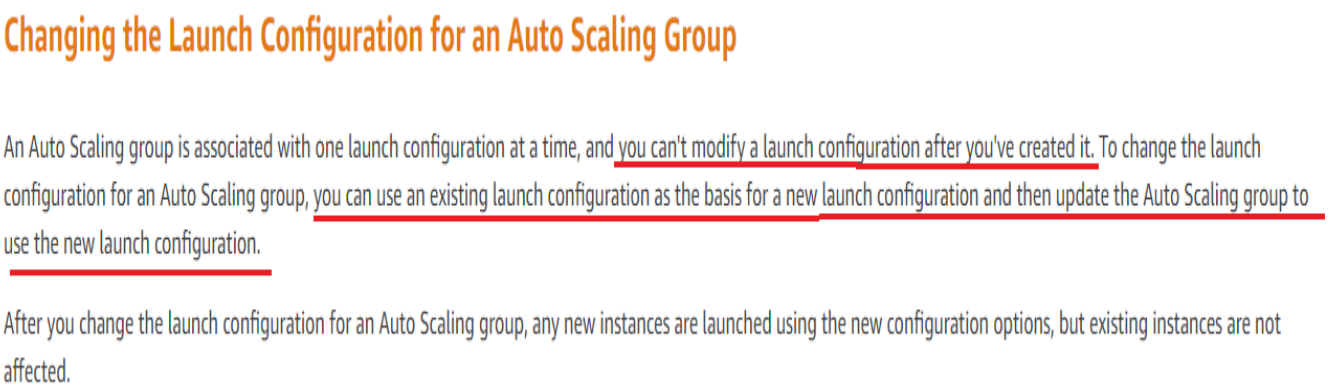
AMI ID	ami-8b2407f1	Instance Type	t2.micro
IAM Instance Profile		Kernel ID	
Key Name		Monitoring	false
EBS Optimized		Security Groups	
Spot Price		Creation Time	
RAM Disk ID		Block Devices	
User data	-	IP Address Type	Do not assign a public IP address to any instances.

Auto Scaling Group:

Details | Activity History | Scaling Policies | Instances | Monitoring | Notifications | Tags | Scheduled Actions | Lifecycle Hooks

Launch Template	-	Termination Policies	Default
Launch Template Version	-	Creation Time	
Launch Configuration		Availability Zone(s)	us-east-1a
Service-Linked Role		Subnet(s)	
		Default Cooldown	300
Classic Load Balancers		Placement Groups	
Target Groups		Suspended Processes	
Desired Capacity	0	Enabled Metrics	
Min	0	Instance Protection	
Max	1		
Health Check Type	EC2		
Health Check Grace Period	300		

Option C is not correct and Option D is correct.



Changing the Launch Configuration for an Auto Scaling Group

An Auto Scaling group is associated with one launch configuration at a time, and you can't modify a launch configuration after you've created it. To change the launch configuration for an Auto Scaling group, you can use an existing launch configuration as the basis for a new launch configuration and then update the Auto Scaling group to use the new launch configuration.

After you change the launch configuration for an Auto Scaling group, any new instances are launched using the new configuration options, but existing instances are not affected.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/change-launch-config.html

Ask our Experts

Rate this Question?

View Queries open

Question 3 Incorrect

Domain : Other

Which of the following is not a default metric type for Auto Scaling Group policy?

A. Average CPU Utilization

B. Memory Utilization

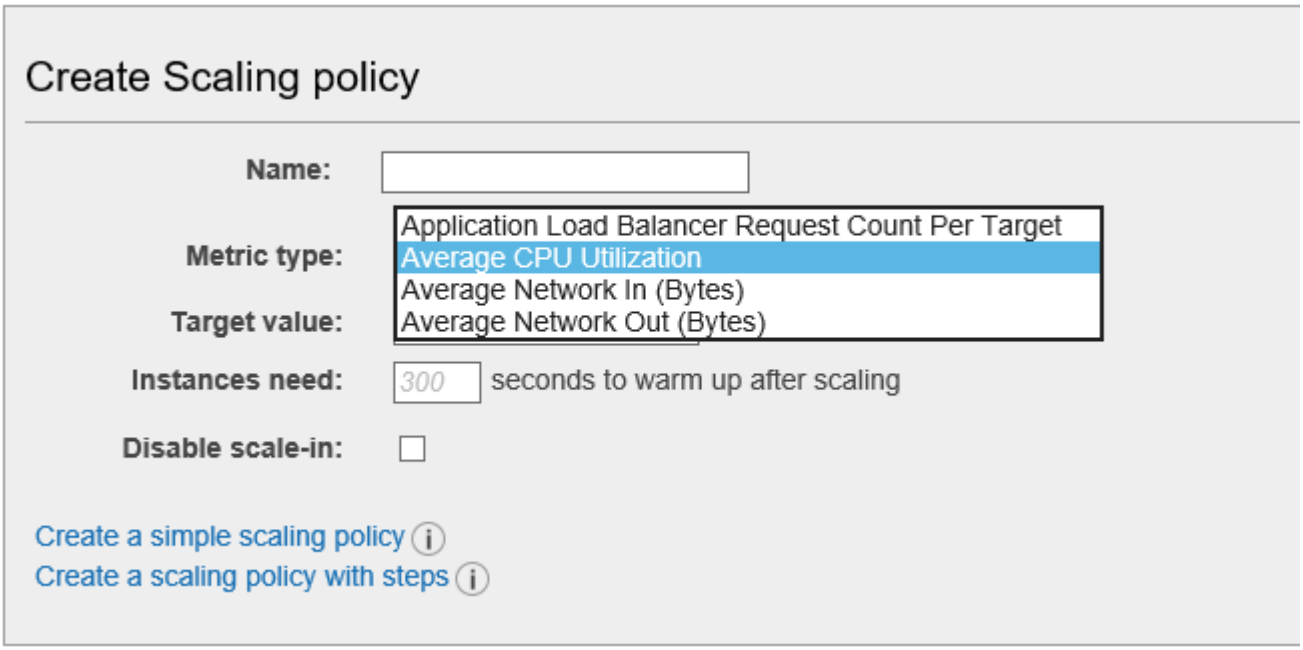
C. Network In

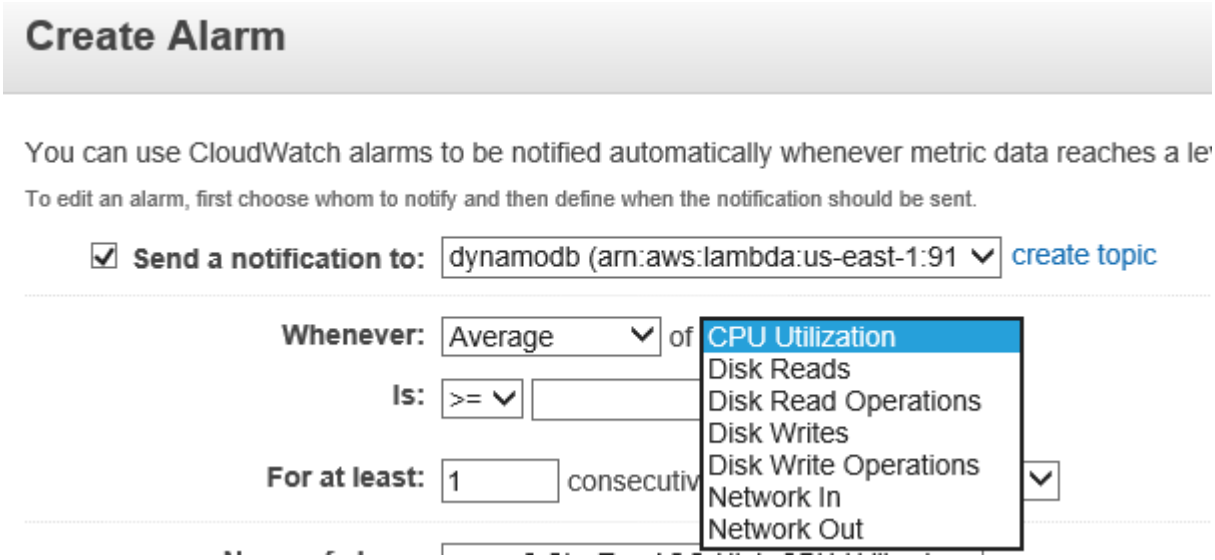
D. Network Out

Explanation:

Answer: B

Following are the default metric types available for Simple Policy and Step Policy





https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html

Ask our Experts

Rate this Question?

View Queries open

Question 4 Incorrect

Domain : Other

In your organization, an application team sets up an autoscaling group configuration (with a simple scaling policy) to launch a new instance when CPU utilization reaches 85%. However, at times, when the EC2 instance comes into in-service, it reports Unhealthy status immediately. As the replacement of the unhealthy instance by another instance (launched by the Autoscaling group) takes more than 15 minutes, the unhealthy instance has to be removed manually. What do you think is the reason behind this?

A. Auto scaling policy alarm incorrectly configured.

B. Health Check Grace Period set to 20 minutes.

C. Termination policy set to Do Not Terminate instances.

D. Launch Configuration is not configured to report Unhealthy status

Explanation:

Answer: B

Option A is incorrect because the Instance health status is not determined by the CloudWatch alarms.

Instance Health Status

Amazon EC2 Auto Scaling determines the health status of an instance using one or more of the following:

- Status checks provided by Amazon EC2 (systems status checks and instance status checks. For more information, see Status Checks for Your Instances in the *Amazon EC2 User Guide for Linux Instances*.
- Health checks provided by Elastic Load Balancing. For more information, see Health Checks for Your Target Groups in the *User Guide for Application Load Balancers* or Configure Health Checks for Your Classic Load Balancer in the *User Guide for Classic Load Balancers*.
- Custom health checks.

By default, Amazon EC2 Auto Scaling health checks use the results of the EC2 status checks to determine the health status of an instance. Amazon EC2 Auto Scaling marks an instance as unhealthy if its instance fails one or more of the status checks.

Option B is correct.

Health Check Grace Period

Frequently, an Auto Scaling instance that has just come into service needs to warm up before it can pass the health check. Amazon EC2 Auto Scaling waits until the health check grace period ends before checking the health status of the instance. While the EC2 status checks and ELB health checks can complete before the health check grace period expires, Amazon EC2 Auto Scaling does not act on them until the health check grace period expires. To provide ample warm-up time for your instances, ensure that the health check grace period covers the expected startup time for your application. Note that if you add a lifecycle hook to perform actions as your instances launch, the health check grace period does not start until the lifecycle hook is completed and the instance enters the `InService` state.

Option C is incorrect because the termination policy does not have a "Do Not Terminate" option.

Amazon EC2 Auto Scaling supports the following custom termination policies:

- `OldestInstance`. Terminate the oldest instance in the group. This option is useful when you're upgrading the instances in the Auto Scaling group to a new EC2 instance type. You can gradually replace instances of the old type with instances of the new type.
- `NewestInstance`. Terminate the newest instance in the group. This policy is useful when you're testing a new launch configuration but don't want to keep it in production.
- `OldestLaunchConfiguration`. Terminate instances that have the oldest launch configuration. This policy is useful when you're updating a group and phasing out the instances from a previous configuration.
- `ClosestToNextInstanceHour`. Terminate instances that are closest to the next billing hour. This policy helps you maximize the use of your instances and manage your Amazon EC2 usage costs.
- `Default`. Terminate instances according to the default termination policy. This policy is useful when you have more than one scaling policy for the group.

Option D is not a correct statement.

Ask our Experts

Rate this Question?

View Queries open

Question 5 Incorrect

Domain : Other

In an auto-scaling group setup, with a default termination policy for scale in, which statement is not correct?

A. Select the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, select the Availability Zone with the instances that use the oldest launch configuration.

B. Determine which unprotected instances in the selected Availability Zone use the newest launch configuration. If there is one such instance, terminate it.

C. If multiple instances use the oldest launch configuration, determine which unprotected instances are closest to the next billing hour and terminate it.

✓ D. If there is more than one unprotected instance closest to the next billing hour, select one of these instances randomly.

Explanation:

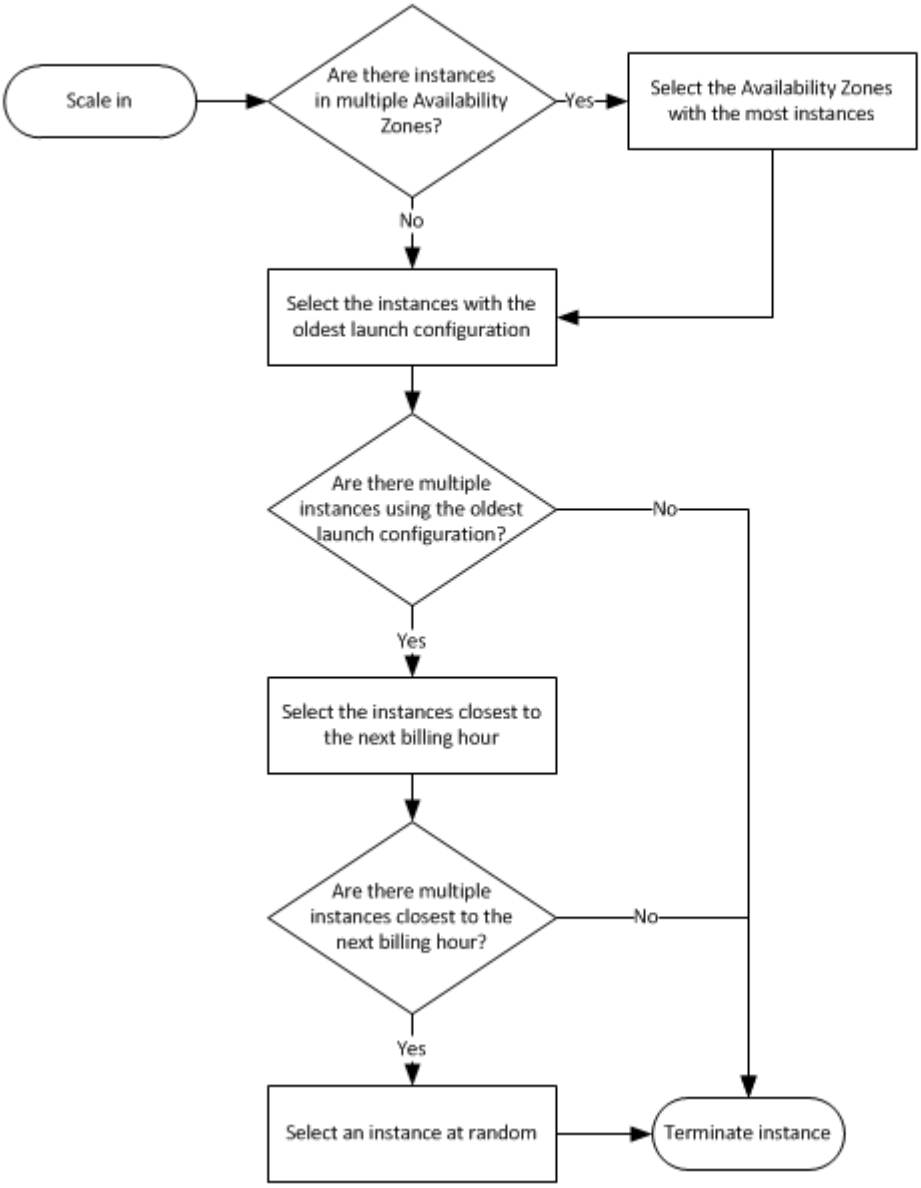
Answer: B

Default Termination Policy

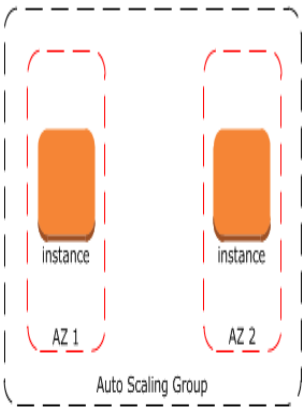
The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly. With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, select the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, select the Availability Zone with the instances that use the oldest launch configuration.
2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.
3. If there are multiple instances that use the oldest launch configuration, determine which unprotected instances are closest to the next billing hour. (This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.
4. If there is more than one unprotected instance closest to the next billing hour, select one of these instances at random.

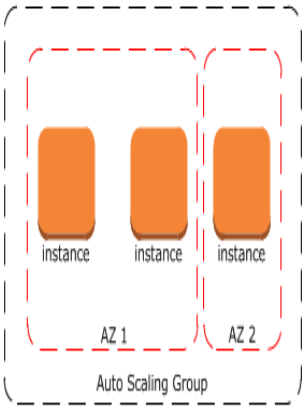
The following flow diagram illustrates how the default termination policy works.



Consider an Auto Scaling group that has two Availability Zones, a desired capacity of two instances, and scaling policies that increase and decrease the number of instances by 1 when certain thresholds are met. The two instances in this group are distributed as follows.



When the threshold for the scale-out policy is met, the policy takes effect and the Auto Scaling group launches a new instance. The Auto Scaling group now has three instances, distributed as follows.



When the threshold for the scale-in policy is met, the policy takes effect and the Auto Scaling group terminates one of the instances. If you did not assign a specific termination policy to the group, it uses the default termination policy. It selects the Availability Zone with two instances, and terminates the instance launched from the oldest launch configuration. If the instances were launched from the same launch configuration, then the Auto Scaling group selects the instance that is closest to the next billing hour and terminates it.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

Ask our Experts

Rate this Question?

View Queries open

Question 6 Unattempted

Domain :Design Resilient Architectures

You had set up an internal HTTP(S) Elastic Load Balancer to route requests to two EC2 instances inside a private VPC. However, one of the target EC2 instance is showing Unhealthy status. Which of the following options is NOT a possible reason for showing an unhealthy status?

A. Port 80/443 is not allowed on EC2 instance's Security Group from load balancer.

B. EC2 instance is in different availability zones than load balancer.

C. The ping path does not exist on the EC2 instance.

D. The target did not return a successful response code.

Explanation:

Answer: B
If a target is taking longer than expected to enter the InService state, it might be failing health checks. Your target is not in service until it passes one health check.

Target Health Status

Before the load balancer sends a health check request to a target, you must register it with a target group, specify its target group in a listener rule, and ensure that the Availability Zone of the target is enabled for the load balancer. Before a target can receive requests from the load balancer, it must pass the initial health checks. After a target passes the initial health checks, its status is `Healthy`.

The following table describes the possible values for the health status of a registered target.

Value	Description
`initial`	The load balancer is in the process of registering the target or performing the initial health checks on the target.
`healthy`	The target is healthy.
`unhealthy`	The target did not respond to a health check or failed the health check.
`unused`	The target is not registered with a target group, the target group is not used in a listener rule for the load balancer, or the target is in an Availability Zone that is not enabled for the load balancer.
`draining`	The target is deregistering and connection draining is in process.

A security group does not allow traffic

The security group associated with an instance must allow traffic from the load balancer using the health check port and health check protocol. You can add a rule to the instance security group to allow all traffic from the load balancer security group. Also, the security group for your load balancer must allow traffic to the instances.

A network access control list (ACL) does not allow traffic

The network ACL associated with the subnets for your instances must allow inbound traffic on the health check port and outbound traffic on the ephemeral ports (1024-65535). The network ACL associated with the subnets for your load balancer nodes must allow inbound traffic on the ephemeral ports and outbound traffic on the health check and ephemeral ports.

The ping path does not exist

Create a target page for the health check and specify its path as the ping path.

The connection times out

First, verify that you can connect to the target directly from within the network using the private IP address of the target and the health check protocol. If you can't connect, check whether the instance is over-utilized, and add more targets to your target group if it is too busy to respond. If you can connect, it is possible that the target page is not responding before the health check timeout period. Choose a simpler target page for the health check or adjust the health check settings.

The target did not return a successful response code

By default, the success code is 200, but you can optionally specify additional success codes when you configure health checks. Confirm the success codes that the load balancer is expecting and that your application is configured to return these codes on success.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-troubleshooting.html#target-not-inservice

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html

Note:

For option B, when EC2 instances are configured in the Load Balancer, only these instances in the same Availability Zones as the ELB can be configured. So the description of the option is improper and it cannot be a possible reason to cause the instance to be unhealthy.

The question is asking to select the wrong answer:

Which of the following options **could not** be a reason for this? Based on this (Could not be a reason) condition, option B is the correct answer.

Ask our Experts

Rate this Question?

View Queries open

Question 7 Unattempted

Domain : Other

In an AWS Setup of a company, a web-based application has a fleet of 10 EC2 instances. 7 EC2 instances are present in Availability Zone A, whereas 3 EC2 instances in Availability Zone B. The percentage (%) of requests received in Availability Zone B is greater than the percentage (%) of requests in Availability Zone A. What can be done at the architecture level to balance the load across the two availability zones? Please select 3 correct options.

A. **Use Application Load Balancer to achieve this ability.**

B. **Enable "split traffic equally" checkbox under load balancer configuration.**

C. **This can be achieved through cross-zone load balancing**

D. **Use Network Load Balancer to achieve his ability.**

Explanation:

Answer: A, C, and D

Option A is correct. Please refer to AWS Link:

With Application Load Balancers, cross-zone load balancing is always enabled.

https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html#availability-zones

Option B is not correct. There is no such option.

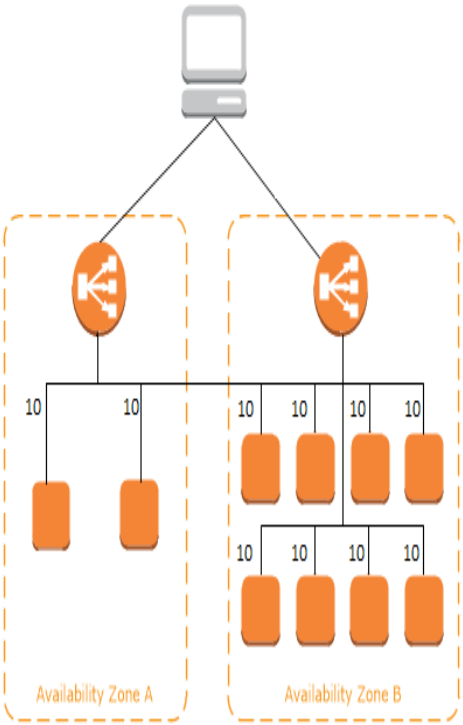
Option C is correct.

Cross-Zone Load Balancing

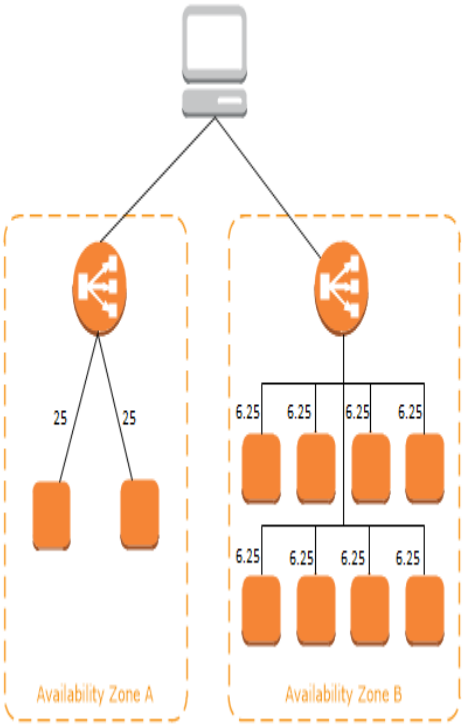
The nodes for your load balancer distribute requests from clients to registered targets. When cross-zone load balancing is enabled, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. When cross-zone load balancing is disabled, each load balancer node distributes traffic across the registered targets in its Availability Zone only.

The following diagrams demonstrate the effect of cross-zone load balancing. There are two enabled Availability Zones, with 2 targets in Availability Zone A and 8 targets in Availability Zone B. Clients send requests, and Amazon Route 53 responds to each request with the IP address of one of the load balancer nodes. This distributes traffic such that each load balancer node receives 50% of the traffic from the clients. Each load balancer node distributes its share of the traffic across the registered targets in its scope.

If cross-zone load balancing is enabled, each of the 10 targets receives 10% of the traffic. This is because each load balancer node can route its 50% of the client traffic to all 10 targets.



If cross-zone load balancing is disabled, each of the 2 targets in Availability Zone A receives 25% of the traffic and each of the 8 targets in Availability Zone B receives 6.25% of the traffic. This is because each load balancer node can route its 50% of the client traffic only to targets in its Availability Zone.



https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html#availability-zones

Option D is correct. Please refer to the below AWS documentation link:

https://aws.amazon.com/about-aws/whats-new/2018/02/network-load-balancer-now-supports-cross-zone-load-balancing/

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 8 Unattempted

Domain : Other

Which of the following are features for monitoring application load balancer? Choose the 3 correct options.

A. CloudWatch metrics ✓

B. Request tracing ✓

C. VPC Flow Logs

D. CloudTrail logs ✓

E. EC2 Flow Logs

Explanation:

Answer: A, B, D

Monitor Your Application Load Balancers

You can use the following features to monitor your load balancers, analyze traffic patterns, and troubleshoot issues with your load balancers and targets.

CloudWatch metrics

You can use Amazon CloudWatch to retrieve statistics about data points for your load balancers and targets as an ordered set of time-series data, known as *metrics*. You can use these metrics to verify that your system is performing as expected. For more information, see CloudWatch Metrics for Your Application Load Balancer.

Access logs

You can use access logs to capture detailed information about the requests made to your load balancer and store them as log files in Amazon S3. You can use these access logs to analyze traffic patterns and to troubleshoot issues with your targets. For more information, see Access Logs for Your Application Load Balancer.

Request tracing

You can use request tracing to track HTTP requests. The load balancer adds a header with a trace identifier to each request it receives. For more information, see Request Tracing for Your Application Load Balancer.

CloudTrail logs

You can use AWS CloudTrail to capture detailed information about the calls made to the Elastic Load Balancing API and store them as log files in Amazon S3. You can use these CloudTrail logs to determine which calls were made, the source IP address where the call came from, who made the call, when the call was made, and so on. For more information, see Logging API Calls for Your Application Load Balancer Using AWS CloudTrail.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-monitoring.html

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Question 9 Unattempted

Domain : Other

You have created a VPC with an application load balancer and selected two EC2 instances as targets. However, when you are trying to make a request to the internet-facing load balancer, the request fails. What could be the reason?

A. **The route table associated with the load balancer's subnet does not have a route to the internet gateway.** ✓

B. **Target EC2 instances are in a public subnet.**

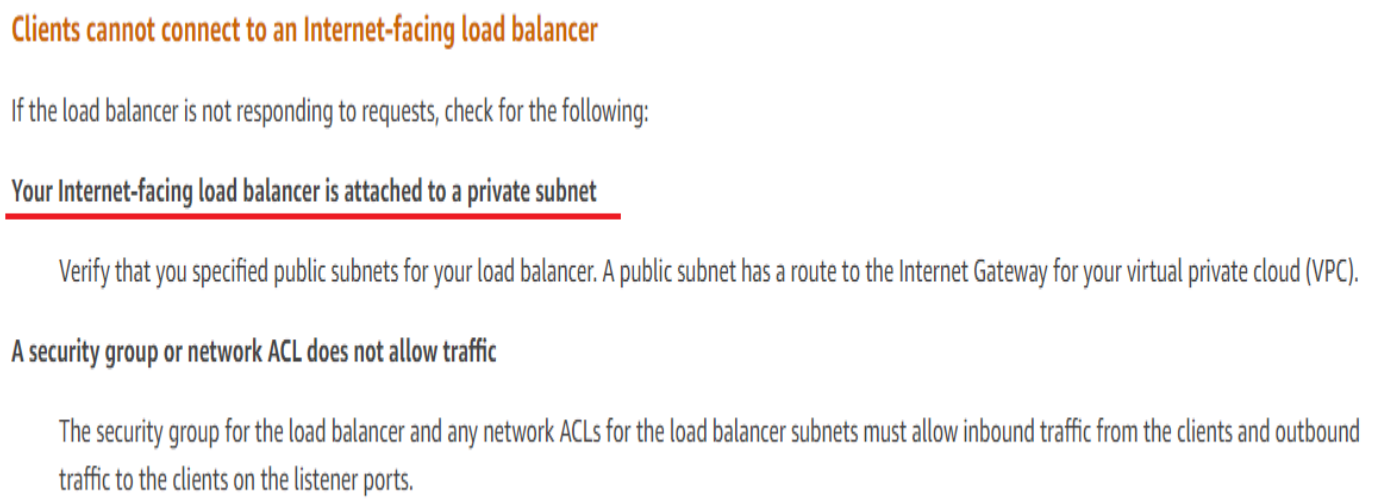
C. **There is no elastic IP address attached to the load balancer.**

D. **Cross-zone load balancing is not enabled.**

Explanation:

Answer: A

Option A is correct because there must be a route in a route table to the internet gateway for internet connectivity



Option B is incorrect because this does not result in the failure mentioned in the question.

Option C is incorrect because any instances in the VPC must either have a public IP address or an attached Elastic IP address. And for the internet-facing load balancer, AWS manages the underlying IP addresses. So no need for an Elastic IP address.

Option D is incorrect because cross-zone load balancing is not a reason to cause the failure.

With Application Load Balancers, cross-zone load balancing is always enabled.

https://aws.amazon.com/premiumsupport/knowledge-center/create-attach-igw-vpc/

Ask our Experts

Rate this Question?

View Queries open

Question 10 Unattempted

Domain : Other

Which of the following is a correct way to register a target in Elastic Load Balancer target group?

A. EC2 instance names

B. IP addresses

C. EC2 imageid

D. EC2 Primary Network Inteface ID

Explanation:

Answer: B

Target Type

When you create a target group, you specify its target type, which determines how you specify its targets. After you create a target group, you cannot change its target type.

The following are the possible target types:

`instance`

The targets are specified by instance ID.

`ip`

The targets are specified by IP address.

When the target type is `ip`, you can specify IP addresses from one of the following CIDR blocks:

- The subnets of the VPC for the target group
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

These supported CIDR blocks enable you to register the following with a target group: ClassicLink instances, instances in a peered VPC, AWS resources that are addressable by IP address and port (for example, databases), and on-premises resources linked to AWS through AWS Direct Connect or a VPN connection.

Important

You can't specify publicly routable IP addresses.

If you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance. If you specify targets using IP addresses, you can route traffic to an instance using any private IP address from one or more network interfaces. This enables multiple applications on an instance to use the same port. Each network interface can have its own security group.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#target-type

Ask our Experts

Rate this Question? ☺ ☹

View Queries open

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Become Our Instructor

Support

Discussions

Blog

Business

Support

Contact Us

Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

Follow us

Question 1 Correct

Domain: Other

Your company is planning on setting up a web-based application onto AWS. This would be a content-based system wherein you have users across the world who would want to access the content. You have to ensure that users worldwide get a seamless user experience when using the web application. Which of the below AWS service needs to be part of the architecture for this application?

A. Amazon SES

B. Amazon Cloudtrail

C. Amazon CloudFront right

D. Amazon S3

Explanation:

Answer – C

The AWS Documentation mentions the following.

Amazon CloudFront is a web service that speeds up the distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Option A is invalid since this is an email service.

Option B is invalid since this is an API monitoring service.

Option D is invalid since this is an object storage service.

For more information on Amazon CloudFront, please visit the below URL-

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

Ask our Experts

View Queries

Question 2 Correct

Domain: Other

Your company is planning to set up a web-based application onto AWS. The application will be connected to an AWS RDS instance. You need to ensure that the performance of the database layer is up to the mark if possible to ensure that recently queried results are delivered in a faster manner. Which of the following would be part of the architecture?

A. MySQL Installed on two Amazon EC2 Instances in a single Availability Zone

B. Amazon RDS for MySQL with Multi-AZ

C. Amazon ElastiCache right

D. Amazon DynamoDB

Explanation:

Answer – C

The AWS Documentation mentions the following.

Amazon ElastiCache offers fully managed Redis and Memcached. Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve your existing apps' performance by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for Gaming, Ad-Tech, Financial Services, Healthcare, and IoT apps.

Option A is invalid since this would not help with the caching of data.

Option B is invalid since this is used for fault tolerance.

Option D is invalid since this is a fully managed NoSQL database.

For more information on AWS ElasticCache, please visit the below URL-
https://aws.amazon.com/elasticache/

Ask our Experts

View Queries

Question 3 Correct

Domain: Other

Your company is planning on setting up a web-based application onto AWS. The IT management has given clear directions on ensuring that the application follows a serverless architecture in order to reduce infrastructure costs. Which of the following services could be used in this regard. Choose 3 answers from the options given below

A. AWS API Gateway right

B. AWS Lambda right

C. AWS DynamoDB right

D. AWS EC2

Explanation:

Answer - A,B and C

The AWS Documentation mentions the following

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling

For more information on API gateway, Lambda and DynamoDB, please visit the below URL

https://aws.amazon.com/api-gateway/

Ask our Experts

View Queries

Question 4 Incorrect

Domain: Other

Your company plans to set up a hybrid connection between their on-premises infrastructure and an AWS VPC via AWS VPN managed connections. As an architect, which of the following need to be in place for the connection to be established? Choose 2 answers from the options given below.

A. A hardware compatible VPN device right

B. A Virtual private gateway right

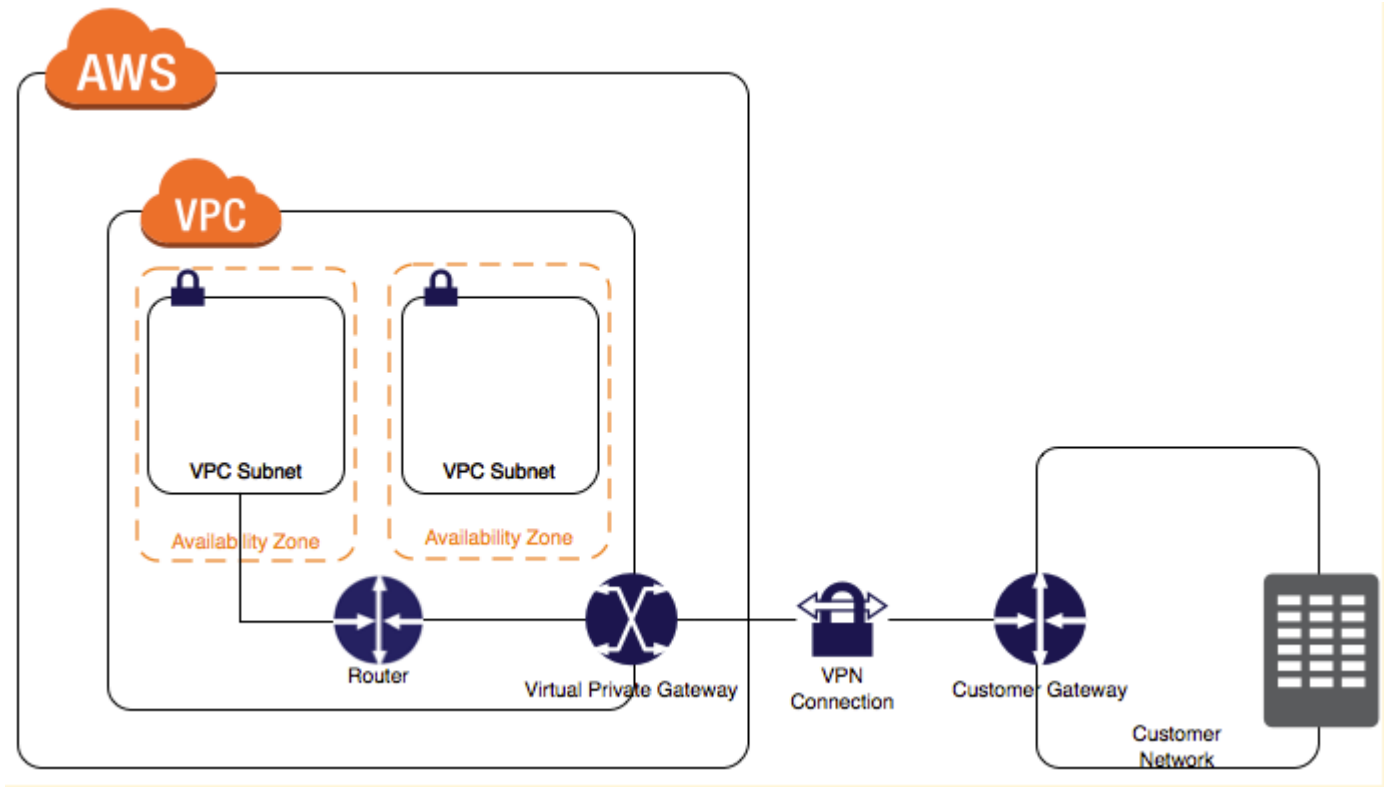
C. An AWS Direct connect device wrong

D. Optical fibre cables

Explanation:

Answer - A and B

When defining a VPN connection between the on-premises network and the VPC, you need to have a customer gateway defined. Since this is accessed over the internet, it needs to have a static internet-routable IP Address.



All other options are invalid since this is only required for an AWS Direct Connect connection.

For more information on AWS VPN connections, please visit the below URL-

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

Ask our Experts

View Queries

Question 5 Incorrect

Domain: Other

Your company currently has setup their data store on AWS DynamoDB. One of your main revenue generating applications uses the tables in this service. Your application is now expanding to 2 different other locations and you want to ensure that the latency for data retrieval is the least from the new regions. Which of the following can help accomplish this?

A. Place a cloudfront distribution in front of the database

B. Enable Multi-AZ for DynamoDB

C. Place an ElastiCache in front of DynamoDB wrong

D. Enable global tables for DynamoDB right

Explanation:

Answer - D

The AWS Documentation mentions the following

To illustrate one use case for a global table, suppose that you have a large customer base spread across three geographic areas—the US east coast, the US west coast, and western Europe. Customers would need to update their profile information while using your application. To address these requirements, you could create three identical DynamoDB tables named CustomerProfiles, in three different AWS regions. These three tables would be entirely separate from each other, and changes to the data in one table would not be reflected in the other tables. Without a managed replication solution, you could write code to replicate data changes among these tables; however, this would be a time-consuming and labor-intensive effort.

Option A is incorrect since cloudfront should ideally be used in front of web distributions

Option B is incorrect since this is not an option for DynamoDB

Option C is incorrect since would not be affective for multiple regions

For more information on AWS DynamoDB global tables, please visit the below URL

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html

Ask our Experts

View Queries

Question 6 Correct

Domain: Other

A company is planning on moving their virtual servers from their on-premises infrastructure to the AWS Cloud. They need to migrate their existing VM's to the cloud. Which of the following could help them in the migration process?

A. AWS VM Import right

B. AWS S3

C. AWS SQS

D. AWS EC2

Explanation:

Answer – A

The AWS Documentation mentions the following

VM Import/Export enables you to easily import virtual machine images from your existing environment to Amazon EC2 instances and export them back to your on-premises environment. This offering allows you to leverage your existing investments in the virtual machines that you have built to meet your IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances. You can also export imported instances back to your on-premises virtualization infrastructure, allowing you to deploy workloads across your IT infrastructure.

Option B is incorrect since this is an object storage service

Option C is incorrect since this is a queuing service

Option D is incorrect since this would be the virtual server on the cloud but would not assist in the actual migration of the server

For more information on AWS VM Import, please visit the below URL

https://aws.amazon.com/ec2/vm-import/

Ask our Experts

View Queries

Question 7 Correct

Domain: Other

A company is planning on moving their applications to the AWS Cloud. They have some large SQL data sets that need to be hosted in a data store on the cloud. The data store needs to have features that support client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools. Which of the following service should be considered for this requirement?

A. Amazon DynamoDB

B. Amazon Redshift right

C. Amazon Kinesis

D. Amazon Simple Queue Service

Explanation:

Answer – B

The AWS Documentation mentions the following.

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers.

Amazon Redshift supports client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools.

Option A is incorrect since this a NoSQL datastore.

Option C is incorrect since this is used for data streaming.

Option D is incorrect since this is used as a messaging service.

For more information on AWS Redshift, please visit the below URL-

https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html

https://docs.aws.amazon.com/redshift/latest/dg/redshift-dg.pdf

Ask our Experts

View Queries

Question 8 Correct

Domain: Other

Your company has a set of 100 servers hosted on the AWS Cloud. They need to stream the Logs from the Instances for analysis purposes. This is being done from a security compliance perspective. Programs will then run to analyse the data for any sort of abnormal behaviour. Which of the following would be used to stream the log data?

A. Cloudfront

B. SQS

C. Kinesis right

D. SES

Explanation:

Answer – C

The AWS Documentation mentions the following

Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

Option A is incorrect since this a content distribution service

Option B is incorrect since this is used as a messaging service

Option D is incorrect since this is an email service

For more information on AWS Kinesis, please visit the below URL

https://aws.amazon.com/kinesis/data-streams/faqs/

Ask our Experts

View Queries

Question 9 Correct

Domain: Other

You have been hired as an AWS Architect for a company. There is a requirement to host an application using EC2 Instances. The Infrastructure needs to scale on demand and also be fault tolerant. Which of the following would you include in the design? Choose 2 answers from the options below

A. AWS Autoscaling right

B. AWS ECS

C. AWS Elastic Load Balancer right

D. AWS Cloudwatch

Explanation:

Answer - A and C

The AWS Documentation mentions the following

You can automatically increase the size of your Auto Scaling group when demand goes up and decrease it when demand goes down. As the Auto Scaling group adds and removes EC2 instances, you must ensure that the traffic for your application is distributed across all of your EC2 instances. The Elastic Load Balancing service automatically routes incoming web traffic across such a dynamically changing number of EC2 instances.

Option B is incorrect since this is used when you need a docker orchestration service

Option D is incorrect since this is a monitoring service

For more information on AWS Autoscaling and ELB, please visit the below URL

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

Ask our Experts

View Queries

Question 10 Incorrect

Domain: Other

Your company has setup EC2 Instances in a VPC for their application. They now have a concern that not all of the EC2 instances are being utilized. Which of the below mentioned services can help you find underutilized resources in AWS? Choose 2 answers from the options given below

A. AWS Cloudwatch right

B. SNS

C. AWS Trusted Advisor right

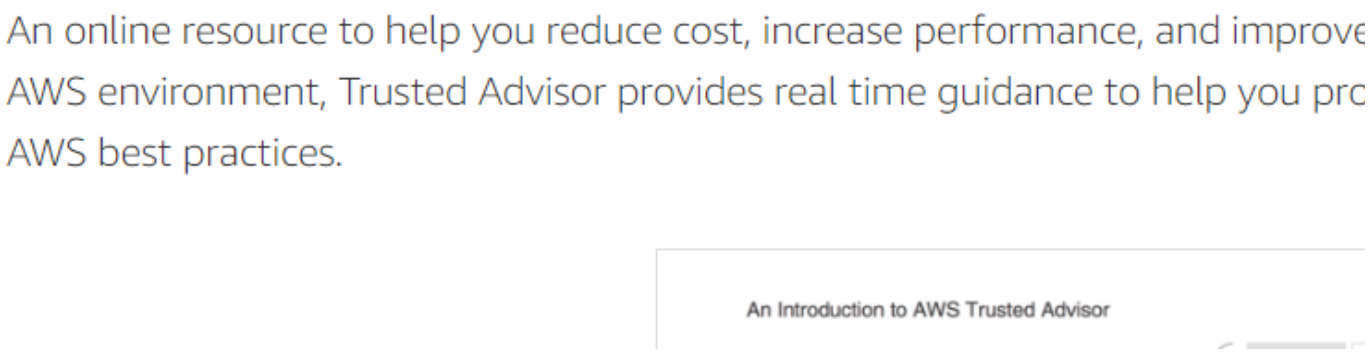
D. Cloudtrail wrong

Explanation:

Answer - A and C

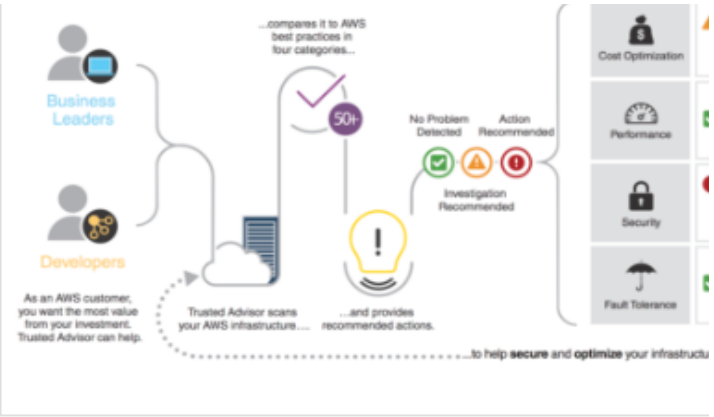
The AWS Documentation mentions the following

"An online resource to help you reduce cost, increase performance,and improve security by optimizing your AWS environment,Trust Advisor provides real time guidance to help you provison your resources following AWS best practices"



An Introduction to AWS Trusted Advisor

(click to enlarge)



Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

Option B is incorrect since this is a notification service

Option D is incorrect since this is an API monitoring service

For more information on AWS Trusted Advisor and Cloudwatch, please visit the below URL

https://aws.amazon.com/premiumsupport/trustedadvisor/

https://aws.amazon.com/cloudwatch/

Ask our Experts

View Queries

Question 11 Correct

Domain: Other

Your company has setup EC2 Instances in a VPC for their application. The IT Security department has advised that all traffic be monitored to the EC2 Instances. Which of the following features can be used to capture information for outgoing and incoming IP traffic from network interfaces in a VPC.

A. AWS Cloudwatch

B. AWS EC2

C. AWS SQS

D. AWS VPC Flow Logs right

Explanation:

Answer – D

The AWS Documentation mentions the following

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Option A is incorrect since this is a monitoring service

Option B is incorrect since this is a compute service

Option C is incorrect since this is a messaging service

For more information on VPC flow logs, please visit the below URL

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

Ask our Experts

View Queries

Question 12 Correct

Domain: Other

Your company has setup EC2 Instances in a VPC for their application. The IT Security department needs to understand what the security mechanisms are available to protect the Instances when it comes to traffic going in and out of the

instance. What are the two layers of security provided by AWS in the VPC? Choose 2 answers from the options given below

A. Security Groups right

B. NACLs right

C. DHCP Options

D. Route Tables

Explanation:

Answer - A and B

The AWS Documentation mentions the following

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance.

A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Option C is incorrect since this is used to decide on the DNS servers for the VPC

Option D is incorrect since this is used for routing traffic in the VPC

For more information on VPC security groups and NACL's, please visit the below URL

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

Ask our Experts

View Queries

Question 13 Correct

Domain: Other

A company has recently chosen to use the AWS API Gateway (including API Cache) service for managing its APIs. Which of the following service can be integrated with the API gateway service in the background to ensure a better response to calls made to the API Gateway?

A. AWS CloudWatch

B. AWS CloudFormation

C. AWS Volume Gateway

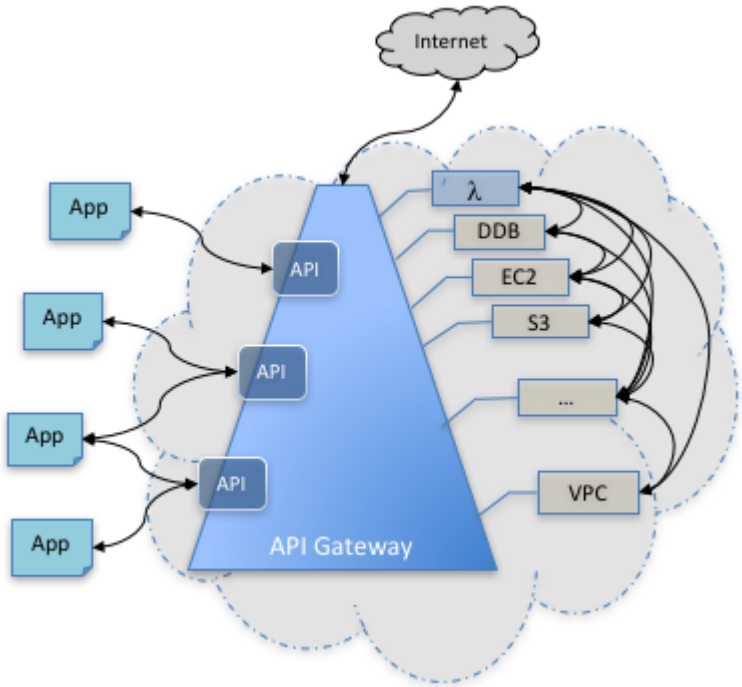
D. AWS Lambda right

Explanation:

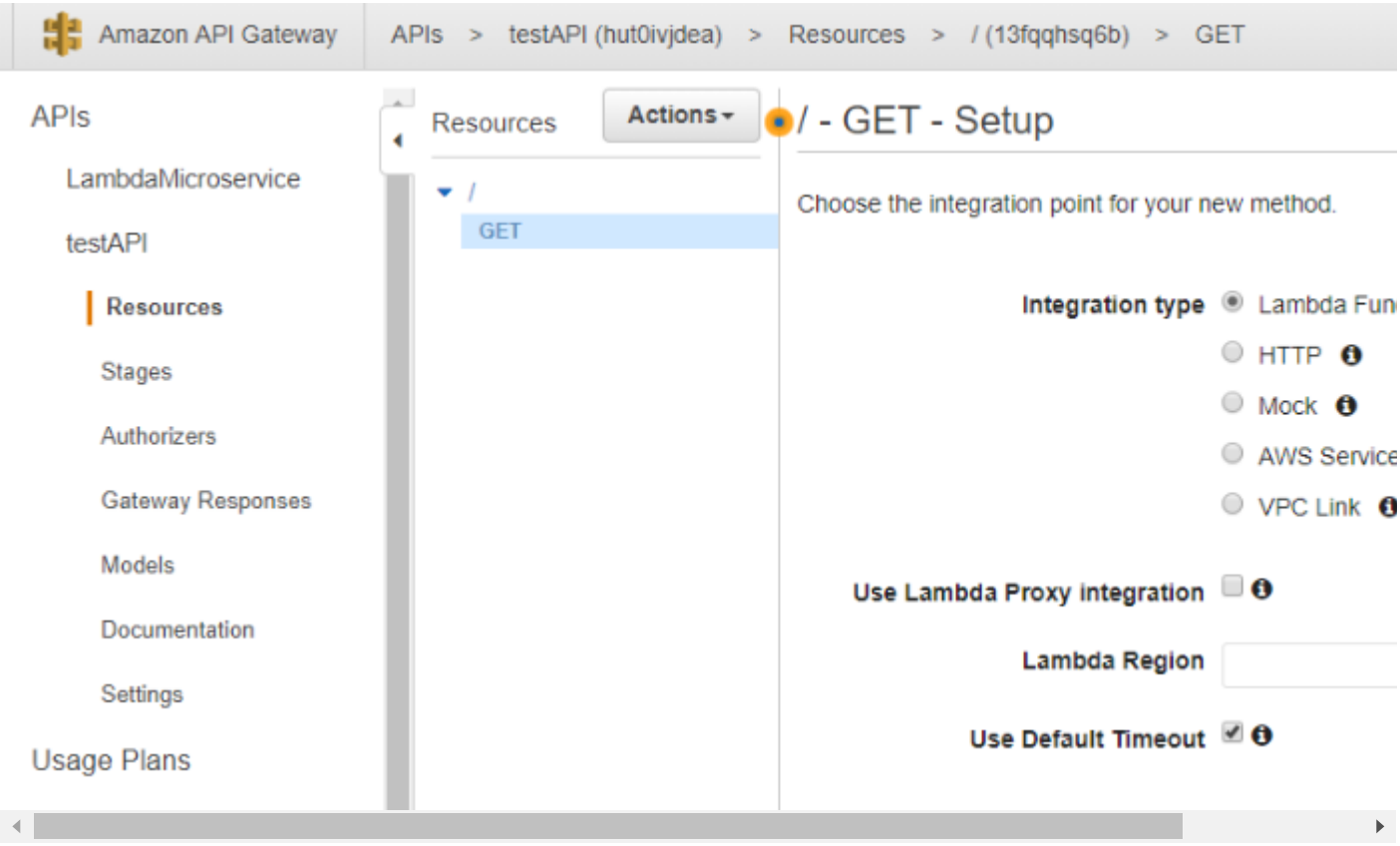
Answer – D

API Gateway is designed for web and mobile developers who want to provide secure, reliable access to back-end APIs for access from mobile apps, web apps, etc.

The business logic behind the APIs can be provided by a publicly accessible endpoint that API Gateway proxies call or can be entirely run as a Lambda function.



For example, an application can call an API in API Gateway to upload a user's annual income and expense data to Amazon S3 or Amazon DynamoDB, process the data in AWS Lambda to compute tax owed, and file a tax return.



Option A is incorrect. CloudWatch offers Cloud Monitoring services for the resources being used.

Option B is incorrect. AWS CloudFormation provides templates for the creation of resources in the AWS cloud.

Option C is incorrect. AWS Volume Gateway service is used to store data in the AWS Cloud. It offers scalable and cost-effective storage.

For more information on the features of the API gateway, please refer to the below URL-

https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html

Ask our Experts

View Queries

Question 14 Correct

Domain: Other

A company has recently chosen to use the AWS API Gateway service for managing their API's. It needs to be ensured that code hosted in other domains can access the API's behind the API gateway service. Which of the below security features of the API gateway can be used to ensure that API's resources can receive requests from a domain other than the API's own domain?

A. API Stages

B. API Deployment

C. API CORS right

D. API Access

Explanation:

Answer – C

The AWS Documentation mentions the following.

When your API's resources receive requests from a domain other than the API's own domain, you must enable cross-origin resource sharing (CORS) for selected methods on the resource. This amounts to having your API respond to the OPTIONS preflight request with at least the following CORS-required response headers:

Access-Control-Allow-Methods

Access-Control-Allow-Headers

Access-Control-Allow-Origin

Option A and B are invalid because these are used to ensure users can call API's.

Option D is invalid because there is no such thing as API Access.

For more information on enabling CORS, please refer to the below URL-

http://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html

Ask our Experts

View Queries

Question 15 Correct

Domain: Other

Your company is planning on developing and deploying an application onto AWS. The application will follow a microservices based architecture which will involve the deployment of several docker containers. Which of the following services is ideal for this scenario?

A. DynamoDB

B. Simple Queue Service

C. Elastic Container Service right

D. CodeCommit

Explanation:

Answer - C

The AWS Documentation mentions the following

Amazon EC2 Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster of Amazon Elastic Compute Cloud (Amazon EC2) instances. Amazon ECS lets you launch and stop container-based applications with simple API calls, allows you to get the state of your cluster from a centralized service, and gives you access to many familiar Amazon EC2 features.

Option A is invalid because this is a fully managed NoSQL database

Option B is invalid because this is a messaging service

Option D is invalid because this is a code versioning service

For more information on Elastic Container service , please refer to the URL:

http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

Ask our Experts

View Queries

Question 16 Correct

Domain: Design Resilient Architectures

A company offers its customers short-lived contests that require users to upload files in hopes of winning prizes. These contests can last up to two weeks, with unknown uploads. The resulting file analysis can last up to three months.

The company needs an economical, scalable object storage solution to hold its customers' files. The files will be accessed once and then deleted, and it requires immediate access. The best solution for this company is:

A. Amazon Glacier

B. Elastic File System

C. Amazon S3 Standard

D. Amazon S3 Standard Infrequent Accessed right

Explanation:

Answer:

D. S3 – IA for data that is accessed less frequently, but requires rapid access when needed.

Incorrect:

A. Amazon Glacier is for data archiving and can be accessed within minutes.

B. Elastic File System is file storage, not object storage as required.

C. S3 standard is for frequently accessed data, and less economical than S3 - IA.

Reference:

https://aws.amazon.com/s3/storage-classes/

https://aws.amazon.com/efs/when-to-choose-efs/

Ask our Experts

View Queries

Question 17 Incorrect

Domain: Specify Secure Applications and Architectures

A company has been using AWS cloud services for six months and just finished a security review. Which finding below is considered a best practice in the security pillar of the well-architected framework?

A. Using the root user to create all-new user accounts, at any time.

B. Monitoring and using alerts using CloudTrail and CloudWatch. right

C. Assigning Private IP address ranges to VPCs that do not overlap. wrong

D. Designing the system using elasticity to meet changes in demand.

Explanation:

Answer:

B. Monitoring and alerting for key metrics and events is a best practice of the Security pillar.

Incorrect:

A. For the root user, you should follow the best practice of only using this login to create another, initial set of IAM users and groups for longer-term identity management operations.

C. Non-overlapping Private IP addresses is in the Reliability pillar.

D. Design using elasticity to meet demand is in the Performance Efficiency pillar (Design for Cloud Operations).

Reference:

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

Ask our Experts

View Queries

Question 18 Incorrect

Domain: Design Resilient Architectures

A website is hosted on two EC2 instances that sit behind an Elastic Load Balancer. The response time of the website has slowed dramatically, and customers are ordering less due to the wait time. Troubleshooting showed one of the EC2 instances failed and left just one instance running. What is the best course of action to prevent this from happening in the future?

A. Change the instance size to the maximum available to compensate for failure. wrong

B. Use CloudWatch to monitor the VPC Flow Logs for the VPC the instances are deployed in.

C. Configure the ELB to perform health checks on the EC2 instances and implement auto-scaling. right

D. Replicate the existing configuration in several regions for failover.

Explanation:

Answer:

Correct:

C. Using the elastic load balancer to perform health checks will determine whether or not to remove a non- or underperforming instance and have the auto-scaling group launch a new instance.

Incorrect:

A. Increasing the instance size doesn't prevent the failure of one or both the instances. Therefore the website can still become slow or unavailable.

B. Monitoring the VPC flow logs for the VPC will capture VPC traffic, not traffic for the EC2 instance. You would need to create a flow log for a network interface.

D. Replicating the same two instance deployment may not prevent failure of instances and could still result in the website becoming slow or unavailable.

Reference:

https://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#working-with-flow-logs

Ask our Experts

View Queries

Question 19 Correct

Domain: Design Cost-Optimized Architectures

A small company started using EBS backed EC2 instances due to the cost improvements over running their own servers. The company's policy is to stop the development servers over the weekend and restart them each week. The first time

the servers were brought back. None of the developers were able to SSH into them. What did the server most likely overlook?

A. The associated Elastic IP address has changed and the SSH configurations were not updated.

B. The security group for a stopped instance needs to be reassigned after start.

C. The public ip4 address has changed on server start and the SSH configurations were not updated. right

D. EBS backed EC2 instances cannot be stopped and were automatically terminated.

Explanation:

Answer:

Correct:

C. The instance retains its private IPv4 addresses and any IPv6 addresses when stopped and restarted. AWS releases the public IPv4 address and assigns a new one when it's restarted.

Incorrect:

A. An EC2 instance retains its associated Elastic IP addresses.

B. Security groups do not need to be reassigned to instances that are restarted.

D. EBS backed instances are the only instance type that can be started and stopped.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html

Ask our Experts

View Queries

Question 20 Correct

Domain: Define Performant Architectures

You want to use AWS to host your own website with a unique domain name that uses the format www.example.com. It needs to be deployed quickly and doesn't require server-side scripting. What is your best option?

A. Register a domain with Route53 and verify ahead of time that a unique S3 bucket name can be created. right

B. Create an auto-scaling group of EC2 instances and manage the web hosting on these instances.

C. Create one large EC2 instance to host the website and replicate it in every region.

D. Create a Content Delivery Network (CDN) to deliver your images and files.

Explanation:

Answer:

Correct:

A. S3 static webhosting is the quickest way to set up this website. Because bucket names are unique across all regions, it is important to know that your S3 bucket is available before purchasing a domain name.

Incorrect:

B. Hosting on EC2 is not necessary here as server-side scripting is not needed, and S3 will scale automatically.

C. Hosting on EC2 is not necessary, and this particular implementation can lead to different configurations on each server.

D. A CDN will improve the delivery time of your files and pages to the customer but is not a hosting solution itself.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront-walkthrough.html

RDS & DynamoDB

Completed on 26-July-2021

Attempt	Marks Obtained	Your score
01	6 / 10	60%

Time Taken	Result
00 H 10 M 55 S	Failed

Domains wise Quiz Performance Report

Join us on Slack community

No	1
Domain	Other
Total Question	10
Correct	6
Incorrect	4
Unattempted	0
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	10
Correct	6
Incorrect	4
Unattempted	0
Marked for review	0

~~Review the Answers~~

~~Sorting by~~ ~~All~~

Question 1 Incorrect

Domain : Other

You are working as a Cloud Architect in a big IT Firm. To ensure high availability of both the web servers and your web application database, you deployed your auto-scaled EC2 instances in multiple Availability Zones with an Application Load Balancer in front. You configured Multi-Availability Zone to your RDS instance. There is a spike in incoming requests in the past few hours, and the performance of the primary database is starting to go down. What would happen to the database if the primary DB instance fails?

A. **The IP address of the primary DB instance is switched to the standby DB instance.**

B. **The RDS DB instance will automatically reboot.**

C. **A new DB instance will be created and immediately replace the primary database.**

D. **The canonical name record is changed from the primary database to the standby database.**

Explanation:

Answer: D

Option A is incorrect because IP Address is associated with A Records in DNS, but for Database, you need to change the CNAME record.

Option B is incorrect because RDS Instance is pointed to standby RDS.

Option C is incorrect because this option is not reliable in real-time.

Option D is correct because the failover mechanism automatically changes the DNS CNAME record of the DB instance to point to the standby DB instance.

Refer:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

Ask our Experts

Rate this Question?

View Queries open

Question 2 Correct

Domain : Other

A company is planning to migrate an on-premise 15 TB MySQL database cluster onto AWS. The replication lag needs to be less than 100 ms for the cluster, and the size is expected to double in the next couple of months. Which of the following would be the ideal data store that should be chosen in AWS?

A. AWS RDS MySQL

✓ B. AWS Aurora

C. AWS DynamoDB

D. AWS Redshift

Explanation:

Answer: B

Option B is correct because all Aurora Replicas returns query results with minimal replica lag—usually much less than 100 milliseconds after the primary instance has written an update. For Scaling, this is the best among all the options. The minimum storage is for AWS Aurora is 10GB. Based on your database usage, your Amazon Aurora storage will automatically grow, up to 64 TB, in 10GB increments with no impact on database performance. There is no need to provision storage in advance. Amazon Aurora is a compatible MySQL database that can take on tremendous growth in terms of the data size.

Refer:

https://aws.amazon.com/rds/aurora/faqs/

Ask our Experts

Rate this Question?

View Queries open

Question 3 Correct

Domain : Other

A complex enterprise application is hosted on an M5.XLarge on-demand EC2 instance with DynamoDB as its database. You created a table called "coursedetails" which has a hash key of "course_id". You can query the data based on the "course_id" hash key without any issues. Your Supervisor then told you that the web application should also be able to query the "coursedetails" table by "student_name". What would you do to configure your DynamoDB to meet the above requirement properly? The table "coursedetails" consists of 3 columns i.e. course_id (hash key), course_name, student_name.

A. Configure the DynamoDB instance to have a second table which contains all the information by "student_name".

B. Set up an In-Memory Acceleration with DAX in your DynamoDB instance.

✓ C. Configure the "coursedetails" table to use "student_name" as a Global secondary index

D. The requirement is beyond the capability of DynamoDB.

Explanation:

Answer: C

Option A is incorrect because DynamoDB is not designed as a relational database and does not support join operations. You can think about DynamoDB as just being a set of key-value pairs. You can have the same keys across multiple tables, but DynamoDB doesn't automatically sync them or have any foreign-key features. The columns in one table, while named the same, are technically a different set than the ones in a different table. It's up to your application software to make sure that those keys are synced.

Option B is incorrect because In-Memory Acceleration with DAX is used for caching the query.

Option C is correct because we don't know the course_id of those "student_name", that's what we want to get. So we find ourselves without knowing the items' hash key values. That's where **GSI** is used. **Global Secondary Indexes** let you define a different hash key for your table. **Note that it will**

not change the primary hash key – "course_id" **will still be the table's hash key.** GSI only provides an additional hash key for you to be able to make more complex queries.

Option D is incorrect because it is under the capability of DynamoDB.

Refer:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-gsi-aggregation.html

Ask our Experts

Rate this Question?

View Queries open

Question 4 Incorrect

Domain : Other

You are working as an AWS Architect for a multinational bank with hybrid cloud architecture. The bank is running a currency exchange website that uses a MySQL Server RDS instance as its database. As part of the company's business continuity plan, there is a need to keep a read replica of the production RDS instance to the bank's on-premise data center. In this scenario, what is the most secure and effective way to meet this requirement?

A. Change the MySQL Server RDS instance as the master node and then enable replication over the public Internet using a secure SSL endpoint to a server on the on-premise data center.

B. Configure the MySQL Server RDS instance to replicate to an EC2 instance with core MySQL and then enable Replication over a secure VPN connection.

C. Use native backup and restore for MySQL Server databases using full backup files by storing it on Amazon S3, and then restore the backup file onto an on-premises server.

D. Create an IPsec VPN connection through the Virtual Private Cloud service and configure replication in MySQL Server.

Explanation:

Answer: D

Option A is incorrect as it is feasible. You could put your RDS DB in a public subnet and configure SSL for it. But you have been asked for the most secure way.

Option B is incorrect because Even EC2 is external to RDS, and it won't be a secure option.

Option C is incorrect because it describes a backup-restore solution.

Option D is correct because it provides the most secure direct connection from the RDS MySQL Server instance to the On-Premise data center, and replication can be configured within the MySQL Server service since it can't be done from the RDS service to the On-Premise data center.

Refer:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl

Ask our Experts

Rate this Question?

View Queries open

Question 5 Correct

Domain : Other

Your team has developed an online feedback application for the best image competition in AWS using CloudFormation. The application accepts high-quality images of each participant and stores them in S3. Then it records the information about the image as well as the participant's profile in RDS. After the competition, the CloudFormation stack is not used anymore and should be terminated to save the cost. Your manager instructed you to back up the RDS database and the S3 bucket so the data can still be used even after the CloudFormation template is deleted. Which of the following options will fulfill this requirement?

A. **Set the DeletionPolicy for the RDS instance to snapshot and then enable S3 bucket replication on the source bucket to a destination bucket to maintain a copy of all the S3 objects.**

B. **Set the DeletionPolicy to retain on both the RDS and S3 resource types on the CloudFormation template.**

C. **Set the DeletionPolicy on the S3 bucket to snapshot**

✓ D. **Set the DeletionPolicy on the RDS resource to snapshot and set the S3 bucket to retain.**

Explanation:

Answer: D

Option A is incorrect because a replica of the S3 bucket is not required. We can directly retain it.

Option B is incorrect because we can retain a snapshot of RDS, not S3.

Option C is incorrect because RDS also needs to be backed up.

Option D is correct because The Retain option keeps the resource in the event of a stack deletion.
The Snapshot option creates a snapshot of the resource before that resource is deleted.
The Delete option deletes the resource along with the stack.

Refer:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html

Ask our Experts

Rate this Question?

View Queries open

Question 6 Incorrect

Domain : Other

You are working as a Cloud Engineer for a startup company that is planning to develop a web application with a ReactJS frontend and DynamoDB with provisioned throughput (1000 Writes/Sec) as its database. They are expecting a high number of writes on the database during peak hours (3000 Writes/Sec). How could you ensure the scalability and cost-effectiveness of the application to reduce the load on the DynamoDB database? (Choose 3 options)

A. **Add more DynamoDB databases to handle the load.**

✓ B. **Use DynamoDB Auto Scaling.**

✓ C. **Increase write capacity of DynamoDB to meet the peak loads.**

D. Use SQS to assist and let the application pull messages and then perform the relevant operation In DynamoDB.

E. Use Kinesis to assist and let the application pull messages and then perform the relevant operation in DynamoDB.

Explanation:

Answer: B, D and E

Option A is incorrect because this option is neither Cost-effective nor reliable.

Option B is correct because if your application can handle some throttling from DynamoDB when there's a sudden increase in traffic, you should use DynamoDB Auto Scaling.

Option C is incorrect because you have to do the same thing manually again and again in the future.

Option D is correct because you could either put all the messages into SQS first or use SQS as an overflow buffer when you exceed the design throughput on your DynamoDB database.

Option E is correct because if the order of the messages coming in is extremely important, Kinesis is another option for you to ingest the incoming messages and then insert them into DynamoDB, in the same order they arrived, at a pace you define.

Refer:

https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

Ask our Experts

Rate this Question?

View Queries open

Question 7 Correct

Domain : Other

Your company has got a client whose data is stored in AWS for a 3-tier application. The relational database should be highly durable and support schema changes. Changes to the database should not result in downtime. As a Cloud Architect of the Company, Which of the following would be the best data storage option for the Client?

A. AWS S3

B. AWS Redshift

C. AWS DynamoDB

✓ D. AWS Aurora 

Explanation:

Answer: D

Option D is correct because Amazon Aurora is a relational database and supports working with schema changes.

Option A, B, C are incorrect none of these are have these features together.

Refer:

https://aws.amazon.com/blogs/database/amazon-aurora-under-the-hood-fast-ddl/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.FastDDL.

Ask our Experts

Rate this Question?  

View Queries open

Question 8 Incorrect

Domain : Other

An online eCommerce WordPress Website is currently storing its records in a Single MySQL RDS database in AWS. After few days, there are severe performance issues on the database. They tried to Scale up the DB Instance. Right now, they are using SQS to pull up the queries in Queue. Which of the

following can be added to the architecture to rectify the performance issue and the solution must be cost-effective?

A. Enable Multi-AZ for the database.

B. Use Elasticache Service.

C. Place a Load Balance in front of database.

D. Use Cloudfront in front of the database.

Explanation:

Answer: B

Option A is incorrect because Multi-AZ is used for standby purposes and not for performance issues.

Option B is correct because the Elasticache service can be used to cache all the common queries. Hence if the same queries are causing the problem, the data sets will be fetched from Elasticache, instead of the database. This will reduce the load on the database server.

Option C is incorrect because Load Balance can't be used on a single database server.

Option D is incorrect because Cloudfront is caching the data on a remote edge location which means that the request is not even going to the origin server.

Refer:

https://aws.amazon.com/elasticache/

Ask our Experts

Rate this Question?

View Queries open

Question 9 Correct

Domain : Other

You are working in a Research and Development Department in IT Company where you as a Cloud Architect, trying to check the impact on real-time transactions. You created a multi-AZ RDS setup consisting of a Primary instance and a Read-replica. What is the impact of the read-replica on the transactions in the primary instance?

A. Transaction are impacted only if you configured it for Synchronous Replication.

B. Transaction are impacted only if you configured it for Asynchronous Replication.

✓ C. Transactions are not impacted.

D. Transactions are impacted.

Explanation:

Answer: C

Option C is correct because, for multi-AZ high availability, RDS uses synchronous replication between primary and standby systems. On the other hand, RDS Read Replica uses asynchronous replication, and any slowness in the Read Replica instance would simply cause data lag only in the read - replica. Transactions in primary are not impacted.

Refer:

https://aws.amazon.com/rds/faqs/

Ask our Experts

Rate this Question?

View Queries open

Question 10 Correct

Domain : Other

A company is planning to migrate its existing on-premise application to the AWS Cloud. The application currently runs on .Net and uses Microsoft SQL Server as the backend database. Your Company has some limitations as they don't have the developers currently to make recent changes to the code. Also, they don't have the Infrastructure team currently to manage the infrastructure on AWS. Which of the following data service would your Company choose on AWS for the best use?

A. AWS RDS

B. AWS DynamoDB

C. AWS Aurora

D. AWS Redshift

Explanation:

Answer: A

Option A is correct because one can use the AWS RDS service and choose the Microsoft SQL Server platform. Since the company does not have the developers available to make large code changes, they can migrate the data and change the connection strings in the code. Also, in the absence of the Infrastructure team, the AWS RDS service takes care of the Infrastructure.

Option B, C, D are incorrect because managing code and Infrastructure can't be done.

Refer to Easy to administer Section:

https://aws.amazon.com/rds/

~~Ask our Experts~~

~~Rate this Question?~~

~~View Queries~~ ~~open~~

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Become Our Instructor

Support

Discussions

Blog

Business

Support

Contact Us

Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

Follow us