



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

Custom View Settings

Topic 1 - Exam A**Topic 1****Question #1**

A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resources stored within VPCs.

The company has the following DNS resolution requirements:

On-premises systems should be able to resolve and connect to cloud.example.com.

All VPCs should be able to resolve cloud.example.com.

There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway.

Which architecture should the company use to meet these requirements with the HIGHEST performance?

- A. Associate the private hosted zone to all the VPCs. Create a Route 53 inbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
- B. Associate the private hosted zone to all the VPCs. Deploy an Amazon EC2 conditional forwarder in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the conditional forwarder.
- C. Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the outbound resolver.
- D. Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

Correct Answer: D

Community vote distribution

A (85%) D (15%)

✉ **buvumathelegend** 3 months, 1 week ago
itexamslab.com

This Answer is correct

upvoted 58 times

✉ **boceni** 2 weeks, 4 days ago

I took the AWS Certified Solutions Architect - Professional exam (SAP-C02) and passed it a week ago on my first attempt (my score was an 825). This was my first ever AWS exam so while taking the CLF and/or SAA may provide additional preparation for the SAP exam

upvoted 1 times

✉ **Odenkyem** 1 week, 5 days ago

Did you use this resource

upvoted 1 times

✉ **robertohyena** 1 year, 4 months ago

A. Correct answer. Source: <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

NOT B. EC2 conditional forwarder will not meet Highest performance requirement.

NOT C. Missing: Need to associate private hosted zone to all VPC.

"All VPC's will need to associate their private hosted zones to all other VPC's if required to."

Source: <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

NOT D. Missing: Need to associate private hosted zone to all VPC.

"All VPC's will need to associate their private hosted zones to all other VPC's if required to."

Source: <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

upvoted 51 times

✉ **awsylum** 1 month, 2 weeks ago

In your link, you missed this sentence:

"The most reliable, performant and low-cost approach is to share and associate private hosted zones directly to all VPCs that need them."

You share the PHZ via the Shared Services VPC. You use the .2 DNS Resolver Address in each VPC to connect to the PHZ in the shared services VPC for domain resolution.

upvoted 1 times

✉ **alexkro** 1 week, 6 days ago

You forgot an additional condition mentioned in the question: "All VPCs should be able to resolve cloud.example.com." Nobody said there are only shared VPCs there.

upvoted 1 times

✉ **ichi2kazu** **Most Recent** 2 days, 15 hours ago

i think A.

upvoted 1 times

✉ **jj888** 5 days, 1 hour ago

Selected Answer: A

All VPC's will need to associate their private hosted zones to all other VPC's if required to

upvoted 1 times

✉ **frmynd** 1 week, 1 day ago

Selected Answer: A

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-cloud-dns-options-for-vpc/route-53-resolver-endpoints-and-forwarding-rules.html>

upvoted 1 times

✉ **gofavad926** 3 weeks, 3 days ago

Selected Answer: A

By associating the Route 53 private hosted zone with all VPCs, resources within any of those VPCs can resolve domain names within the cloud.example.com domain.

upvoted 1 times

✉ **MoTOne** 4 weeks ago

Selected Answer: D

Using "share service" is the magic word here

upvoted 1 times

✉ **leoncao** 1 month ago

Selected Answer: A

D is definitely wrong

upvoted 2 times

✉ **Dgix** 1 month, 1 week ago

A and B are out since they talk about attaching the private domain to all accounts. This is wrong; you attach it to the shared VPC in the networking account which then is used for any local VPCs. This reduces the question to whether we need an inbound or outbound resolver for the on-prem infra; the answer is that for on-prem to be able to resolve the domain, we need an inbound resolver. And therefore the only possible correct answer is D.

I see that most people voted A, but I'm afraid that's wrong.

upvoted 1 times

✉ **24Gel** 1 month, 1 week ago

B C are definitely not answers

upvoted 1 times

✉ **luis_guevara** 1 month, 2 weeks ago

Selected Answer: D

Most efficient way to get all the VPC's to be able to resolve the private domain is using a shared services VPC.

upvoted 3 times

✉ **awsylum** 1 month, 2 weeks ago

The answer is D. Why? Because you associate a single Private Hosted Zone with DNS Resolvers in multiple VPCs (.2 address). You don't associate a PHZ in each VPC. That's the point of each VPC having a DNS Resolver address. So, you use the Shared Services VPC to host the PHZ with the Route53 inbound endpoint. Each VPC uses the DNS Resolver address to connect to the Shared Services VPC. And on the flip side, the Transit Gateway allows the on-prem traffic to connect to all VPCs using the Route53 inbound endpoint. Scroll down to the On premises section of this page: <https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/>

upvoted 2 times

✉ **awsylum** 1 month, 2 weeks ago

Just to clarify, the Transit Gateway is to provide Layer 3 networking between the on-prem and AWS environments, while the Inbound Route53 Endpoint is used to join the DNS of on-prem and AWS environments. I kind of mixed the two up in my explanation above.

upvoted 1 times

✉ **awsgEEK75** 2 months, 1 week ago

Selected Answer: A

BC don't have a resolver setup for on-prem traffic as outbound resolver is on AWS side. Even if D works, the traffic will have taken a longer route.
D It is not connecting all the VPCs

upvoted 2 times

👤 **GibaSP45** 3 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/>

upvoted 3 times

👤 **atirado** 3 months, 3 weeks ago

Selected Answer: A

All options mention a Shared Services VPC that is not in the question. This is used for Route 53 for cloud.example.com.

Option A - Associating all VPCs with the private hosted zone allows resolution of cloud.example.com; an inbound resolves allows on-premise resource to resolve to cloud.example.com; the final bit of connectivity allows on-premise to connect and resolve to cloud.example.com

Option B - An Amazon EC2 Conditional Forwarder does not apply in this situation because an Active Directory is not in play in this situation

Option C - Would not work because it is relying on an Outbound resolver (from cloud to on-premise)

Option D - Would not work because the other VPCs are not connected to the private zone. Moreover, connectivity is not complete because only the Shared Services VPC is connected to the Transit Gateway

upvoted 3 times

👤 **folmedispi** 3 months, 3 weeks ago

Selected Answer: A

itexamstest.com

no dissucusion A :)

upvoted 35 times

👤 **cgsoft** 3 months, 4 weeks ago

Selected Answer: A

All VPCs should be able to resolve cloud.example.com. This is possible if all VPCs are associated with the private hosted zone.

upvoted 1 times

Question #2

Topic 1

A company is providing weather data over a REST-based API to several customers. The API is hosted by Amazon API Gateway and is integrated with different AWS Lambda functions for each API operation. The company uses Amazon Route 53 for DNS and has created a resource record of weather.example.com. The company stores data for the API in Amazon DynamoDB tables. The company needs a solution that will give the API the ability to fail over to a different AWS Region.

Which solution will meet these requirements?

- A. Deploy a new set of Lambda functions in a new Region. Update the API Gateway API to use an edge-optimized API endpoint with Lambda functions from both Regions as targets. Convert the DynamoDB tables to global tables.
- B. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- C. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a failover record. Enable target health monitoring. Convert the DynamoDB tables to global tables.
- D. Deploy a new API Gateway API in a new Region. Change the Lambda functions to global functions. Change the Route 53 DNS record to a multivalue answer. Add both API Gateway APIs to the answer. Enable target health monitoring. Convert the DynamoDB tables to global tables.

Correct Answer: C

Community vote distribution

C (99%)

 **buvumathelegend**  3 months, 1 week ago
itexamslab.com

This Answer is correct
upvoted 46 times

 **folmedispi**  3 months, 3 weeks ago
itexamstest.com

no discussion c :)
upvoted 34 times

 **gofavad926**  3 weeks, 3 days ago
Selected Answer: C

C, failover record, this is the typical failover configuration on route53. Be careful, chatgpt suggests the option B "multivalue answer"
upvoted 1 times

 **MoTOne** 4 weeks ago
Selected Answer: C

Choosing C cause you want the API GW and Lambda functions work as a combination behind the DNS with failover, can think of Route53 here as a CDN provider like Cloudflare
upvoted 1 times

 **atirado** 3 months, 3 weeks ago
Selected Answer: C

Option A - Does not provide a way to fail over to a new region but rather a way for API gateway to respond from the region closest to the client

Option B - Does not provide a way to fail over to a new region because when the main region is healthy name resolution will provide 2 possible regions to connect to

Option C - Provides a way to fail over to a new region through the use of a Route 53 failover record and health monitoring and deployment in another region

Option D - Does not provide a way to fail over to a new region because when the main region is healthy name resolution will provide 2 possible regions to connect to

upvoted 4 times

 **ninomfr64** 4 months ago

Selected Answer: C

Not A. "edge-optimized API endpoint" make use of CloudFront to optimize global each, however API Gateway instance is deployed in a single region thus no ability to fail over to a different AWS Region

Not B. "Route 53 DNS record to a multivalue" implements a active-active scenario, while we are requested to have fail over

Not D. I am not aware of "global function" also "Route 53 DNS record to a multivalue" is not the best fit (see above)

Thus C. is correct has it come with all the required pieces

upvoted 3 times

 **abeb** 4 months, 2 weeks ago

C is correct

upvoted 1 times

 **edder** 4 months, 2 weeks ago

Selected Answer: B

The answer is B.

A: There is no Route 53, so it cannot be switched in the event of a failure.

C: It's good to change to a failover record, but compared to other questions, there is no step to add a DNS record answer, so you can't switch to a new region.

D: The global function is meaningless.

B: A health check is additionally set, and failover is possible because the corresponding records are not returned in the event of a region failure.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-configuring.html>

upvoted 1 times

 **severlight** 5 months ago

Selected Answer: C

failover is required

upvoted 1 times

 **Jean_PA** 6 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 2 times

 **ansgohar** 6 months, 2 weeks ago

Selected Answer: C

C. Deploy a new API Gateway API and Lambda functions in another Region. Change the Route 53 DNS record to a failover record. Enable target health monitoring. Convert the DynamoDB tables to global tables.

upvoted 1 times

 **Simon523** 7 months, 2 weeks ago

Selected Answer: C

<https://thewebspark.com/2020/07/14/handling-multi-region-fail-over-with-amazon-route-53-tutorial/>

upvoted 1 times

 **dimitry_khan_arc** 7 months, 2 weeks ago

Selected Answer: C

C is my choice

upvoted 1 times

 **whenthan** 8 months ago

Selected Answer: C

https://d1.awsstatic.com/events/reinvent/2019/REPEAT_1_Best_practices_for_building_multi-region,_active-active_serverless_applications_SVS337-R1.pdf

upvoted 1 times

 **stevegod0** 8 months, 2 weeks ago

C is correct.

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: C

It's C

upvoted 1 times

 **cheese929** 10 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

Question #3

Topic 1

A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services.

The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization. Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies. Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

- A. Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account.
- B. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the new account to the Production OU when adjustments to AWS Config are complete.
- C. Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporarily apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account.
- D. Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete.

Correct Answer: B*Community vote distribution*

buvumathelegend Highly Voted 3 months, 1 week ago
itexamslab.com

This Answer is correct
upvoted 41 times

Snip Highly Voted 1 year, 4 months ago

Right answer is D.
An SCP at a lower level can't add a permission after it is blocked by an SCP at a higher level. SCPs can only filter; they never add permissions. SO you need to create a new OU for the new account assign an SCP, and move the root SCP to Production OU. Then move the new account to production OU when AWS config is done.
upvoted 39 times

TonytheTiger Most Recent 1 week, 1 day ago

Selected Answer: D
Option D: The link doesn't give you a full explanation on why "D" is correct however it does check all the boxes

<https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/transitional-ou.html>
upvoted 1 times

Dgix 1 month, 1 week ago

This question is ambiguous. If D was formulated like this:

"D. Create a temporary OU named Onboarding for the new account. Apply a Config non-blocking SCP to the Onboarding OU to allow AWS Config actions. Apply the organization's root SCP to the Production OU instead of to the root OU. Move the new account to the Production OU when adjustments to AWS Config are complete."

Then D would be a viable option. However, it isn't, and even if it were, it fails to mention the crucial fact that the Root OU always must have an SCP, which in this case must Allow everything. For someone with some experience this is a given, but as it isn't mentioned, I'd go for B.

However, AWS should reformulate the question and the answers. They are really subpar.
upvoted 2 times

JOKERO 1 month ago

AWS Config will still be restricted despite the Allow SCP in Onboarding because of the Deny SCP in the root of the organization
upvoted 1 times

awsylum 1 month, 2 weeks ago

I don't like any of the answers to be honest. Let's look at D since that's the one most people think is right. The problem with D is that you can't detach the last SCP associated with a root container, OU, or account. There has to be at least one. So, removing the SCP from the root and moving it down to the Production OU is a no-go unless you add a permissible SCP to the root. Check the section on detaching here:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_attach.html

The only way B is correct is if the reason the new admins don't have access to Config is not because Config is in the Deny List, but because the

management account doesn't have the appropriate IAM Policy giving PERMISSION to Config. You need both an IAM Policy and a permissible SCP to have permission and access to a service. But, why wasn't IAM Policy mentioned in choice B. Clearly, without that information, choice B also is not right.

upvoted 1 times

 **awsylum** 1 month, 2 weeks ago

Also, even if you could remove a root SCP, you would never do that in production. You would never just flat remove an SCP with a Deny list just to give one account access to some service. Even if it's temporary, that's a fatal mistake as the other accounts will not be restricted from certain services they shouldn't have access to.

upvoted 1 times

 **awsylum** 1 month, 2 weeks ago

The question mentioned a Deny List architecture, but it didn't specifically say Config was in the Deny List. We are assuming that, which could lead to the wrong answer. Unfortunately, I'm not satisfied with any of the answers. Hopefully, this is a question that would be thrown out from the exam. LOL.

upvoted 1 times

 **DmitriKonnovNN** 2 months, 1 week ago

The question itself is a bit confusing. It says "Deny List in the root", which should be understood as Deny List Architecture, but can be misinterpreted as "Allow List Architecture with attached Deny List in the root that explicitly deny AWS Config". Since AWS Config on Production OU is denied, an appropriate SCP is attached to it, which explicitly denies AWS Config. Thus, the root has FullAWSAccess SCP attached to it. That's why we just need to create Onboarding OU with no explicit deny of AWS Config and that's it. So the correct answer is truly correct, but the question is a bit tricky and easy to misunderstand.

upvoted 1 times

 **kobi44** 2 months, 2 weeks ago

option D - how creating new OU will solve the problem? the root SCP will deny it , isn't?
also why do we need to Move the organization's root SCP to the Production OU ?

upvoted 1 times

 **GabrielShiao** 3 months, 1 week ago

Answer D is the answer most accurate. it would be good that add another statement to say" Add awsFullAccess SCP policy on the root and move the deny list scp policy from root to production OU"

upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: C

Option A - This option actually rolls out AWS Config across the company which is exactly the opposite of what they are doing

Option B - This option does not work because AWS Config will still be restricted despite the Allow SCP in Onboarding because of the Deny SCP in the root of the organization

Option C - This option allows access to AWS Config in the new business unit and restricts access to everything else. However, the SCP will require regular updates to add new AWS services

Option D - This option applies the correct level of access to each OU without needing updates: Onboarding gets access to AWS Config, Production does not and FullAWSAccess is established at the root after the company's Deny SCP is moved.

upvoted 1 times

 **folmedispi** 3 months, 3 weeks ago

itexamstest.com

no discussion D :)

upvoted 34 times

 **cgsoft** 3 months, 4 weeks ago

Selected Answer: D

SCP at root must be moved to Production OU to prevent it from being applied to onboarded account.

upvoted 1 times

 **ninomfr64** 4 months ago

Selected Answer: D

This was not easy for me due to wording, however here is my take:

Not A. here we permanently remove SCPs that limit access to AWS Config, while we are requested to continue to enforce the current policies
Not B. temporary OU and related SCP that allows AWS Config are nested under root where SCPs that limit access to AWS Config are applied. As SCP can only remove permission and not add, this will not work

Not C. converting deny list into allow list here is not beneficial also temporarily apply SCP allowing AWS Config does not meet the request to avoid additional long-term maintenance.

Thus D does the job.

upvoted 1 times

 **abeb** 4 months, 2 weeks ago

D is correct

upvoted 1 times

 **swadeey** 4 months, 2 weeks ago

The Root is not an OU. It is a container for the management account, and for all OUs and accounts in your organization. Conceptually, the Root contains all of the OUs. It cannot be deleted. You cannot govern enrolled accounts at the Root level within AWS Control Tower. Instead, govern enrolled accounts within your OUs. The SCP don't apply at root OU. This will impact production as when you move SCP from root to Production you are changing SCP for all OU which are part of it. Will customer allow to change existing production SCP to on board a new. I don't think D is correct

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

B is horribly wrong. Correct answer must be D.

upvoted 1 times

 **severlight** 5 months ago

Selected Answer: D

need to get rid of deny in root scp

upvoted 2 times

 **Sandeep_B** 5 months, 2 weeks ago

Option D looks to be correct answer. Can anyone please confirm if you have got this question in the exam and cleared it..

upvoted 2 times

Question #4

Topic 1

A company is running a two-tier web-based application in an on-premises data center. The application layer consists of a single server running a stateful application. The application connects to a PostgreSQL database running on a separate server. The application's user base is expected to grow significantly, so the company is migrating the application and database to AWS. The solution will use Amazon Aurora PostgreSQL, Amazon EC2 Auto Scaling, and Elastic Load Balancing.

Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

- A. Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.
- B. Enable Aurora Auto Scaling for Aurora writers. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.
- C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky sessions enabled.
- D. Enable Aurora Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled.

Correct Answer: C

Community vote distribution



folmedispi 3 months, 3 weeks ago

itexamstest.com

no discussion c :)

upvoted 34 times

buvumathelegend 3 months, 1 week ago

itexamslab.com

This Answer is correct

upvoted 29 times

gofavad926 3 weeks, 3 days ago

Selected Answer: C

C, Enable Aurora Auto Scaling for Aurora Replicas

upvoted 1 times

MoTOne 4 weeks ago

Selected Answer: C

Single writer: In an Aurora PostgreSQL DB cluster, there is only one writer instance at a time. All write operations, such as INSERT, UPDATE, and DELETE statements, are directed to the writer instance.

upvoted 3 times

GNB2024 1 month, 3 weeks ago

Selected Answer: C

It's C

upvoted 1 times

liux99 3 months, 1 week ago

B, D are distractor, as there is no writer replica in aurora autoscale.

NLB does not support sticky session so A is out. The answer is C.

upvoted 1 times

rhinozD 1 month, 3 weeks ago

NLB Sticky Session: <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#sticky-sessions>

upvoted 1 times

atirado 3 months, 3 weeks ago

Selected Answer: C

Option A - Allows the tiers to grow but NLB does not make load balancing decisions that way

Option B - No such thing as Aurora Autoscaling for Aurora Writers

Option C - Allows the tiers to grow and ALB using sticky sessions provides consistent user experience

Option D - No such thing as Aurora Autoscaling for Aurora Writers

Note: The application is web-based so choosing ALB shouldn't be an issue.

upvoted 3 times

✉ **ninomfr64** 4 months ago

Selected Answer: C

- Auto Scaling for Aurora writers does not exists (distractor)
- NLB does not support least outstanding requests routing algorithm (it only supports Flow Hash)
- NLB does not allow to enable Sticky Sessions, this is always enabled with Flow Hash where each TCP/UDP connection is routed to a single target for the life of the connection

Thus C is correct

upvoted 2 times

✉ **abeb** 4 months, 2 weeks ago

C Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky session

upvoted 1 times

✉ **severlight** 5 months ago

Selected Answer: C

Aurora - AS only for read replicas. NLB doesn't support the least outstanding requests or round-robin algorithms, only flow hash is supported.

upvoted 1 times

✉ **ansgohar** 6 months, 2 weeks ago

Selected Answer: C

C. Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the round robin routing and sticky sessions enabled.

upvoted 1 times

✉ **rsn** 7 months ago

Selected Answer: A

NLB scales better than ALB. Also least outstanding requests algorithm works better than round robin algorithm. Any thoughts?

upvoted 2 times

✉ **Ganshank** 7 months ago

The correct answer is whatever the examiner says it is. Depending on how you look at it either A or C can be the correct answer.

NLB scales better and supports LOR algorithm which are both factors in its favor, however stickiness is not supported for TLS connections in NLBs. While this has not been called out explicitly, I doubt anyone in today's world would support non-TLS connections to their applications. If that turns out to be a dealbreaker, then the only option is C, to use ALB, however round-robin doesn't guarantee the best performance especially where stickiness is concerned.

Your call.

upvoted 3 times

✉ **dimitry_khan_arc** 7 months, 2 weeks ago

Selected Answer: C

write replica is distractor. NLB does not support round robin

upvoted 2 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: C

it's C

upvoted 1 times

✉ **ptpho** 10 months, 1 week ago

It's C

No idea about NLB.

Aurora Scaling -> Auto Scaling for Aurora Replicas (writer just in Primary)

upvoted 1 times

✉ **Limlimwdwd** 11 months ago

Selected Answer: C

Aurora Replicas and ALB will meet the purpose

upvoted 1 times

✉ **EthicalBond** 11 months, 3 weeks ago

Selected Answer: C

Read Replicas

ALB with sticky sessions (due to stateful application)

upvoted 2 times

Question #5

Topic 1

A company uses a service to collect metadata from applications that the company hosts on premises. Consumer devices such as TVs and internet radios access the applications. Many older devices do not support certain HTTP headers and exhibit errors when these headers are present in responses. The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers.

The company wants to migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices. The company has already migrated the applications into a set of AWS Lambda functions.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header.
- B. Create an Amazon API Gateway REST API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Modify the default gateway responses to remove the problematic headers based on the value of the User-Agent header.
- C. Create an Amazon API Gateway HTTP API for the metadata service. Configure API Gateway to invoke the correct Lambda function for each type of request. Create a response mapping template to remove the problematic headers based on the value of the User-Agent. Associate the response data mapping with the HTTP API.
- D. Create an Amazon CloudFront distribution for the metadata service. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB. Configure the ALB to invoke the correct Lambda function for each type of request. Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of the User-Agent header.

Correct Answer: B

Community vote distribution



✉ **EricZhang** 1 year, 3 months ago

A. The only difference between A and D is CloudFront function vs Lambda@Edge. In this case the CloudFront function can remove the response header based on request header and much faster/light-weight.

upvoted 54 times

✉ **vn_thanhung** 7 months, 3 weeks ago

After read, answer A "Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header" not really clear and fuzzy, "The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices" => "Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of the User-Agent header" => D make sense

upvoted 6 times

✉ **folmedispi** 3 months, 3 weeks ago

Selected Answer: A

itexamstest.com

no dissucusion A :)

upvoted 35 times

✉ **Weninka** 1 week, 1 day ago

Selected Answer: D

CloudFront functions can't be triggered in to run on the response from the origin (in this case to modify the response returned by the Lambda functions), so looks like it's D.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions-choosing.html>

upvoted 1 times

✉ **4555894** 2 weeks ago

Selected Answer: D

The other options have drawbacks:

A. CloudFront function is not available: CloudFront functions are not a supported feature.

B & C. API Gateway modification: These options require modifying responses at the API Gateway level. While achievable, they wouldn't process requests based on User-Agent headers before reaching the origin, potentially causing errors on older devices.

By utilizing Lambda@Edge, the company can:

Maintain a serverless architecture with Lambda functions for core logic.

Filter out unsupported headers close to the user, preventing errors on older devices.

Leverage CloudFront's caching and edge locations for improved performance.

upvoted 1 times

✉ **gofavad926** 3 weeks, 3 days ago

Selected Answer: A

A, you can do it with cloudfront functions or lambda@edge, but cloudfront functions is faster and cheaper...

upvoted 1 times

✉ **Dgix** 3 weeks, 3 days ago

Selected Answer: A

On second thought, A.

upvoted 1 times

✉ **Dgix** 3 weeks, 3 days ago

Selected Answer: D

CloudFront functions are not for this type of use case. Therefore, D.

upvoted 1 times

✉ **MoTOne** 4 weeks ago

Selected Answer: B

In AWS API Gateway, a response mapping template is used to transform the output received from the backend integration into a format that is suitable for the API client. It allows you to customize the structure and content of the response before it is sent back to the client.

upvoted 1 times

✉ **tushar321** 1 month ago

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions-choosing.html#:~:text=CloudFront%20Functions%20is,to%20every%20request>.

upvoted 1 times

✉ **titi_r** 1 month, 1 week ago

Selected Answer: A

Answer is A.

CloudFront Functions is ideal for lightweight, short-running functions for use cases like the following:

Header manipulation – You can insert, modify, or delete HTTP headers in the request or response. For example, you can add a True-Client-IP header to every request.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions-choosing.html>

upvoted 1 times

✉ **24Gel** 1 month, 1 week ago

For A and C,

I didn't see any point to use ALB here, the purpose is to remove headers, not increase performance.

upvoted 1 times

✉ **awsylum** 1 month, 2 weeks ago

The answer could be B or C. The main thing is the solution should be serverless, so that rules out ALB and CloudFront even though both integrate with serverless components. But, using either of them doesn't make it an entirely serverless architecture. The issue I have with the selected answer is that Parameter Mapping can be utilized in API Gateway to remove specific headers with HTTP APIs. I believe REST APIs are a superset which are more powerful, but if HTTP APIs can do the same job cheaper, then why not use HTTP APIs and select C? See this documentation for confirmation: <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-parameter-mapping.html>

upvoted 3 times

✉ **awsylum** 1 month, 2 weeks ago

Actually, the more I read about it, the more it seems that the parameter mapping is only for HTTP API. That would make C the answer. These questions and answers make things even more confusing because you're not sure whether to trust the selected answers here.

upvoted 2 times

✉ **24Gel** 1 month, 1 week ago

Agree, that is my choice too

upvoted 1 times

✉ **rhinozD** 1 month, 3 weeks ago

Selected Answer: C

You guys are discussing CloudFront function and Lambda@Edge but the question says: "adopt serverless technologies". ALB is not a serverless service.

I think C is the correct answer.

upvoted 4 times

✉ **GNB2024** 1 month, 3 weeks ago

Selected Answer: A

I agree with A

upvoted 1 times

✉ **Rajarshi** 2 months ago

Ans D because Cloudfront Function can not modify headers

upvoted 1 times

✉ **hogtrough** 1 month, 3 weeks ago

"CloudFront can remove headers that it received from the origin, or add headers to the response, before sending the response to viewers."

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/modifying-response-headers.html>

upvoted 1 times

✉ **rhinozD** 1 month, 3 weeks ago

Actually, It can

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions-choosing.html>

upvoted 2 times

✉ **SwapnilAWS** 2 months ago

option A : <https://dev.to/aws-heroes/cloudfront-functions-vs-lambdaedge-whats-the-difference-1g60#:~:text=Scale%3A%20CloudFront%20Functions%20can%20scale,128MB%20%2D%203GB%20of%20memory%20available.>

upvoted 1 times

✉ **master9** 2 months, 2 weeks ago

Selected Answer: A

To migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices, the company can use AWS Application Load Balancer (ALB). The ALB is a serverless technology that can be used to route incoming traffic to serverless functions such as AWS Lambda. The Serverless Framework makes it possible to set up the connection between Application Load Balancers and Lambda functions with the help of the alb event.

To support the older devices, the company can configure the ALB to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers. The ALB's focus on HTTP allows it to use parts of the protocol to make decisions about caching and save you some Lambda executions.

upvoted 1 times

Question #6

Topic 1

A retail company needs to provide a series of data files to another company, which is its business partner. These files are saved in an Amazon S3 bucket under Account A, which belongs to the retail company. The business partner company wants one of its IAM users, User_DataProcessor, to access the files from its own AWS account (Account B).

Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Choose two.)

A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A.

B. In Account A, set the S3 bucket policy to the following:

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": "arn:aws:s3:::AccountABucketName/*"  
}
```

C. In Account A, set the S3 bucket policy to the following:

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": [  
        "arn:aws:s3:::AccountABucketName/*"  
    ]  
}
```

D. In Account B, set the permissions of User_DataProcessor to the following:

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": "arn:aws:s3:::AccountABucketName/*"  
}
```

E. In Account B, set the permissions of User_DataProcessor to the following:

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"  
    },  
    "Action": [  
        "s3:GetObject",  
        "s3>ListBucket"  
    ],  
    "Resource": [  
        "arn:aws:s3:::AccountABucketName/*"  
    ]  
}
```

Correct Answer: D

Community vote distribution

C (64%)

D (33%)

 **robertohyena**  1 year, 4 months ago

Answer: C & D

Source:

<https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example4.html>

upvoted 27 times

✉ **higashikumi**  1 year, 1 month ago

C & D

To allow User_DataProcessor to access the S3 bucket from Account B, the following steps need to be taken:

In Account A, set the S3 bucket policy to allow access to the bucket from the IAM user in Account B. This is done by adding a statement to the bucket policy that allows the IAM user in Account B to perform the necessary actions (GetObject and ListBucket) on the bucket and its contents.

In Account B, create an IAM policy that allows the IAM user (User_DataProcessor) to perform the necessary actions (GetObject and ListBucket) on the S3 bucket and its contents. The policy should reference the ARN of the S3 bucket and the actions that the user is allowed to perform.

Note: turning on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account A is not necessary for this scenario as it is typically used for allowing web browsers to access resources from different domains.

upvoted 16 times

✉ **MoTOne**  4 weeks ago

Selected Answer: C

Cross-Origin Resource Sharing (CORS) is a security feature in Amazon S3 that allows you to control access to your S3 resources from a different domain (origin) than the one serving the resources. CORS defines a way for client web applications running in one origin to interact with resources in a different origin, which is otherwise restricted by the same-origin policy enforced by web browsers.

upvoted 1 times

✉ **Dgix** 1 month, 1 week ago

C and D.

upvoted 1 times

✉ **awsylum** 1 month, 2 weeks ago

The answer is C and D. You need to give the IAM User in Account B an IAM Policy and you need to give a Bucket Policy in Account A.

Who is maintaining this database of questions? Someone needs to seriously set the correct answers before making a lot of people confused and potentially screw up their exam.

upvoted 1 times

✉ **chelbsik** 2 months ago

Selected Answer: D

Correct answer: C and D

Adding my vote for D to balance the result

Moderator, please fix the vote in this ticket.

upvoted 1 times

✉ **ftaws** 2 months, 1 week ago

why we need two steps? I think that we get only one from resource-based policy or identity-based policy.

upvoted 1 times

✉ **Vaibs099** 2 months, 2 weeks ago

Answer C & D

upvoted 1 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: C

Option A - CORS does not address cross-account access to S3 buckets

Option B - This option would not work because the bucket policy is missing the Principal

Option C - This option provides a valid S3 bucket policy that grants access to User_DataProcessor

Option D - These permissions allow User_DataProcessor to get objects out of the bucket

Option E - This option would not work because it is not a valid IAM policy

upvoted 1 times

✉ **shaaam80** 4 months, 1 week ago

Selected Answer: C

Answer - C & D

upvoted 2 times

✉ **severlight** 5 months ago

Selected Answer: D

C, D, D and not E, because it is an identity-based inline policy already attached to the specific principal.

upvoted 4 times

✉ **alonis2201** 5 months ago

A,C

Access setting need to be done only on Account A as it's an owner. So Enabling Cross origin access and access to the bucket for account B IAM user.

upvoted 2 times

✉ **rif** 5 months, 3 weeks ago

Answer : C&D.

upvoted 2 times

✉ **puffetor** 6 months, 1 week ago

Hello I've just tested it on my AWS account to be 100% sure.

Correct answer in C & D. Only C is enough only for same account access, but for cross-account like in this case D is needed too, otherwise it does not work.

upvoted 3 times

✉ **ansgohar** 6 months, 2 weeks ago

Selected Answer: C

Answer: C

upvoted 2 times

✉ **career360guru** 7 months, 1 week ago

A & C are the right answer

upvoted 3 times

✉ **[Removed]** 8 months, 3 weeks ago

C & D: first allow the b account user to get access to the bucket objects and list. then on the b account give the user the permissions to do that

upvoted 2 times

Question #7

Topic 1

A company is running a traditional web application on Amazon EC2 instances. The company needs to refactor the application as microservices that run on containers. Separate versions of the application exist in two distinct environments: production and testing. Load for the application is variable, but the minimum load and the maximum load are known. A solutions architect needs to design the updated application with a serverless architecture that minimizes operational complexity.

Which solution will meet these requirements MOST cost-effectively?

- A. Upload the container images to AWS Lambda as functions. Configure a concurrency limit for the associated Lambda functions to handle the expected peak load. Configure two separate Lambda integrations within Amazon API Gateway: one for production and one for testing.
- B. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.
- C. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Kubernetes Service (Amazon EKS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the EKS clusters.
- D. Upload the container images to AWS Elastic Beanstalk. In Elastic Beanstalk, create separate environments and deployments for production and testing. Configure two separate Application Load Balancers to direct traffic to the Elastic Beanstalk deployments.

Correct Answer: B

Community vote distribution

B (84%)

Other

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load. Deploy tasks from the ECR images. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.

This option meets the requirement of using a serverless architecture by utilizing the Fargate launch type for the ECS clusters, which allows for automatic scaling of the containers based on the expected load. It also allows for separate deployments for production and testing by configuring separate ECS clusters and Application Load Balancers for each environment. This option also minimizes operational complexity by utilizing ECS and Fargate for the container orchestration and scaling.

upvoted 18 times

 **zhangyu20000** Highly Voted 1 year, 4 months ago

Answer is A. ABC all works but A is most COST EFFECTIVE

upvoted 12 times

 **masetromain** 1 year, 3 months ago

Is true but " you can now package and deploy Lambda functions as container images of up to 10 GB in size." the size is not specified, personally I find it too small

upvoted 3 times

 **anita_student** 1 year, 1 month ago

10GB image is too small for what? I'm curious how do you containerise those images?

I'd say the average image size is ~300-400MB

upvoted 3 times

 **zhangyu20000** 1 year, 4 months ago

<https://aws.amazon.com/blogs/aws/new-for-aws-lambda-container-image-support/>

upvoted 3 times

 **anita_student** 1 year, 1 month ago

Yes, would be cheap, but can't run a web app from Lambda

upvoted 5 times

 **yuyuyuyuyu** 1 year, 3 months ago

I do not think A is the right answer.

Because image must be upload to the ECR.

upvoted 3 times

 **TonytheTiger** Most Recent 1 week, 4 days ago

Selected Answer: B

Option B and NOT Option C: I wasn't able to find a good comparison btw AWS ECS vs AWS EKS pricing in AWS documentation however I found a few articles saying that AWS EKS has additional cost for using EKS control plane. I will leave it up to you to decide.

<https://www.densify.com/eks-best-practices/aws-ecs-vs-eks/>

upvoted 1 times

✉ **MoTOne** 4 weeks ago

AWS Elastic Beanstalk is not considered a serverless architecture. While it abstracts away some of the underlying infrastructure management, it still involves running and managing EC2 instances, which are virtual servers.

upvoted 1 times

✉ **_Jassybanga_** 2 months ago

D - because BCD are right solution , D because - beanstalk runs ECS in backend + Reduce operation complexity which is asked in the question

upvoted 1 times

✉ **liux99** 3 months, 1 week ago

The confusion here is choice between B and C. Both ECS and EKS are container orchestration service which supports fargate. But ECS is aws fully managed, better suited for simple application and also more cost effective.

upvoted 1 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This option might not work. AWS Lambda provides a cheap option to run containers however nothing is said about execution times could be a concern, i.e. AWS Lambda only provides 15 minutes of execution time

Option B - This option will work. ALB, ECR, ECS and Fargate in combination will deliver a running solution.

Option C - This option will work. ALB, ECR, EKS and Fargate will deliver a running solution.

Option D - This option will work: Beanstalk will rely on ECS to run the containers. See

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_ecs.html

Cheapest option is B.

upvoted 2 times

✉ **ninomfr64** 4 months ago

Selected Answer: B

Not A. as Lambda is not good for running a "traditional web application", also you can use container with Lambda but ECS is "ideal for organizations that want a simple and cost-effective way to deploy and manage containerized applications"

Not C. as there is o pointer to EKS (e.g. open-source, industry standard, etc.) and also ECS is "ideal for organizations that want a simple and cost-effective way to deploy and manage containerized applications"

Not D. as Beanstalk is not serverless

Hence B.

upvoted 1 times

✉ **severlight** 5 months ago

Selected Answer: B

B. Not D as Beanstalk isn't serverless. Not C because there are no pointers to use EKS. Not A, because microservices are requested.

upvoted 1 times

✉ **hui521** 6 months, 1 week ago

anyone helps to explain why D is not correct?

upvoted 1 times

✉ **Chainshark** 6 months ago

Beanstalk is a PaaS, it isn't truly serverless.

upvoted 1 times

✉ **ansgohar** 6 months, 2 weeks ago

Selected Answer: B

B. Image on ECR and ECS cost effective over EKS.

upvoted 2 times

✉ **task_7** 6 months, 4 weeks ago

Selected Answer: D

I would go with d
a serverless architecture that minimizes operational complexity.

upvoted 2 times

✉ **cheese929** 7 months ago

Selected Answer: B

B is correct.

upvoted 1 times

career360guru 7 months, 1 week ago

B is right option.

A is possible but Lambda container images has 10GB size limitation and requires you to keep updating these container images as customer refactors the code. I feel A will have higher operational overhead. B is best option that will be most cost effective and operationally efficient.

upvoted 1 times

dimitry_khan_arc 7 months, 2 weeks ago

Selected Answer: B

B. Image on ECR and ECS cost effective over EKS.

upvoted 1 times

asim_rasheed 7 months, 3 weeks ago

Guys please dont put any damn answer which you think, this is community effort and with your answer which does not make any sense(if thrown without logic and reading), it will confuse others and present you like stupid. So contribute if you really want to else move on without making this forum dirty

upvoted 5 times

jahmad0730 5 months, 3 weeks ago

You're a dirty dog.

upvoted 2 times

Shijokingo 8 months, 2 weeks ago

B seems right. https://docs.aws.amazon.com/AmazonECS/latest/developerguide/launch_types.html

C seems distractor as there is no option as Amazon EKS with Fargate Launch type.

upvoted 2 times

aviathor 7 months, 1 week ago

You can indeed use FarGate with EKS...

<https://docs.aws.amazon.com/eks/latest/userguide/fargate.html>

upvoted 1 times

Question #8

Topic 1

A company has a multi-tier web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB and the Auto Scaling group are replicated in a backup AWS Region. The minimum value and the maximum value for the Auto Scaling group are set to zero. An Amazon RDS Multi-AZ DB instance stores the application's data. The DB instance has a read replica in the backup Region. The application presents an endpoint to end users by using an Amazon Route 53 record.

The company needs to reduce its RTO to less than 15 minutes by giving the application the ability to automatically fail over to the backup Region. The company does not have a large enough budget for an active-active strategy.

What should a solutions architect recommend to meet these requirements?

- A. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the HTTPCode_Target_5XX_Count metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.
- B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.
- C. Configure the Auto Scaling group in the backup Region to have the same values as the Auto Scaling group in the primary Region. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs. Remove the read replica. Replace the read replica with a standalone RDS DB instance. Configure Cross-Region Replication between the RDS DB instances by using snapshots and Amazon S3.
- D. Configure an endpoint in AWS Global Accelerator with the two ALBs as equal weighted targets. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Create an Amazon CloudWatch alarm that is based on the HTTPCode_Target_5XX_Count metric for the ALB in the primary Region. Configure the CloudWatch alarm to invoke the Lambda function.

Correct Answer: B

Community vote distribution



B (100%)

✉  **masetromain**  1 year, 4 months ago

Selected Answer: B

I go with B

https://docs.amazonaws.cn/en_us/Route53/latest/DeveloperGuide/welcome-health-checks.html

upvoted 18 times

✉  **masetromain** 1 year, 2 months ago

B is correct, because it meets the company's requirements for reducing RTO to less than 15 minutes and not having a large budget for an active-active strategy.

In this solution, the company creates an AWS Lambda function in the backup region which promotes the read replica and modifies the Auto Scaling group values. Route 53 is configured with a health check that monitors the web application and sends an Amazon SNS notification to the Lambda function when the health check status is unhealthy. The Route 53 record is also updated with a failover policy that routes traffic to the ALB in the backup region when a health check failure occurs. This way, when the primary region goes down, the failover policy triggers and traffic is directed to the backup region, ensuring a quick recovery time.

upvoted 13 times

✉  **gofavad926**  3 weeks, 3 days ago

Selected Answer: B

B for sure

upvoted 1 times

✉  **Vaibs099** 2 months, 2 weeks ago

This explains Lambda promoting backup read replica in other region - <https://medium.com/ankercloud-engineering/aws-lambda-promoting-rds-read-replica-on-cross-region-using-aws-lambda-113db758869>

upvoted 1 times

✉  **ftaws** 2 months, 3 weeks ago

why we need Lambda Function ? Is it enough a Route 53 failover policy ?

upvoted 1 times

✉  **rhinozD** 1 month, 3 weeks ago

What about RDS failover?

You need lambda to promote read replica.

upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This option will not work as needed: The client will get errors when the closest region is the application's backup region

Option B - This option implements an active-passive strategy as needed: When the health check fails, Route 53 will resolve to the backup region and the Lambda function will ensure the backup region has resources to function

Option C - This option implements an active-active strategy

Option D - This option will not work as needed: The client will get errors 50% of the time

upvoted 2 times

 **ninomfr64** 4 months ago

Selected Answer: B

The problem is not detecting the right answer, but reading quickly enough through all the words in the question!

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

Selected Answer: B

B satisfies all the requirements.

upvoted 1 times

 **severlight** 5 months ago

Selected Answer: B

Health check is a metric, hence alarms can be executed, and alarms are integrated with SNS, SNS integrated with lambda. This sounds weird, but it will work.

upvoted 1 times

 **ansgohar** 6 months, 2 weeks ago

Selected Answer: B

B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group values. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.

upvoted 2 times

 **dimitry_khan_arc** 7 months, 2 weeks ago

Selected Answer: B

Health check+SNS. This does not need to have active-active which satisfy the requirement.

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

it's a B again

upvoted 1 times

 **Parimal1983** 9 months, 2 weeks ago

Selected Answer: B

As company can not afford with active active configuration and with lambda data layer can be promoted to primary

upvoted 1 times

 **SkyZeroZx** 10 months ago

Selected Answer: B

SNS + Health check

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

SNS + Health check

upvoted 1 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

upvoted 1 times

 **higashikumi** 1 year, 1 month ago

The best option to meet the requirements and reduce RTO to less than 15 minutes is to choose option B.

Option B involves creating an AWS Lambda function in the backup region to promote the read replica and modify the Auto Scaling group values.

Additionally, Route 53 can be configured with a health check that monitors the web application and sends an Amazon SNS notification to the Lambda function when the health check status is unhealthy. The application's Route 53 record can be updated with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.

This option is cost-effective as it does not require an active-active strategy, and it uses AWS services to minimize the RTO. The Lambda function can be invoked to promote the read replica in the backup region, and the Auto Scaling group values can be updated to launch EC2 instances in the backup region. Furthermore, the Route 53 health check feature can be used to monitor the web application and initiate the failover process.

upvoted 1 times

✉ **Sarutobi** 1 year, 1 month ago

Selected Answer: B

It would be interesting to see if this actually works. SNS is a regional service, in the last outage of the Virginia Region, we lost SNS completely.

upvoted 2 times

✉ **frfavoreto** 1 year ago

The SNS topic is in the backup region, not the primary. If you have an issue with the backup region at the same time there is not much you can do as your entire architecture is affected.

upvoted 2 times

✉ **Sarutobi** 12 months ago

That is a good point, but how do you need to do some health-API integration? How does SNS in one region know about failure in another? What if your application was not a complete regional outage, or only a service in that region failed? I know this is no longer the initial question :).

upvoted 1 times

✉ **frfavoreto** 6 months, 3 weeks ago

First of all, SNS in one region doesn't need to know anything about the other region. In the backup region, SNS receives a message from Route53 that triggers a Lambda Function, this is simple as that.

Secondly, you need to implement proper health checks in your frontend web server in order to return a 5xx or 4xx error codes to the probes coming from Route53. If anything is wrong (database, high latency or even the web server itself), Route53 notices the error code/timeout and immediately triggers the failover solution with SNS messaging. Route53 doesn't need to care about what exactly went wrong, just by receiving any unexpected results from the health checks it triggers the failover region.

upvoted 1 times

Question #9

Topic 1

A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.

A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.

Which combination of steps will meet these requirements? (Choose three.)

- A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
- B. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.
- C. Modify the DB instance to create a read replica in the same Availability Zone. Promote the read replica to be the primary DB instance in failure scenarios.
- D. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
- E. Create a replication group for the ElastiCache for Redis cluster. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
- F. Create a replication group for the ElastiCache for Redis cluster. Enable Multi-AZ on the cluster.

Correct Answer: ADF

Community vote distribution

ADF (97%)



✉️  **masetromain**  1 year, 4 months ago

Selected Answer: ADF

I go with ADF
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>
 upvoted 14 times

✉️  **spencer_sharp** 1 year, 3 months ago

Why C is wrong?
 upvoted 2 times

✉️  **Karamen** 8 months, 1 week ago

let suppose in case one of used AZ is failed?
 upvoted 1 times

✉️  **masetromain** 1 year, 2 months ago

Other options like B. and C. does not meet the requirement because the instances are configured in unlimited mode, it will not be possible to ensure that there is always at least one healthy instance to handle traffic if there is a failure.
 upvoted 1 times

✉️  **God_Is_Love** 1 year, 1 month ago

Issue with C - Read replica in the same AZ does not sound High availability
 upvoted 6 times

✉️  **dtha1002** 10 months, 2 weeks ago

in question "can automatically recover from failure with the least possible downtime"
 C is correct but D is least possible downtime
 upvoted 1 times

✉️  **masetromain** 1 year, 2 months ago

A. Using an Elastic Load Balancer (ELB) to distribute traffic across multiple EC2 instances can help ensure that the application remains available in the event that one of the instances becomes unavailable. By configuring the instances as part of an Auto Scaling group with a minimum capacity of two instances, you can ensure that there is always at least one healthy instance to handle traffic.

D. Modifying the DB instance to create a Multi-AZ deployment that extends across two availability zones can help ensure that the database remains available in the event of a failure. In the event of a failure, traffic will automatically be directed to the secondary availability zone, reducing the amount of downtime.

F. Creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ can help ensure that the in-memory data store remains available in the event of a failure. This will allow traffic to be automatically directed to the secondary availability zone, reducing the amount of downtime.

upvoted 11 times

✉ **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: ADF

ADF, as mentioned in the other comments

upvoted 1 times

✉ **DmitriKonnovNN** 2 months, 1 week ago

"The infrastructure can automatically recover from failure with the least possible downtime", to me this sounds rather resilient than highly-available, since it focuses on MTTR but not explicitly on up-time.

upvoted 1 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: ADF

Option A - Ensures there is always at least a healthy instance responding to requests. Nothing is said about whether the Auto Scaling Group includes multiple AZs (but it must)

Option B - No such thing as EC2 Unlimited Mode

Option C - Does not provide a place to fail over to

Option D - Provides a place to fail over to

Option E - Does not provide a place to fail over to

Option F - Provides a place to fail over to

Choose A, D, F

upvoted 1 times

✉ **severlight** 5 months ago

Selected Answer: ADF

obvious

upvoted 1 times

✉ **ansgohar** 6 months, 2 weeks ago

Selected Answer: ADF

A, D, F

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: ADF

it's of course ADF

upvoted 1 times

✉ **Parimal1983** 9 months, 2 weeks ago

Selected Answer: ADF

For high availability, need to spin up instances in another zone with auto scaling and multi AZ options

upvoted 1 times

✉ **rtguru** 10 months, 3 weeks ago

ADF will meet the described provisions

upvoted 1 times

✉ **RunkieMax** 11 months ago

Selected Answer: ADF

Fit the best the question

upvoted 1 times

✉ **Maja1** 11 months, 2 weeks ago

Selected Answer: ADF

I wasn't sure if E or F was correct until I read this:

"This replacement results in some downtime for the cluster, but if Multi-AZ is enabled, the downtime is minimized. The role of primary node will automatically fail over to one of the read replicas. There is no need to create and provision a new primary node, because ElastiCache will handle this transparently. This failover and replica promotion ensure that you can resume writing to the new primary as soon as promotion is complete." <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>

upvoted 4 times

✉ **dev112233xx** 1 year ago

Selected Answer: ADF

ADF the correct answers ✓

upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: ADF

ADF is the best fit.

upvoted 1 times

✉  **gameoflove** 1 year ago

Selected Answer: ADF

I believe, This is correct approach <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>

upvoted 1 times

✉  **vherman** 1 year, 1 month ago

Selected Answer: ADF

adf correct

upvoted 1 times

✉  **spd** 1 year, 1 month ago

Selected Answer: ADE

Selecting E because - "Multi-AZ is enabled by default on Redis (cluster mode enabled) clusters" as per <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>

upvoted 1 times

✉  **higashikumi** 1 year, 1 month ago

Option B is incorrect because unlimited mode is a configuration option for an Auto Scaling group that is used to handle bursty workloads, and it does not provide any additional availability benefits.

Option C is incorrect because creating a read replica in the same Availability Zone does not provide any additional availability benefits, and it would not be able to take over in the event of a failure of the primary instance.

Option F is incorrect because Multi-AZ is not an option for ElastiCache for Redis clusters.

upvoted 1 times

✉  **frfavoreto** 1 year ago

ElastiCache for Redis does support Multi-AZ:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoFailover.html>

Option 'F' is correct.

upvoted 2 times

Question #10

Topic 1

A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones.

After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs.

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors.

Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

- A. Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.
- B. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- C. Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- E. Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

Correct Answer: CE*Community vote distribution*

Raj40 Highly Voted 1 year, 3 months ago

A & E

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponsePages.html#custom-error-pages-procedure>

upvoted 29 times

kz407 Most Recent 3 weeks, 4 days ago

Selected Answer: AE

The only problem with E is that it says "Modify DNS records to point to a publicly accessible web page" at the end. It doesn't make sense to begin with. And configuring custom error responses in CF has nothing to do with DNS anyway.

upvoted 1 times

MoTOne 4 weeks ago

I think why is not A is because of this sentence - "The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs." - so let's not think it as requiring a maintenance page

upvoted 1 times

atirado 3 months, 3 weeks ago

Selected Answer: AE

Option A - This option helps: Allows exposing custom error pages from a highly-available location

Option B - This option requires a lot of set up

Option C - This option might not work because modifying DNS will redirect all traffic to a publicly accessible webpage

Option D - This option requires a lot of set up

Option E - This option helps: Shows a custom error page when the error occurs

upvoted 4 times

abeb 4 months, 2 weeks ago

should be AE

upvoted 2 times

severlight 5 months ago

Selected Answer: AE

I haven't found out why we should use C.

upvoted 1 times

✉ **bur4an** 7 months, 1 week ago

Selected Answer: AE

Agree with Raj40

upvoted 2 times

✉ **dimitry_khan_arc** 7 months, 2 weeks ago

Selected Answer: CE

C & E.

B & D are incorrect. Managing lambda is overhead.

A is incorrect. Static page from S3 need to retrieve with custom code.

upvoted 2 times

✉ **jainparag1** 4 months, 2 weeks ago

Do you have any further reference to your explanation of custom code requirement to fetch the error page from S3?

upvoted 1 times

✉ **_Jassybang_** 2 months ago

not really , you just need to static url provided by aws when you use the bucket for static webpage and embed it anywhere to reach to the static website

upvoted 1 times

✉ **cattle_rei** 8 months, 3 weeks ago

Selected Answer: AE

AE because it accomplishes the task and is the least complex.

upvoted 3 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: AE

AE is right

upvoted 1 times

✉ **Parimal1983** 9 months, 2 weeks ago

Selected Answer: AE

Custom error pages need to setup in different location then source (where web pages is hosted), configure CloudFront to use those custom error pages

upvoted 1 times

✉ **rtguru** 10 months, 3 weeks ago

Correct answer is A&E

upvoted 2 times

✉ **Sarutobi** 12 months ago

Selected Answer: AE

We need a combination, so A provides the error page; should we go with DNS health-check (C+A) or CloudFront (E+A)? In my case, I try to stick to a single service to do failover, and DNS is a great option, but it looks like, in this question, CloudFront is already present with the least-operational overhead.

upvoted 4 times

✉ **mfsec** 1 year ago

Selected Answer: AE

AE - easy

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: AE

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

upvoted 1 times

✉ **higashikumi** 1 year, 1 month ago

Explanation:

Option A allows the creation of a custom error page that can be hosted on an S3 bucket. Option E provides a way to configure a custom error response for CloudFront, which can point to the S3 bucket hosting the error page. This allows visitors to see a custom error page without modifying any of the application infrastructure.

upvoted 3 times

✉ **dev112233xx** 1 year, 1 month ago

Selected Answer: AE

A&E are the correct answers imo

upvoted 1 times

Question #11

Topic 1

A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.

The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets.

Which combination of actions should the solutions architect perform to meet these requirements? (Choose two.)

- A. Create a transit gateway in the infrastructure account.
- B. Enable resource sharing from the AWS Organizations management account.
- C. Create VPCs in each AWS account within the organization in AWS Organizations. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account. Peer the VPCs in each individual account with the VPC in the infrastructure account.
- D. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each subnet to associate with the resource share.
- E. Create a resource share in AWS Resource Access Manager in the infrastructure account. Select the specific AWS Organizations OU that will use the shared network. Select each prefix list to associate with the resource share.

Correct Answer: AD

Community vote distribution

BD (86%)

14%

✉  **masetromain**  1 year, 3 months ago

Selected Answer: BD

I go with BD

upvoted 24 times

✉  **masetromain** 1 year, 2 months ago

Step B is needed because it enables the organization to share resources across accounts.

Step D is needed because it allows the infrastructure account to share specific subnets with the other accounts in the organization, so that the other accounts can create resources within those subnets without having to manage their own networks.

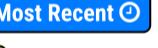
upvoted 12 times

✉  **razguru**  1 year, 3 months ago

A - Doesn't seem correct as the question didn't state multiple VPs, so transit gateway is not relevant.

I will go with B & D

upvoted 8 times

✉  **rapatajones**  1 week, 3 days ago

Selected Answer: BE

B E correta

upvoted 1 times

✉  **rapatajones** 1 week, 3 days ago

BE com certeza

upvoted 1 times

✉  **gofavad926** 3 weeks, 3 days ago

Selected Answer: BD

BD, as mentioned in other comments

upvoted 1 times

✉  **atirado** 3 months, 3 weeks ago

Selected Answer: BD

Option A - Does not assist with allowing OUs to create resources in the subnets

Option B - Allows sharing resources across the entire organization

Option C - This option does not work as a way to share subnets because it creates multiple VPCs and subnets in the accounts rather than allowing managing resources in shared subnets

Option D - Directly shares the subnets

Option E - Does not assist because it only shares pre-built CIDR blocks rather than subnets

upvoted 1 times

✉ **shaaam80** 4 months, 1 week ago

Selected Answer: BD

Answer - B & D.

A is wrong. No TGW needed as customer has just 1 VPC.

E is wrong - can't share resources via RAM using prefix lists.

C is wrong - talks about creating VPCs with same CIDR ranges and VPC peering (not possible with overlapping CIDRs and not needed for this solution as there is just 1 VPC).

upvoted 1 times

✉ **GibaSP45** 4 months, 1 week ago

Selected Answer: BE

<https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html>

upvoted 3 times

✉ **abeb** 4 months, 2 weeks ago

BE is good

upvoted 1 times

✉ **AlbertS82** 4 months, 3 weeks ago

Selected Answer: BD

B&D is the only correct answer

upvoted 1 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: BD

I don't see the way you can share a prefix list.

upvoted 1 times

✉ **senthilsekaran** 5 months, 1 week ago

B & D correct

upvoted 1 times

✉ **ansgohar** 6 months, 2 weeks ago

Selected Answer: BD

I go with B & D

upvoted 1 times

✉ **srs27** 4 months, 4 weeks ago

Do you really need Management account to share the resources among the accounts? I doubt.

upvoted 1 times

✉ **sreed77** 6 months, 4 weeks ago

Selected Answer: BD

Option B allows the infrastructure team to manage the network in the infrastructure account. It also allows individual accounts to create AWS resources within subnets. This is done by creating a resource share in AWS Resource Access Manager (RAM) in the infrastructure account. The resource share is then associated with the specific AWS Organizations OU that will use the shared network. The subnets are then associated with the resource share.

Option D is also necessary because it allows the infrastructure team to control who has access to the shared network. This is done by assigning permissions to the resource share.

Here are the steps involved in implementing this solution:

Create a resource share in RAM in the infrastructure account.

Select the specific AWS Organizations OU that will use the shared network.

Select each subnet to associate with the resource share.

Assign permissions to the resource share.

upvoted 4 times

✉ **dimitry_khan_arc** 7 months, 2 weeks ago

Selected Answer: BD

B & D are most relevant

upvoted 1 times

✉ **whenthan** 7 months, 3 weeks ago

Selected Answer: BD

<https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/>

upvoted 3 times

✉ **cattle_rei** 8 months, 3 weeks ago

Selected Answer: BD

BD is the most correct, the rest are distractors

upvoted 1 times

Question #12

Topic 1

A company wants to use a third-party software-as-a-service (SaaS) application. The third-party SaaS application is consumed through several API calls. The third-party SaaS application also runs on AWS inside a VPC.

The company will consume the third-party SaaS application from inside a VPC. The company has internal security policies that mandate the use of private connectivity that does not traverse the internet. No resources that run in the company VPC are allowed to be accessed from outside the company's VPC. All permissions must conform to the principles of least privilege.

Which solution meets these requirements?

- A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides. Create a security group to limit the access to the endpoint. Associate the security group with the endpoint.
- B. Create an AWS Site-to-Site VPN connection between the third-party SaaS application and the company VPC. Configure network ACLs to limit access across the VPN tunnels.
- C. Create a VPC peering connection between the third-party SaaS application and the company VPC. Update route tables by adding the needed routes for the peering connection.
- D. Create an AWS PrivateLink endpoint service. Ask the third-party SaaS provider to create an interface VPC endpoint for this endpoint service. Grant permissions for the endpoint service to the specific account of the third-party SaaS provider.

Correct Answer: A*Community vote distribution*

Raj40 Highly Voted 1 year, 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>

upvoted 17 times

masetromain Highly Voted 1 year, 3 months ago

Selected Answer: A

I go with A

upvoted 8 times

masetromain 1 year, 2 months ago

A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides. Create a security group to limit the access to the endpoint. Associate the security group with the endpoint.

This solution uses AWS PrivateLink, which creates a secure and private connection between the company's VPC and the third-party SaaS application VPC, without the traffic traversing the internet. The use of a security group and limiting access to the endpoint service conforms to the principle of least privilege.

upvoted 11 times

gofavad926 Most Recent 3 weeks, 3 days ago

Selected Answer: A

A, the service provider creates an endpoint service and grants their customers access to the endpoint service. As the service consumer, you create an interface VPC endpoint, which establishes connections between one or more subnets in your VPC and the endpoint service.

upvoted 1 times

atirado 3 months, 3 weeks ago

Selected Answer: A

Option A - The interface VPC Endpoint will provide local access to the SaaS service from within the company's VPC. Moreover, traffic to and from the SaaS VPC will traverse the AWS network rather than the internet. This is considered private traffic.

Option B - This option might not work: Nothing is said about whether the CIDR blocks in each VPC overlap. Moreover, nothing is said about whether bandwidth limitations on Site-to-Site VPN could be an issue.

Option C - This option might not work: Nothing is said about whether the CIDR blocks in each VPC overlap.

Option D - This option will not work: A PrivateLink Endpoint service is used for facilitating access to AWS services.

upvoted 2 times

shaam80 4 months, 1 week ago

Selected Answer: A

Answer - A.

VPC Interface endpoint to access any service privately without traversing the internet.

AWS PrivateLink VPC endpoint to access the SaaS application.

upvoted 1 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: A

obvious

upvoted 1 times

✉ **senthilsekaran** 5 months, 1 week ago

Correct Answer : A

upvoted 1 times

✉ **task_7** 6 months, 4 weeks ago

Selected Answer: D

A VS D

A. Create an AWS PrivateLink interface VPC endpoint. Connect this endpoint to the endpoint service that the third-party SaaS application provides.

D. Create an AWS PrivateLink endpoint service. Ask the third-party SaaS provider to create an interface VPC endpoint for this endpoint service
D is right SaaS provider has create interface VPC endpoint for this endpoint service

upvoted 3 times

✉ **_Jassybang_** 2 months ago

exactly , we need to access the resource from SAAS Provider and not vice versa , Hence in this case the VPC Gateway endpoint should be provided from SAAS Provider for the privatelink endpoint we provide it to them - we use this for Snowflake Saas :)

upvoted 1 times

✉ **whenthan** 7 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>

<https://aws.amazon.com/blogs/apn/enabling-new-saas-strategies-with-aws-privatelink/>

upvoted 1 times

✉ **cattle_rei** 8 months, 3 weeks ago

Selected Answer: A

It's A because in this scenario we are consuming a service , not providing one, so that eliminates E .

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: A

it s a

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: A

Create an AWS PrivateLink interface VPC endpoint.

upvoted 1 times

✉ **2aldous** 11 months, 3 weeks ago

Selected Answer: A

Access SaaS products through AWS PrivateLink is the answer.

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

Create an AWS PrivateLink interface VPC endpoint.

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>

upvoted 1 times

✉ **ptpho** 1 year, 3 months ago

It's A .clearly

upvoted 4 times

✉ **spencer_sharp** 1 year, 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html>

upvoted 4 times

Question #13

Topic 1

A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances. Which set of actions should a solutions architect take to meet these requirements?

- A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports.
- B. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use Amazon QuickSight integration with OpsWorks to generate patch compliance reports.
- C. Use an Amazon EventBridge rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports.
- D. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

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

✉  **masetromain**  1 year, 3 months ago

Selected Answer: A

A is good

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patch-management-hybrid-cloud/design-on-premises.html>

upvoted 13 times

✉  **masetromain** 1 year, 2 months ago

A is correct. AWS Systems Manager can manage patches on both on-premises servers and EC2 instances and can generate patch compliance reports. AWS OpsWorks and Amazon Inspector are not specifically designed for patch management and therefore would not be the best choice for this use case. Using Amazon EventBridge rule and AWS X-Ray to generate patch compliance reports is not a practical solution as they are not designed for patch management reporting.

upvoted 11 times

✉  **gofavad926**  3 weeks, 3 days ago

Selected Answer: A

A is the correct answer

upvoted 1 times

✉  **MoTOne** 4 weeks ago

Selected Answer: A

AWS OpsWorks is a configuration management service that provides a way to automate the deployment, configuration, and management of applications on EC2 instances. It is designed to help you manage the entire lifecycle of your applications.

upvoted 1 times

✉  **atirado** 3 months, 3 weeks ago

Selected Answer: A

Option A - Systems Manager patches and generates patch compliance reports.

Option B - This option does not apply because Chef or Puppet are not mentioned in the question. Moreover, either one does not directly perform patch management.

Option C - Inspector would generate a report for on-premise resources

Option D - This option does not apply because Chef or Puppet are not mentioned in the question. Moreover, X-Ray does apply.

upvoted 1 times

✉  **severlight** 4 months, 4 weeks ago

Selected Answer: A

obvious

upvoted 1 times

✉  **whenthan** 7 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **stevegod0** 8 months, 2 weeks ago

A is correct:

<https://www.amazonaws.cn/en/systems-manager/>

upvoted 1 times

 **cattle_rei** 8 months, 3 weeks ago

Selected Answer: A

Other options are distractors. Opswork would be right only if customer wanted to make use of existing script or know-how in chef or puppet.

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: A

yep - A

upvoted 1 times

 **EricZhang** 10 months, 2 weeks ago

A is the best but Systems Manager cannot generate the patch compliance reports.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patch-management-hybrid-cloud/design-on-premises.html>

- A resource data sync in Systems Manager Inventory gathers the patching details and publishes them to an S3 bucket.

- Patch compliance reporting and dashboards are built in Amazon QuickSight from the S3 bucket information.

upvoted 1 times

 **gameoflove** 11 months, 1 week ago

Selected Answer: A

A is the right answer for this question as per information shared by them

upvoted 2 times

 **2aldous** 11 months, 3 weeks ago

Selected Answer: A

Easy question :)

A is the answer.

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: A

Use AWS Systems Manager to manage patches

upvoted 1 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patch-management-hybrid-cloud/design-on-premises.html>

upvoted 1 times

 **gameoflove** 1 year, 1 month ago

Selected Answer: A

AWS System Manager support On-premise and EC2 instance patching

upvoted 2 times

 **dev112233xx** 1 year, 1 month ago

Selected Answer: A

A is correct ofc.. easy one)

upvoted 1 times

 **spencer_sharp** 1 year, 3 months ago

Selected Answer: A

AS THE SAME WITH SAP-C01 QUESTION 782

upvoted 2 times

Question #14

Topic 1

A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.

Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
- B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
- C. Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data. Create an Amazon EventBridge rule to detect EC2 instance termination. Invoke an AWS Lambda function from the EventBridge rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic. From the SNS notification, call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: B

B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance. This approach will use the Auto Scaling lifecycle hook to execute the script that copies log files to S3, before the instance is terminated, ensuring that all log files are copied from the terminated instances.

upvoted 12 times

 **rtgfdv3**  1 year, 3 months ago

Selected Answer: B

<https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-instance/>
upvoted 7 times

 **gofavad926**  3 weeks, 3 days ago

Selected Answer: B

B is the correct answer
upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This option might not work: Preventing ASG termination could create further trouble and there is no guarantee the script will run if the instance happens to be unhealthy
 Option B - This option could work: Running the script from the SSM API guarantees the script will run, using EventBridge to capture the ASG termination event provides a perfect place to hook in the call to SSM which will also pause the termination until the script runs. Then CONTINUE allows the ASG termination to continue.
 Option C - This option does not work because it does not solve the problem: Terminating instances within the 15 minute window causes log files to be lost.
 Option D - This option might not work: It does not rely on EventBridge to detect the ASG termination event. It also could create further trouble because no other actions will be performed due to sending ABANDON though nothing is said about other actions in the question
upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: B

both abandon and continue will lead to instance termination, the difference is abandon will prevent from running other lifecycle hooks
upvoted 1 times

 **ansgohar** 6 months, 2 weeks ago

Selected Answer: B

B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.

upvoted 1 times

 **cattle_rei** 7 months, 2 weeks ago

Selected Answer: B

I think this is B. It could be A as well, but B is better solution because the document with SM can be re-utilized with other instances. Also A would require using a custom image with the script or user data to create the script, so more points of failure.

upvoted 1 times

 **cattle_rei** 7 months, 2 weeks ago

I think this is B. It could be A as well, but B is better solution because the document with SM can be re-utilized with other instances. Also A would require using a custom image with the script or user data to create the script, so more points of failure.

upvoted 1 times

 **softarts** 7 months, 3 weeks ago

Selected Answer: B

d is wrong, shouldn't be "ABANDON"

upvoted 2 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

it's a B

upvoted 1 times

 **gameoflove** 11 months, 1 week ago

Selected Answer: B

B is the right answer due to Auto Scaling lifecycle hook and an Amazon EventBridge rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send

upvoted 1 times

 **F_Eldin** 11 months, 1 week ago

Selected Answer: B

A- Wrong because prevent termination is not needed.

C- Wrong because 5-minute frequency creates an overhead or delay . Using user data for the script adds complexity

D- Wrong because SNS

upvoted 2 times

 **2aldous** 11 months, 3 weeks ago

Selected Answer: B

B.

Smart solution :)

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: B

Systems manager + eventbridge

upvoted 3 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: B

<https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-instance/>

upvoted 2 times

 **Untamables** 1 year, 3 months ago

Selected Answer: B

B

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

upvoted 4 times

 **masetromain** 1 year, 3 months ago

I find answer C correct.

but can at the same time that an instance is terminated run a lambda function that executes the script?

upvoted 1 times

 **masetromain** 1 year, 3 months ago

I'm wrong the answer is B

<https://www.examtopics.com/discussions/amazon/view/69532-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

Question #15

Topic 1

A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A. The company's applications and databases are running in Account B.

A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db.example.com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.

During deployment, the application failed to start. Troubleshooting revealed that db.example.com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53.

Which combination of steps should the solutions architect take to resolve this issue? (Choose two.)

- A. Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone.
- B. Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv.conf file.
- C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- D. Create a private hosted zone for the example com domain in Account B. Configure Route 53 replication between AWS accounts.
- E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A.

Correct Answer: BC*Community vote distribution*

CE (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: CE

C and E are correct.

C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.

This step is necessary because the VPC in Account B needs to be associated with the private hosted zone in Account A to be able to resolve the DNS records.

E. Associate a new VPC in Account B with a hosted zone in Account A. Delete the association authorization in Account A.

This step is necessary because the association authorization needs to be removed in Account A after the association is done in Account B.

upvoted 29 times

 **kiran15789**  1 year, 1 month ago

Selected Answer: CE<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs-different-accounts.html>

upvoted 9 times

 **8608f25**  2 months ago

Selected Answer: CE

Correct answers

upvoted 1 times

 **8608f25** 2 months ago

Explanation:

- * Option C is correct because, in a multi-account AWS setup, to use a Route 53 private hosted zone from one account (Account A) in another account's VPC (Account B), you first need to create an authorization. This authorization is necessary for allowing the private hosted zone in one account to be associated with a VPC in another account. This step enables the resolution of DNS records stored in the private hosted zone across accounts.

- * Option E is correct as it follows up on the authorization created in Option C. Once the authorization is in place, you can then associate the new VPC in Account B with the private hosted zone in Account A. This association is what actually allows the EC2 instances within the VPC in Account B to resolve DNS queries using the private hosted zone in Account A, ensuring that db.example.com can be resolved as intended.

upvoted 3 times

 **8608f25** 2 months ago

Why the others are incorrect:

- * Option A is not a direct solution to the problem of DNS resolution across AWS accounts. Deploying the database on an EC2 instance does not address the issue of DNS resolution for the RDS endpoint across accounts.

- * Option B is not a scalable or AWS-recommended solution. Manually adding RDS endpoint IP addresses to the /etc/resolv.conf file on an EC2 instance is not practical for environments that require automation and could lead to issues if the RDS endpoint changes.

- * Option D involves creating a separate private hosted zone in Account B and configuring Route 53 replication between AWS accounts. This option is unnecessary and more complex than required. The direct association of VPCs across accounts to a single hosted zone is a simpler and more effective solution.

Therefore, Options C and E are the steps that directly address the issue with the least complexity and enable the intended DNS resolution across AWS accounts.

upvoted 2 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: CE

Option A - This option does not work - It does not provide for solving address name resolution in the new VPC

Option B - This option works but it breaks the company's architecture where all DNS names are stored in the private zone in Account A

Option C - This option contributes to the solution.

Option D - Breaks the company's architecture

Option E - This option contributes to the solution

upvoted 1 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: CE

obvious

upvoted 1 times

 **SfQ** 5 months, 3 weeks ago

Selected Answer: CE

C and E are correct.

B is not a best solution. It's a manual setup and it may lose the configuration if we are using ASG and launching new instance.

upvoted 1 times

 **Chainshark** 6 months ago

Why is B marked as correct?

upvoted 2 times

 **SfQ** 5 months, 3 weeks ago

B is not a best solution. It's a manual setup and it may lose the configuration if we are using ASG and launching new instance.

upvoted 2 times

 **whenthan** 7 months, 3 weeks ago

Selected Answer: CE

<https://repost.aws/knowledge-center/route53-private-hosted-zone>

Create an authorization to associate the private hosted zone and as a best practice , it is recommended to delete the association authorization in account A-This step prevents you from recreating the same association later. To delete the authorization, reconnect to the EC2 instance in Account A

upvoted 2 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: CE

it's CE

upvoted 1 times

 **Jonalb** 9 months, 3 weeks ago

Selected Answer: CE

cccccccccccccceeeeeeeeeeee

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

 **SkyZeroZx** 10 months ago

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

 **AWS_Sam** 11 months ago

C + E are correct

upvoted 1 times

 **gameoflove** 11 months, 1 week ago

Selected Answer: CE

C & E as Issue is associated with authorization

upvoted 1 times

 **Maria2023** 11 months, 3 weeks ago

Selected Answer: CE

C and E are correct
upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: CE
CE seems like the best choice
upvoted 2 times

 **mKrishna** 1 year, 1 month ago
ANS: A & C

B is incorrect because modifying the /etc/resolv.conf file on the EC2 instance would not resolve the issue since the issue is with the Route 53 configuration.
upvoted 1 times

Question #16

Topic 1

A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume. The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos. Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
- C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
- D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

Correct Answer: C*Community vote distribution*

masetromain Highly Voted 1 year, 2 months ago

Selected Answer: C

C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.

Amazon CloudFront is a content delivery network (CDN) that can be used to deliver content to users with low latency and high data transfer speeds. By configuring a CloudFront distribution for the blog site and pointing it at an S3 bucket, the videos can be cached at edge locations closer to users, reducing buffering and timeout issues. Additionally, S3 is designed for scalable storage and can handle high levels of user traffic. Migrating the videos from EFS to S3, would also improve the performance and scalability of the website.

upvoted 22 times

spencer_sharp Highly Voted 1 year, 3 months ago

Selected Answer: C

No brainer

upvoted 9 times

Christophe_ Most Recent 1 month, 3 weeks ago

Selected Answer: D

Option C - Does not support new content added later by users, does not accelerate site content
Option D - Accelerate site and videos, allow content added

upvoted 1 times

e4bc18e 1 month ago

Cloudfront caches data to serve more rapidly at the edge and not have to serve content from the backend, that is acceleration. Also you can now write to S3 for new data. Sorry your choice is not correct.

upvoted 2 times

atirado 3 months, 3 weeks ago

Selected Answer: C

Option A - This option might not work and is not cheap: It will increase costs and has limited scalability. EFS is an expensive storage solution for videos

Option B - This option might not work: Nothing is mentioned about whether the application is stateful or stateless and whether the ALB has client stickiness so using instance store could provide an inconsistent user experience. S3 is a cheap storage option

Option C - This option will work and is cheap: A CloudFront distribution and S3 will provide the most scalability and availability possible from AWS; and both are very cheap options for distribution and storage of content

Option D - This option might work but is not cheap: Moving all content to CloudFront ensures it will be served from the edge cache for the duration of the cache mitigating issues during high usage. However, nothing is said in the question about usage patterns, i.e performance issue will happen again for older content. Moreover, EFS is an expensive storage solution for video files compared to S3.

upvoted 1 times

ninomfr64 3 months, 3 weeks ago

Selected Answer: C

Not A as Max I/O increase IOPS but negatively impact latency, ultimately you will have little to no performance improvement. Also you cannot enable Max IO on an existing filesystem.

Not B as this is not a cheap option (instance store generally cost more than EBS backed), also without a CDN there will be little performance improvement

Not D as this provides performance improvements, but this provide comparable performance to option C at higher costs as in D videos are stored on EFS that cost more than S3 and all traffic goes through CDN rather than only videos that actually needs edge caching

Thus C provide performance improvements (thanks for CloudFront) with cost-effective approach (S3 is cheap)
upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Also this follows AWS best practices to separate static content from dynamic content allowing for better scalability
upvoted 1 times

 **geekos** 4 months, 1 week ago

Selected Answer: C

C is good
upvoted 1 times

 **abeb** 4 months, 2 weeks ago

C is good
upvoted 1 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: C

obvious
upvoted 1 times

 **cattle_rei** 7 months, 1 week ago

Selected Answer: C

No doubt it's C. To me the keyword there is scalable. S3 will be able to handle any amount of content users can generate. EFS is not the right solution for object storage, s3 is. EFS is a solution for a sharable network filesystem, that can be mounted and used by many operation systems.
upvoted 1 times

 **Magoose** 9 months ago

Selected Answer: D

C and D are both viable. But D would be less overhead as you would most likely need to reconfigure the web application more to get it working with S3. Option D with Elastic Beanstalk provides a higher level of abstraction and automates many aspects of the application management, which can reduce operational overhead and simplify the re-architecting process
upvoted 1 times

upvoted 1 times

 **totopopo** 8 months, 3 weeks ago

D is not cost effective, which was the demand for the question.
If it was about less changes, I would go with it.
Here, right answer is C.
upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

C more cost efficient
upvoted 1 times

 **karim_arous** 9 months, 3 weeks ago

Selected Answer: C
C without a doubt
upvoted 1 times

 **gameoflove** 11 months, 1 week ago

Selected Answer: C
C is only option which meet their requirement
upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: C
Configure an Amazon CloudFront distribution.
upvoted 2 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: C
by configuring a CloudFront distribution for the blog site and pointing it at an S3 bucket, the videos can be cached at edge locations closer to users, reducing buffering and timeout issues.
upvoted 2 times

 **dev112233xx** 1 year, 1 month ago

Selected Answer: C
C ofc.. i hope i will get such easy question in the real exam
upvoted 3 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is the correct

upvoted 2 times

Question #17

Topic 1

A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC.

A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.

Which solution meets these requirements?

- A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.
- B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
- D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: A

A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.

This solution provides a redundant Direct Connect connection in the same Region by creating a new private virtual interface on each connection, and connecting both private virtual interfaces to a Direct Connect gateway. The Direct Connect gateway is then connected to the single VPC. This solution also allows the company to expand into other Regions while providing connectivity through the same pair of Direct Connect connections.

The Direct Connect Gateway allows you to connect multiple VPCs and on-premises networks in different accounts and different regions to a single Direct Connect connection.

It also provides automatic failover and routing capabilities.

upvoted 20 times

 **anita_student** 1 year, 1 month ago

Option D is not possible at all. You connect to TGW using transit VIF, not private VIF

upvoted 6 times

 **AMohanty** 6 months, 3 weeks ago

Transit GW - connects both over Private VIF and Transit VIF

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Option D is not the best solution because it uses a Transit Gateway, which is used to connect multiple VPCs and on-premises networks in different accounts and different regions, but it is not necessary in this scenario. The company only wants to add a redundant Direct Connect connection in the same Region and connect it to the same VPC. Additionally, using a Transit Gateway in this scenario would add more complexity and might not be necessary.

Also, Transit Gateway does not provide automatic failover and routing capabilities, which is required in this scenario.

The Direct Connect Gateway is a better choice in this scenario as it provides the necessary functionality of automatic failover and routing capabilities, and it is more suitable for connecting multiple Direct Connect connections to a single VPC.

upvoted 11 times

 **Sarutobi** 1 year, 1 month ago

All options here are problematic. The DX-GW is a control plane-only device; in other words, no actual traffic goes over it; it is just a Route-Reflector it only carries the routing table. TGW is not a region construct, so by itself, it cannot provide regional redundancy. In any case, all things considered, maybe A is the closest but it should mention VGW.

upvoted 2 times

 **Sarutobi** 1 year, 1 month ago

I meant to say, "TGW is a region construct".

upvoted 1 times

 **zozza2023**  1 year, 2 months ago

Selected Answer: A

A is the correct solution and the best

upvoted 5 times

 **kz407**  3 weeks, 4 days ago

What I don't understand is why do you need to delete the existing private VIF? Can't that be reassigned?

upvoted 1 times

 **MoTOne** 3 weeks, 6 days ago

Private Virtual Interface is a logical connection between your Direct Connect connection and a Direct Connect gateway. It is a virtual representation of the physical connection and allows you to establish connectivity to the VPCs associated with the Direct Connect gateway.

upvoted 1 times

 **KyleZheng** 3 months, 1 week ago

A

Because "Transit GW can also communicate from on-premises to AWS, but this one uses Site to Site VPN (IPSec VPN)."

upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: A

Option A - This option might work however it is missing a step: Connecting the Direct Connect Gateway to a Virtual Private Gateway in the single VPC (and any VPC in a new region)

Option B - This option will not work: It does not allow to grow into new regions and it does not create a redundant link

Option C - This option will not work: Using a Public Virtual interface does not connect VPC resources to on-premise

Option D - This option might work however it missing multiple steps: Each VPC will require its own Transit Gateway. Each Transit Gateway will connect through an association with Direct Connect gateway. Each Direct Connect connection will connect to the Direct Connect Gateway using a Transit VIF

upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Selected Answer: A

I have to admit that initially I picked a wrong answer, here is my findings after some docs browsing:

Not B as this will provide Direct Connect (DX) redundancy but does not provide connectivity to other Regions

Not C as this will not even provide DX redundancy for the VPC because the public VIF on the new connection does not provide access to the VPC

Not D as Transit Gateway (TGW) is a regional resources and does not allows to provide connectivity to other Regions (you can peer with a TGW in another Region). Also you need to have a Transit virtual interface to connect a DX to a TGW or you need to have DXGW to connect a VIF to a TGW.

A is correct as a DXGW is a global resources that allows cross-region attachments

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

Selected Answer: A

Answer A. DCGW is the only option here as it supports both DC connections plus allows expansion into other regions. TGW does not span regions.

upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: A

multiple regions - dx gateway

upvoted 1 times

 **AMohanty** 6 months, 3 weeks ago

None of the options seem to satisfy the condition "Solution must provide connectivity to other regions through same pair of Direct Connect Connections."

In both option A and D, we don't talk of associating second region VPC to the Transit GW or Direct Connect GW.

upvoted 1 times

 **whenthan** 7 months, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/>

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: A

It's A.

D is not supported

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: A

A

keyword === Direct Connect gateway

upvoted 1 times

 **gameoflove** 11 months, 1 week ago

Selected Answer: A

A. Is the Correct Option as Direct Connect Gateway with Private Virtual Interface will meet the requirement

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: A

Provision a Direct Connect gateway.

upvoted 2 times

 **God_Is_Love** 1 year, 1 month ago

Logical answer : B and C are good for existing architecture in question. But with redundant DX connection requirement, only solution is Gateway. that resolves to A(Direct connect gateway) or D(Transit gateway), but D as transit gateway is wrong because it mentions private interfaces connecting with transit gateway which is weird [usually VPC attachments are made connecting transit gateway]. So answer is A - Direct Connect Gateway. (Infact, this is future proof when we want different VPCs in different regions later with this architecture)

upvoted 3 times

 **Untamables** 1 year, 3 months ago

Selected Answer: A

A

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-vgw-multi-regions-and-aws-public-peering.html>

upvoted 3 times

Question #18

Topic 1

A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization.

The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2 instances running in an Auto Scaling group to process an Amazon SQS queue. The company wants to re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software.

Which solution meets these requirements?

- A. Use Amazon ECS containers for the web application and Spot instances for the Auto Scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.
- B. Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notification to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

Correct Answer: D

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: C

This solution meets the requirements by using multiple managed services offered by AWS which can reduce the operational overhead. Hosting the web application in Amazon S3 would make it highly available, scalable and can handle variable traffic. The uploaded videos can be stored in S3 and processed using S3 event notifications that trigger a Lambda function, which calls the Amazon Rekognition API to categorize the videos. SQS can be used to process the event notifications and also it is a managed service.

This solution eliminates the need to manage EC2 instances, EBS volumes and the custom software. Additionally, using Lambda function in this case, eliminates the need for managing additional servers to process the SQS queue which will reduce operational overhead.

By using this solution, the company can benefit from the scalability, reliability, and cost-effectiveness that these services offer, which can help to reduce operational overhead and improve the overall performance and security of the application.

upvoted 26 times

✉️ **Mahakali** 6 months, 2 weeks ago

Any explanation on option A ?

upvoted 1 times

✉️ **RaghavendraPrakash** 1 year ago

D. Because, you cannot host web application in S3, only static web assets. ElasticBeanStalk provides an easy way to onboard autoscaling web apps with minimal operational overheads.

upvoted 11 times

✉️ **gofavad926** 3 weeks, 3 days ago

"The company wants to re-architect the application "...

upvoted 1 times

✉️ **Arnaud92** 7 months, 1 week ago

But it is specifically specified that the web app is just static content...

upvoted 1 times

✉️ **Boops** 7 months ago

"The website contains static content"

Contains do not means that all the website is just static

upvoted 1 times

✉️ **Six_Fingered_Jose** 7 months ago

They also do not mention the website has any dynamic content so there's that

upvoted 8 times

✉️ **jpa8300** 3 months, 1 week ago

D is right and it is valid, but C seems to me a more complete and better solution. And I agree that the site seems to be only static content. Usually, when it has dynamic content it is mentioned in the question.

upvoted 1 times

 **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: C

C, this is a typical scenario

upvoted 1 times

 **kz407** 3 weeks, 4 days ago

Selected Answer: C

While I vote for C, I do think however that whether we can go with C really depends on the application codebase.

The use case mentions that the application enables file uploads. We know that handling files require a backend, if your application is written in something like Java. If that's the case, you won't be able to host your application in S3. The phrase "website contains static content" is really vague, as it does not reveal anything about the backend of the application.

Now, the fact that the application has EBS to store Video files give up a hint, that suggests that the application has some BE code.

I am taking a hint from "re-architect" I assume involves some revamping of the applications codebase. So, here's how I'd go about "re-architecting"

1. Move storage of files to S3.

2. Eliminate the BE codebase, revamp the FE codebase to rely entirely on AWS JS SDK and handle file uploads with that. Now you don't need to manage any compute resources at all.

3. Go about the rest of the solution.

upvoted 1 times

 **MoTOne** 3 weeks, 6 days ago

re-architect the application to reduce operational overhead

upvoted 1 times

 **grire974** 3 months ago

Selected Answer: C

If it were D - how would Rekognition access the videos to classify? Rekognition would need to ssh into the EBS volume of various beanstalk instances running under an ASG (impossible as far as I know). I agree though - I think the wording is terrible for 'contains static content'; as how on earth would this type of app practically run on s3 alone for login/ user auth etc.. would need to be coupled with other serverless products such as lambda/cognito etc.

upvoted 1 times

 **grire974** 3 months ago

per my previous comment; s3 is the only viable data source for rekognition

<https://aws.amazon.com/rekognition/faqs/#:~:text=Amazon%20Rekognition%20Video%20operations%20can,are%20MPEG%2D4%20and%20MOV.>

from my experience this is the same too with similar services like elastic transcoder

upvoted 1 times

 **924641e** 3 months, 4 weeks ago

Selected Answer: C

The mention of static content really throws this question off and clearly the community thinks this as well. The argument of static website vs static content being the key to selecting D isn't really a strong argument but that doesn't exclude D from being a viable solution. Operational overhead is minimized with Elastic Beanstalk and removes dependencies on third party tools/software.

upvoted 2 times

 **24Gel** 3 weeks, 6 days ago

thanks, this is the best explain

upvoted 1 times

 **subupro** 4 months ago

Elastic bean stack is not required , it is a static content only, better can go with S3. So Answer is C

upvoted 1 times

 **abeb** 4 months, 2 weeks ago

C videos in Amazon S3

upvoted 1 times

 **KevinYao** 4 months, 2 weeks ago

Selected Answer: D

Web application is never hosted in S3, that is storage normally.

upvoted 1 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: C

C is a well-explained and detailed solution. For D it isn't like that, for instance, there is no solution provided for storing images.

upvoted 1 times

 **M4D3V1L** 6 months, 1 week ago

It's A, I had the same question in Jon Bonzo's tests and the right answer is A.

upvoted 2 times

✉ **alexua** 6 months, 2 weeks ago

I go with D. "web site has static content" it's not the same be static web site. And web site on S3 does not go with https, so upload the video without Authentication & SSL/TLS !???

upvoted 1 times

✉ **Simon523** 7 months, 1 week ago

Selected Answer: C

The case is similar to the blogs below, and seem normally Amazon Rekognition is trigger by AWS Lambda function.

<https://aws.amazon.com/tw/blogs/architecture/detecting-solar-panel-damage-with-amazon-rekognition-custom-labels/>

upvoted 1 times

✉ **whenthan** 7 months, 3 weeks ago

Selected Answer: C

While AWS Elastic Beanstalk can simplify deployment, it might not fully meet the requirement of removing dependencies on third-party software, as it still requires using Amazon Rekognition. This option introduces additional complexity by maintaining a separate worker environment for SQS queue processing.

upvoted 2 times

✉ **chico2023** 8 months, 1 week ago

Answer D.

It says: "The website contains static content...", not "It's a static website".

Still, even if you argue that it's possible to host a web application in S3 with a combination of S3 + Lambda + ..., you would fall into increasing the operational overhead with so many moving parts.

AWS Elastic Beanstalk is a platform as a service used for deploying and scaling web applications and services and, although it won't make everything serverless (they are not asking for that), it will make management and deployment easier while still using AWS Managed Services.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts-worker.html>

upvoted 4 times

✉ **Arnaud92** 7 months, 1 week ago

Why would they specify that the web app contains static content if not 100% static content ? It wouldn't make sense here. You have to assume that it is a static website.

upvoted 2 times

✉ **8608f25** 2 months, 4 weeks ago

It can't be a static website because users are able to upload contents to it. It is a dynamic website. The scenario mentions static content because that is part of the overall solutions.

upvoted 1 times

✉ **Russ99** 8 months, 3 weeks ago

Selected Answer: C

The main concern with option D is that it still relies on managing EC2 instances for both the web application and the worker environment, which might not be the most cost-effective and operationally efficient solution compared to the serverless architecture in option C.

upvoted 1 times

Question #19

Topic 1

A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified.

How can this be accomplished?

- A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- B. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon CloudWatch alarms are triggered.
- C. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.
- D. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

Correct Answer: B

Community vote distribution



B (100%)

✉  **masetromain**  1 year, 2 months ago

Selected Answer: B

AWS Serverless Application Model (SAM) is a framework that helps you build, test and deploy your serverless applications. It uses CloudFormation under the hood, so it is a way to simplify the process of creating, updating, and deploying CloudFormation templates. CodeDeploy is a service that automates code deployments to any instance, including on-premises instances and Lambda functions. With AWS SAM you can use the built-in CodeDeploy to deploy new versions of the Lambda function, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code.

You can also define CloudWatch Alarms to trigger a rollback in case of any issues.

This allows for a faster and more efficient deployment process, as well as a more reliable rollback process when errors are identified. This way you can increase the speed of deployment and reduce the time to detect and revert when errors are identified.

upvoted 26 times

✉  **gofavad926**  3 weeks, 3 days ago

Selected Answer: B

B, use SAM to deploy serverless applications on aws

upvoted 1 times

✉  **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This work will allow reverting to previous versions of the Lambda functions but reverting means all functions will be reverted. This does not minimize the the time needed to detect and revert errors.

Option B - This option minimizes the time needed to deploy functions and detect and revert errors: As each function is deployed it can be tested and reverted individually. Moreover, the option provides a straightforward mechanism to detect and revert errors: Detect errors in CloudWatch, fix the functions' code in SAM, redeploy with AWS CodeDeploy.

Option C - This option does not minimize the time needed to detect and revert errors. It only automates the current process.

Option D - This option does not minimize the time needed to detect and revert errors: It takes time for CloudFormation to switch origins and nothing has been done to about the current process for deploying and testing functions.

upvoted 1 times

✉  **shaam80** 4 months, 1 week ago

Selected Answer: B

Answer B. Use SAM and Codedeploy. Revert if any errors to the previous version.

upvoted 1 times

✉  **severlight** 4 months, 4 weeks ago

Selected Answer: B

obvious

upvoted 1 times

✉ **whenthan** 7 months, 2 weeks ago

Selected Answer: B

requirmeents :
decrease the time to deploy new versions of the application logic provided by the Lambda functions,
revert when errors identified

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

B no do0ubt
upvoted 1 times

✉ **Jonalb** 9 months, 2 weeks ago

Selected Answer: B

100% B
upvoted 1 times

✉ **gameoflove** 11 months, 1 week ago

Selected Answer: B

B solve the problem which is causing in the current scenario
upvoted 1 times

✉ **2aldous** 11 months, 3 weeks ago

Selected Answer: B

Definitile B
https://docs.aws.amazon.com/es_es/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html
upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: B

Use AWS SAM and built-in AWS CodeDeploy
upvoted 1 times

✉ **5up3rm4n** 1 year ago

Selected Answer: B

<https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverless-apps.html>

AWS Serverless Application Model (AWS SAM) comes built-in with CodeDeploy to provide gradual AWS Lambda deployments. With just a few lines of configuration, AWS SAM does the following for you:

Deploys new versions of your Lambda function, and automatically creates aliases that point to the new version.

Gradually shifts customer traffic to the new version until you're satisfied that it's working as expected. If an update doesn't work correctly, you can roll back the changes.

Defines pre-traffic and post-traffic test functions to verify that the newly deployed code is configured correctly and that your application operates as expected.

Automatically rolls back the deployment if CloudWatch alarms are triggered.

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: B

AWS Serverless Application Model (SAM)
upvoted 1 times

✉ **spencer_sharp** 1 year, 3 months ago

Selected Answer: B

sam typical use case
upvoted 3 times

✉ **masetromain** 1 year, 3 months ago

Selected Answer: B

AWS CodeDeploy is intended for this kind of use
<https://aws.amazon.com/fr/codedeploy/>
upvoted 2 times

✉ **masetromain** 1 year, 3 months ago

<https://www.examtopics.com/discussions/amazon/view/5158-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 1 times

Question #20

Topic 1

A company is planning to store a large number of archived documents and make the documents available to employees through the corporate intranet. Employees will access the system by connecting through a client VPN service that is attached to a VPC. The data must not be accessible to the public.

The documents that the company is storing are copies of data that is held on physical media elsewhere. The number of requests will be low. Availability and speed of retrieval are not concerns of the company.

Which solution will meet these requirements at the LOWEST cost?

- A. Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.
- B. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic File System (Amazon EFS) file system to store the archived data in the EFS One Zone-Infrequent Access (EFS One Zone-IA) storage class. Configure the instance security groups to allow access only from private networks.
- C. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic Block Store (Amazon EBS) volume to store the archived data. Use the Cold HDD (sc1) volume type. Configure the instance security groups to allow access only from private networks.
- D. Create an Amazon S3 bucket. Configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default. Configure the S3 bucket for website hosting. Create an S3 interface endpoint. Configure the S3 bucket to allow access only through that endpoint.

Correct Answer: D*Community vote distribution*

tman22 Highly Voted 1 year, 3 months ago

A - Glacier Deep Archive can't be used for web hosting, regardless if the company says retrieval time is no concern.

upvoted 31 times

tman22 1 year, 3 months ago

Nevermind, I go for D.

It should be technically possible - and mostly dependent on the intranet web application logic - It could present users with the ability to start file retrieval, for then to later access the data.

upvoted 14 times

zhangyu20000 Highly Voted 1 year, 3 months ago

A is correct. HA is not required here.

D use Glacier deep archive that need hours to access that will cause time out for web

upvoted 19 times

TonytheTiger Most Recent 1 week, 1 day ago

Selected Answer: D

Option D: 2 major points for the company. 1. Availability and speed of retrieval are NOT concerns of the company. 2. Meets these requirements at the LOWEST cost. Only S3 Glacier Deep Archive gives the company those requirement. The question doesn't state how fast the employees need to access the files but the company does, see point 1. S3 Glacier Deep Archive is the lowest-cost storage option in AWS. Standard-IA and S3 One Zone-IA objects are available for millisecond access

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

upvoted 1 times

Smart 1 week, 4 days ago

Selected Answer: A

Objects in Glacier Deep Archive needs to be 'restored'. A click on simple static website will not make AWS API call to restore the object and make it available.

upvoted 1 times

red_panda 3 weeks ago

Selected Answer: A

For me is A.

I'm not sure that S3 Glacier Deep Archive can be used as website. Also more than 12 hours to retrieve is so much for document systems (also if is not a concern the speed up).

Going with A

upvoted 1 times

MoTOne 3 weeks, 6 days ago

Selected Answer: D

LOWEST cost when compared with A
upvoted 1 times

 **a54b16f** 2 months ago

Selected Answer: A

pay attention to "copies of data that is held on physical media elsewhere", this is hint for one zone. Using Glacier is possible in theory, but won't work out of box. Need to develop a whole new application to submit unarchive request when user request a file, wait for up to 48 hour, create the s3 link, notify the user and ask user to come back to view the file. This is ANOTHER application

upvoted 6 times

 **24Gel** 3 weeks, 6 days ago

I agree, "copies of data that is held on physical media elsewhere", this is hint for one zone,

However, it could be multiple zone as well.

Availability and speed of retrieval are not concerns of the company.

So I go with D

upvoted 1 times

 **kz407** 3 weeks, 4 days ago

This! It's also worth mentioning that, the application we have to develop for option D, will be very difficult, if not impossible to be hosted in S3, because it will be a stateful application.

upvoted 1 times

 **gustori99** 2 months, 1 week ago

B and C does not make sense.

BUT A and D also contains nonsense information. It is not possible to configure a bucket to use S3 One Zone-IA storage class or Glacier storage class as default. You can only specify a different storage class during upload. Also configuring bucket for website hosting does not make sense because a website endpoint is only accessible from the public internet (if the bucket policy allows it) and it is not supported for interface endpoint.

upvoted 1 times

 **gustori99** 2 months, 1 week ago

B and C does not make sense.

BUT A and B also contains nonsense information. It is not possible to configure a bucket to use S3 One Zone-IA storage class or Glacier storage class as default. Standard storage class is always default and cannot be changed. You can only specify a different storage class during upload. Also lifecycle policy cannot help because it allows transition to S3 One-Zone-IA only after 30 days. Configuring bucket for website hosting does not make sense because a website endpoint is only accessible from the public internet (if the bucket policy allows it) and it is not supported for interface endpoint.

upvoted 1 times

 **liux99** 3 months, 1 week ago

Confusion here is A and D. D is cheaper but is not viable. You cannot use S3 bucket of Deep Glacier class for web hosting.

upvoted 2 times

 **24Gel** 3 weeks, 6 days ago

this should not be a concern here.

You cannot create a deep archive bucket, when you create a bucket, you either create a normal bucket or a single zone bucket, then you can configure it to use deep archive in it.

upvoted 1 times

 **Jay_2pt0_1** 3 months, 2 weeks ago

I think I'll go for A when I take the exam, but, like most people, I'm on the fence.

upvoted 2 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: A

Option A - This option will work and S3 One Zone is a cheap storage solution for a large number of documents

Option B - This option might not work: Nothing is said in the question about whether the Client VPN is connecting to a private subnet. Moreover, EFS might not be a cheap storage solution for a large number of documents

Option C - This option might not work: Nothing is said in the question about whether the Client VPN is connecting to a private subnet. Moreover, EBS Cold HDD might not be a cheap storage solution for a large number of documents

Option D - This option will not work: S3 Deep Glacier Vaults cannot be configured for static hosting. You would need to write an application for accessing the archives.

upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Selected Answer: D

In the exam I would go for D, but both A and D have an issue: you do not need to enable static website hosting on the bucket, as this is only for public website endpoints. However, having static website hosting enabled doesn't prevent you from access the bucket using API.

See <https://aws.amazon.com/blogs/networking-and-content-delivery/hosting-internal-https-static-websites-with-alb-s3-and-private-link/#:~:text=You%20do%20not%20need%20to%20enable%20static%20website%20hosting%20on%20the%20bucket%2C%20as%20this%20is%20only%20for%20public%20website%20endpoints.%20Requests%20to%20the%20bucket%20will%20be%20going%20through%20a%20private%20REST%20API%20instead.>

upvoted 1 times

✉ **924641e** 3 months, 4 weeks ago

Tricky but answer D would provide the LOWEST cost vs answer A. Answer A would be the best design balance between cost and use for end-users.

upvoted 1 times

✉ **ixdb** 3 months, 4 weeks ago

Selected Answer: D

S3 bucket does not support to set a default storage class. You can create lifecycle rule with Day 0 to move to Glactier deep archive class and enable web hosting. You can do it on aws console.

upvoted 1 times

✉ **kmstan** 4 months ago

Selected Answer: A

D is out because "To retrieve data stored in S3 Glacier Deep Archive, initiate a "Restore" request using the Amazon S3 APIs or the Amazon S3 Management Console."

upvoted 2 times

✉ **shaaam80** 4 months, 1 week ago

Selected Answer: A

Answer A.

B and C are not relevant.

D is close to create confusion but can't be used as an option for 2 reasons:

1. You can't create a S3 bucket with Glacier deep archive as a default storage class. Need lifecycle transition from any other S3 classes.
2. S3 Glacier deep archive can't be used for website hosting.

upvoted 1 times

✉ **_Jassybang_** 2 months ago

1 You can create - read here <https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

2> Yes you are correct on this - So will go with answer A too..

upvoted 1 times

Question #21

Topic 1

A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company's AWS accounts, which are using AWS Organizations. AWS Site-to-Site VPN connectivity already exists between the on-premises environment and all the company's AWS accounts.

The company's security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location.

Which solution will meet these requirements?

- A. Configure AWS IAM Identity Center (AWS Single Sign-On) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using attribute-based access controls (ABACs).
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) by using IAM Identity Center as an identity source. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using IAM Identity Center permission sets.
- C. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provider. Provision IAM users that are mapped to the federated users. Grant access that corresponds to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM users.
- D. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provider. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM roles.

Correct Answer: D*Community vote distribution*

masetromain Highly Voted 1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/74174-exam-aws-certified-solutions-architect-professional-topic-1/>

Both option C and option A are valid solutions that meet the requirements for the scenario.

ABAC, or attribute-based access control, is a method of granting access to resources based on the attributes of the user, the resource, and the action. This allows for fine-grained access control, which can be useful for implementing a security policy that requires conditional access to the accounts based on user groups and roles.

AWS IAM Identity Center (AWS SSO) allows you to connect to your on-premises Active Directory service using SAML 2.0. With this, you can enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol, which allows for the management of user identities in a single location.

upvoted 25 times

masetromain 1 year, 2 months ago

In option C, the company will use IAM to use a SAML 2.0 identity provider, and it will use the appropriate groups in Active Directory to grant access to the required AWS accounts by using cross-account IAM users. In this way, it can implement its security policy of conditional access to the accounts based on user groups and roles.

In summary, both option A and C are valid solutions, both of them allow you to use your on-premises Active Directory service for user authentication, and both of them allow you to manage user identities in a single location and grant access to the AWS accounts based on user groups and roles.

upvoted 2 times

bititan Highly Voted 1 year, 2 months ago

Selected Answer: A

A is has options for SAML and SCIM configuration with AD

C is all about users and no roles are mentioned. AD User attributes cannot be mapped to IAM users direct

D is openID based, MS AD would not support this

so I go with A

upvoted 12 times

trap 4 months, 4 weeks ago

native AD doesn't support SAML 2.0 without an ADFS server. SCIM is also not supported at all. SCIM provisioning is supported by other IDPs like Azure AD

upvoted 3 times

✉ **gonzjo52** 2 days, 6 hours ago

Si, si son compatibles. <https://aws.amazon.com/es/directoryservice/faqs/>
upvoted 1 times

✉ **trap** 4 months, 4 weeks ago

<https://docs.aws.amazon.com/singlesignon/latest/userguide/supported-idps.html>
upvoted 2 times

✉ **Vaibs099** **Most Recent** 2 months, 2 weeks ago

A is correct

Reasons -

Option A mentions about Active Directory as identity Source configuration which solves the purpose of establishing trust and sync from on-prem AD using Directory Service. Solves the purpose of using on-prem AD as Single Sign On asked in the question.

It is also mentioned that AWS org is in place, which works well with AWS Identity Centre. Gives another validation. It gives us hint of efficiently managing AWS Org accounts / OUs with Identity Centre (Permission Set behind the scene) to manage RBAC within accounts.

Finally this line - "The company's security policy requires conditional access to the accounts based on user groups and roles." is talking about conditional access which can only be solved by ABAC(Attribute Based Access Control). For example user with green attribute should only get access to resources with green attribute. This can be solved by Tag functionality within AWS Identity Centre.

upvoted 1 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: D

Option A - This option works however it moves authentication and managing user identities from Active Directory to Identity Center but the question states the company wants to use the same authentication service to sign into AWS in reference to Active Directory

Option B - This option works but it moves user identity management and authentication tie Identity Center which is not what the question states the company wants to do

Option C - This option does not work because in AWS you provision cross-account IAM roles rather than users.

Option D - This option might work but it is missing AD FS, a component that enables OIDC flows in AD. Otherwise it maintains user identity management in one place and allows the company to keep using Active Directory for authentication as the question states

upvoted 2 times

✉ **ninomfr64** 3 months, 3 weeks ago

Selected Answer: B

Didn't spent time checking if C and D works, because when you have an AWS Organization and need to use AD to sign-in to the company's AWS accounts AWS IdC is the way to go.

Now, with AWS IdC we need ADFS and while ADFS does not support SCIM, it is possible to still have your users and groups automatically synchronize with the IAM IDC by using the SCIM API and PowerShell as per <https://aws.amazon.com/blogs/modernizing-with-aws/synchronize-active-directory-users-to-aws-iam-identity-center-using-scim-and-powershell/#:~:text=While%20ADFS%20does%20not%20support,the%20SCIM%20API%20and%20PowerShell>.

Finally, ABAC is an authorization strategy and it is not alternative to IdC Permission Sets. Also the scenario requires conditional access to the accounts based on user groups and roles, this point me to RBAC strategy. I would pick ABAC if the request mentioned user attributes like Department, Cost Center or Project thus.

upvoted 2 times

✉ **ninomfr64** 2 months, 1 week ago

After reviewing it, the correct answer is A. "User identities must be managed in a single location" -> "Configure AWS IAM Identity Center (AWS Single Sign-On) to connect to Active Directory by using SAML 2.0" while B states "Configure AWS IAM Identity Center (AWS Single Sign-On) by using IAM Identity Center as an identity source". Using AWS IdC as identity source will not meet requirement to manage all users in a single place

upvoted 1 times

✉ **924641e** 3 months, 4 weeks ago

Answer A for AWS SSO would be the right answer at first glance since IAM roles can be mapped to AD groups but it would require additional AD functions like ADFS for SCIM so the next best option is D.

upvoted 3 times

✉ **subupro** 4 months ago

A is a correct one, because need to use the SAML for single sign on from the on-premise directory and also C is not correct because the federated should not come in to the picture federated is for only facebook, twitter, gmail account sign on - but we should use the company's active directory, so A is a correct one.

upvoted 1 times

✉ **siasiasia** 4 months, 2 weeks ago

Selected Answer: C

AD and SCIM don't go together so forget A and B. I've never seen a document talking about integrating OpenID with AWS account login so D is also out. C is doable so I go with C.

upvoted 1 times

✉  **gonzjo52** 2 days, 6 hours ago

P: ¿Puedo usar la autenticación basada en lenguaje de marcado de aserción de seguridad (SAML) 2.0 con aplicaciones de la nube que usen AWS Managed Microsoft AD?

Sí. Puede usar los servicios federados de Microsoft Active Directory (AD FS) para Windows 2016 con su dominio administrado de AWS Managed Microsoft AD para autenticar usuarios en aplicaciones en la nube compatibles con SAML.

<https://aws.amazon.com/es/directoryservice/faqs/>

upvoted 1 times

✉  **sizzla83** 4 months, 2 weeks ago

I am with B on this one. A is incorrect because you can only use ABAC (Attribute-Based Access Control) with IAM Identity Center Identity Store NOT with Active Directory

upvoted 1 times

✉  **ninomfr64** 3 months, 3 weeks ago

Agree with you on B, but:

- You can use IAM Identity Center to manage access to your AWS resources across multiple AWS accounts using user attributes that come from any IAM Identity Center identity source - <https://docs.aws.amazon.com/singlesignon/latest/userguide/abac.html>

- ABAC is an authorization strategy that defines permissions based on attributes and it is implemented using IdC Permission Sets.

upvoted 1 times

✉  **enk** 4 months, 2 weeks ago

Selected Answer: A

As mentioned, SAML 2.0 doesn't directly integrate with AD and requires ADFS proxy as a go between, so the lack of ADFS being mentioned in A or B is throwing people off. However, AD on-premise with direct/VPN connectivity...IAM identify center is the way to go for SSO. I believe ADFS is implied when the question casually mentions "IAM Identify Center connect to AD using SAML 2.0".

upvoted 1 times

✉  **severlight** 4 months, 4 weeks ago

Selected Answer: A

federated IdP is required and access to multiple accounts

upvoted 1 times

✉  **trap** 5 months ago

Answer A and B are wrong!!!

Active Directory doesn't support SAML without the use of Active Directory Federation Server!! SCIM is also not supported. The articles that all are pasting here mention the need of an AD connect or the trust between the local AD and an AWS managed Microsoft AD which is not the case here.

C is also wrong. Cross account IAM users option doesn't exist.

The correct is D!! You can use an OpenID Connect (OIDC) identity provider (e.g OKTA or Azure AD) and sync AD groups in it. You can then use cross account roles to grant access to the federated users

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_oidc.html

<https://help.okta.com/en-us/content/topics/directory/ad-agent-manage-users-groups.htm>

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html

upvoted 3 times

✉  **M4D3V1L** 6 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/singlesignon/latest/userguide/onelogin-idp.html#onelogin-passing-abac>

upvoted 1 times

✉  **imvb88** 6 months, 1 week ago

Selected Answer: A

A: combination SSO + SAML2.0 + AD sounds correct. Automatic provisioning with SCIM means creating users and groups that synced with AD. ABAC seems not too fit for this as the requirements is "requires conditional access to the accounts based on user groups and roles" but that already satisfied with SCIM.

B: "use Identity Center as an identity source" -> not using on premise AD -> wrong

D: use OIDC -> wrong as on premise AD does not support OIDC. Cannot find an exact source for this but ChatGpt says so..

C: creating users mapped to federated users sounds red flags. Could have been correct if it was "creating roles", the same way with the classic "creating roles for EC2 to access S3 instead of user..."

Conclusion: A

upvoted 3 times

✉  **whenthan** 7 months, 1 week ago

Selected Answer: C

More comprehensive approach

how to map users, grant access based on groups, and utilize cross-account IAM users.

upvoted 2 times

✉  **whenthan** 7 months, 1 week ago

C provides more comprehensive approach

upvoted 1 times

 **bur4an** 7 months, 1 week ago

Selected Answer: A

A. Configure AWS IAM Identity Center (AWS Single Sign-On) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using attribute-based access controls (ABACs).

Option B does not mention the use of SAML integration with Active Directory, which is needed for the company's requirement of using the existing Active Directory for user authentication.

Option C involves managing cross-account IAM users, which can be more complex and less centralized compared to using a dedicated identity service like AWS SSO.

Option D involves OpenID Connect (OIDC), which is not mentioned as a requirement, and using cross-account IAM roles. While IAM roles are a valid way to grant access, the solution provided in option A offers a more centralized and streamlined approach through AWS SSO.

upvoted 1 times

Question #22

Topic 1

A software company has deployed an application that consumes a REST API by using Amazon API Gateway, AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the PUT calls come from a small number of clients that are authenticated with specific API keys.

A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation.

What should the solutions architect recommend to improve the customer experience?

- A. Implement retry logic with exponential backoff and irregular variation in the client application. Ensure that the errors are caught and handled with descriptive error messages.
- B. Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.
- C. Turn on API caching to enhance responsiveness for the production stage. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload.
- D. Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic.

Correct Answer: B

Community vote distribution

B (71%)

A (27%)

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: B

API throttling is a technique that can be used to control the rate of requests to an API. This can be useful in situations where a small number of clients are making a large number of requests, which is causing errors. By implementing API throttling through a usage plan at the API Gateway level, the solutions architect can limit the number of requests that a client can make, which will help to reduce the number of errors.

It's important that the client application handles the code 429 replies without error, this will help to improve the customer experience by reducing the number of errors that are displayed to customers. Additionally, it will prevent the API's reputation from being damaged by the errors.

upvoted 38 times

 **masetromain** 1 year, 2 months ago

It is important to note that other solutions such as retry logic with exponential backoff and irregular variation in the client application or turn on API caching to enhance responsiveness for the production stage may help to improve the customer experience and reduce errors, but they do not address the root cause of the problem which is a large number of requests coming from a small number of clients.

Implementing reserved concurrency at the Lambda function level can provide resources that are needed during sudden increases in traffic, but it does not address the issue of a client making a large number of requests and causing errors.

upvoted 14 times

 **zhangyu20000** Highly Voted 1 year, 3 months ago

B is correct. API gateway throttling is applied to single account - <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html>. Retry will make it even worse.

upvoted 8 times

 **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: B

B. C only will help with GET requests, and A and D don't prevent it

upvoted 1 times

 **anubha.agrahari** 1 month ago

Selected Answer: B

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

upvoted 1 times

 **duriselvan** 1 month, 3 weeks ago

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

upvoted 1 times

 **AimarLeo** 2 months ago

This question missing MASSIVE information.. none of the answers can fulfil the requirements..

upvoted 1 times

 **bjexamprep** 2 months, 3 weeks ago

Selected Answer: A

There is no evidence indicating the problem is with the throughput. If it is throughput, other clients will have similar problem. And “the errors are displayed to customers and are causing damage to the API’s reputation.”, this means the solution should be able to reduce the error message showed on the client side, while, throttling the client will actually close the service for this particular client, which is against the “clients can tolerate retries of unsuccessful calls”.

I vote A for this question.

upvoted 1 times

 **sarfraz_khan** 3 months, 3 weeks ago

The solutions architect should recommend option B: Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.

Option B is the most directly related recommendation to improving the customer experience, as it addresses the issue of API rate limiting and ensures a more predictable and controlled experience for users.

upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This option will make retries take longer on each retry for all clients rather than for the few causing issues in the application

Option B - This option will work: An usage plan will allow throttling requests from specific clients identified by their API Key and ensuring client applications can handle throttling errors provides a consistent experience

Option C - This option has no relation with the problem at hand

Option D - This option assumes there is a capacity issue managing the increase in volumes but given that errors occur due to a small number of clients then reserved concurrency will not address the cause of the issue

upvoted 2 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: B

Option A - This option will make retries take longer on each retry for all clients rather than for the few causing issues in the application

Option B - This option will work: An usage plan will allow throttling requests from specific clients identified by their API Key and ensuring client applications can handle throttling errors provides a consistent experience

Option C - This option has no relation with the problem at hand

Option D - This option assumes there is a capacity issue managing the increase in volumes but given that errors occur due to a small number of clients then reserved concurrency will not address the cause of the issue

upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Selected Answer: B

Usage Plan throttling prevents a group of users or a single user to saturate the API concurrency capacity. Thus B. Also A and D can help in this scenario, but they will have less benefit with respect to B. While C does not help in this scenario as I do not see how API Gateway caching can help PUT requests

upvoted 1 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: B

obvious

upvoted 1 times

 **whenthan** 7 months, 1 week ago

Selected Answer: B

Implementing API throttling through a usage plan at the API Gateway level would directly address the issue of too many requests from a single client causing errors. Properly handling status code 429 can help clients understand the situation, and throttling ensures fair usage and prevents overload, ultimately improving the customer experience.

upvoted 1 times

 **bur4an** 7 months, 1 week ago

Selected Answer: B

B. Implement API throttling through a usage plan at the API Gateway level. Ensure that the client application handles code 429 replies without error.

Options A and D might help with general improvements in resilience and resource allocation, but they do not specifically address the issue of a single client causing a large number of errors.

Option C, involving API caching, is not the most appropriate solution in this scenario, as caching might not directly address the issue of the client generating a high volume of errors. It might improve responsiveness for frequently accessed data, but it doesn't directly address the issue of client errors.

upvoted 2 times

 **CloudHandsOn** 7 months, 3 weeks ago

Selected Answer: B

B. The error message is damaging the reputation, which is the icing on the cake when deciding between A and B. One option continues to show an error, which will continue to damage the reputation. Option A will not show an error to the end user, and will handle the issue.

upvoted 1 times

 **CloudHandsOn** 7 months, 3 weeks ago

CORRECTION - "Option B will not show an error.."

upvoted 1 times

 **chico2023** 8 months, 1 week ago

Selected Answer: B

Answer: B

It's not clear what error customers are getting. We can guess, however, that it is related to throttling: "A solutions architect has identified that a large number of the PUT requests originate from one client."

The usual way to handle throttling is by using an exponential backoff technique, which answer A, however, if I want to avoid, or limit throttling to all clients and improve the reputation of my API, I would go with answer B, which limits calls, impacting only the culprits and, also handles 429 without error (which makes me assume that my application will catch the error and will retry).

upvoted 1 times

 **Piccaso** 8 months, 1 week ago

Selected Answer: B

code 429 means "Too many requests"

upvoted 2 times

Question #23

Topic 1

A company is running a data-intensive application on AWS. The application runs on a cluster of hundreds of Amazon EC2 instances. A shared file system also runs on several EC2 instances that store 200 TB of data. The application reads and modifies the data on the shared file system and generates a report. The job runs once monthly, reads a subset of the files from the shared file system, and takes about 72 hours to complete. The compute instances scale in an Auto Scaling group, but the instances that host the shared file system run continuously. The compute and storage instances are all in the same AWS Region.

A solutions architect needs to reduce costs by replacing the shared file system instances. The file system must provide high performance access to the needed data for the duration of the 72-hour run.

Which solution will provide the LARGEST overall cost reduction while meeting these requirements?

- A. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.
- B. Migrate the data from the existing shared file system to a large Amazon Elastic Block Store (Amazon EBS) volume with Multi-Attach enabled. Attach the EBS volume to each of the instances by using a user data script in the Auto Scaling group launch template. Use the EBS volume as the shared storage for the duration of the job. Detach the EBS volume when the job is complete
- C. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using batch loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.
- D. Migrate the data from the existing shared file system to an Amazon S3 bucket. Before the job runs each month, use AWS Storage Gateway to create a file gateway with the data from Amazon S3. Use the file gateway as the shared storage for the job. Delete the file gateway when the job is complete.

Correct Answer: D

Community vote distribution

A (87%)

13%

✉  **sambb**  1 year, 1 month ago

Selected Answer: A

- A: Lazy loading is cost-effective because only a subset of data is used at every job
 B: There are hundreds of EC2 instances using the volume which is not possible (one EBS volume is limited to 16 nitro instances attached)
 C: Batching would load too much data
 D: storage gateway is used for on premises data access, I don't know if you can install a gateway in AWS, but Amazon would never advise this
 upvoted 17 times

✉  **b3llman** 8 months ago

file storage gateway can be installed on EC2 and it is exactly used for accessing S3 from EC2 as a file system
 upvoted 1 times

✉  **Chainshark** 6 months ago

It's used a lot, I've used it for customers to access and analyze data imported via Snowball from Windows machines.
 upvoted 1 times

✉  **dqwsrnwwvtgxwkgvcv** 7 months, 3 weeks ago

There is one S3 file gateway

<https://aws.amazon.com/storagegateway/file/s3/>

upvoted 1 times

✉  **Tofu13** 6 months, 2 weeks ago

<https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>
 upvoted 2 times

✉  **chico2023**  8 months, 1 week ago

Answer: D

I think the main point here is to understand what they mean by "The file system must provide high performance access to the needed data" while "provide the LARGEST overall cost reduction"?

For answer A, we have to remember that lazy load is SLOW for the first time you try to access the file (as it is being fetched from S3), BUT, as we are talking about hundreds of instances, then it might be OK. S3 Intelligent-Tiering, although doesn't seem to fit much, the part that says "The job runs once monthly, reads a subset of the files from the shared file system", indicates that at least part of the 200TB of data won't be accessed,

which helps not going for answer C, for example.

My only issue with answer D is that Storage Gateway can be slower than FSx for Lustre, HOWEVER, what is the cost X performance ratio they are seeking here? We can guess that costs trumps maximum performance here: "Which solution will provide the LARGEST overall cost reduction" and, as Storage Gateway is way cheaper than FSx for Lustre per TB, it's safe to say that D is the most correct answer.

upvoted 10 times

 **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: A

A: Lazy loading is cost-effective because only a subset of data is used at every job

upvoted 1 times

 **kz407** 3 weeks, 3 days ago

Selected Answer: A

Problem with D is that, AWS Storage GW and File GW are solutions for integrating on-premise storage with AWS storage solutions, particularly (but not limited to) S3.

<https://aws.amazon.com/storagegateway/>
<https://aws.amazon.com/storagegateway/file/>

Compute resources are residing in AWS, so having Storage GW and File GW won't solve a thing.

As far as option B is concerned, it comes down to the limitations of EBS (such as the max block size, and max number of instance that can be attached etc). Also, attaching and detaching of the EBS volumes seems a bit complicated too. On top of that, EBS does not offer the cost optimizations offered by S3 Intelligent Tiering. The question clearly mentions that only a subset of the data will be used. Intelligent tiering ensures a substantial cost optimization over time.

Hence, the answer should be A.

upvoted 1 times

 **kspendli** 3 weeks, 6 days ago

Option D, migrating the data to an Amazon S3 bucket and using AWS Storage Gateway, seems to provide the largest overall cost reduction while meeting the requirements of high-performance access during the job run and minimizing costs when the storage is not actively being used. Therefore, Option D is the most suitable choice.

upvoted 1 times

 **anubha.agrahari** 1 month ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/new-enhancements-for-moving-data-between-amazon-fsx-for-lustre-and-amazon-s3/>

upvoted 2 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: A

Option A - This option might work. However, AWS FSx for Lustre does not have a feature called "lazy loading" - its default behavior is to load a file from S3 when it is first accessed (restore). It can provide high-performance as needed though nothing is said in the question about whether a slow initial load time due to restore operations could be an issue. S3 Intelligent-Tiering minimizes storage costs.

Option B - This option will provide a high-performance storage option. However, storage in EBS is expensive compared to other AWS storage services

Option C - This option might work. However, AWS FSx for Lustre does not have a feature called "batch loading". Files can be pre-loaded issuing a hsm-restore command. S3 Standard is a cheap storage option yet not the cheapest option in S3

Option D - This option does not work as described in the option

upvoted 2 times

 **AimarLeo** 2 months, 1 week ago

Actually AWS FSx for Lustre does not have a direct feature 'Lazy loading' but the question is the support of that when Amazon FSx will import the objects in our S3 bucket as files, and "lazy-load" the file contents from S3 when first access the files.. Any data processing job on Lustre with S3 as an input data source can be started without Lustre doing a full download of the dataset

first - Data is lazy loaded: only the data that is actually processed is loaded, meaning you can decrease your costs and latency

upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Not B because using EBS still involves EC2 instances that are expensive (the instances that host the shared file system run continuously). Also, multi-attach is supported only for io1/oi2 EBS disk types that are expensive;

Not C as batch loading does not exist in the doc/console, I think they might refer to the option to pre-populate the data using lfs hsm_restore command as mentioned here <https://docs.aws.amazon.com/fsx/latest/LustreGuide/preload-file-contents-hsm-dra.html>. This would be a more expensive option

Not D as Storage Gateway provides less performance than FSx for Lustre and it requires at least an EC2 instance and this will introduce additional cost

AA is a viable option as S3 is cheaper storage, FSx for Lustre provides performance. Lazy loading allows to actually move in the filesystem data that is actually used and intelligent tiering make sure those files that are not used are moved to less expensive S3 storage tiers.

upvoted 1 times

 **subupro** 4 months ago

Intelligent tiering is not required, because the job would be running for every month, so there is no purpose for intelligent tiering. The question is having cost impact also one of the option. So go with option D.

upvoted 1 times

 **e4bc18e** 1 month ago

"Only a subset of data is accessed each run" So that means after 30 days data can tier down so yes there is cost savings in using INT
upvoted 1 times

 **Japanese1** 5 months, 1 week ago

Selected Answer: D

Functional requirements should be met before non-functional requirements.

In the first place, only option D allows the application to change the data in the shared file during the monthly job execution. With options A and C, data changes made during the job are discarded after the job runs.

On top of that, although D is inferior to A in performance, it meets the requirements because it is the cheapest.

upvoted 4 times

 **kz407** 3 weeks, 5 days ago

You can configure a DRA for automatic import only, for automatic export only, or for both. "A data repository association configured with both automatic import and automatic export propagates data in both directions between the file system and the linked S3 bucket. As you make changes to data in your S3 data repository, FSx for Lustre detects the changes and then automatically imports the changes to your file system. As you create, modify, or delete files, FSx for Lustre automatically exports the changes to Amazon S3 asynchronously once your application finishes modifying the file."

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/create-dra-linked-data-repo.html>

upvoted 1 times

 **grire974** 3 months ago

Oh yeh - of course; if you delete the FSx volume; the changes are lost.

upvoted 1 times

 **bur4an** 7 months, 1 week ago

Selected Answer: A

A. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Intelligent-Tiering storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using lazy loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.

Option B (using Amazon EBS) would result in higher costs due to the continuous usage of large EBS volumes. Similarly, option C involves creating a new FSx for Lustre file system with batch loading, which may not be as cost-effective as lazy loading.

Option D (using AWS Storage Gateway) would involve additional complexity and potentially higher costs compared to directly utilizing S3 and FSx for Lustre.

upvoted 1 times

 **dqwsmwwvtgxwkvgcvc** 7 months, 3 weeks ago

Selected Answer: D

@chico already explain the logic behind, @sambb chose A because S3 file gateway wasn't clear to him

upvoted 1 times

 **chiajy** 8 months, 2 weeks ago

Question mentioned "The file system must provide high performance access to the needed data for the duration of the 72-hour run." Assuming S3 Intelligent-Tiering don't move data into Archive Access tiers(which are optional) [Ref: docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html] . Thus, need to ensure data is always in storage tiers that provide "low latency and high throughput performance.". As S3 Intelligent-Tiering delivers automatic storage cost savings, Answer A can be the potential answer.

upvoted 1 times

 **waoo** 8 months, 2 weeks ago

A一定是错的，因为数据都是不常访问的，如果放到s3的智能存储中，会默认变成冷数据，再被访问时，需要重新激活，需要付出很高的成本
upvoted 2 times

 **Asamara** 9 months, 1 week ago

ption C. Migrate the data from the existing shared file system to an Amazon S3 bucket that uses the S3 Standard storage class. Before the job runs each month, use Amazon FSx for Lustre to create a new file system with the data from Amazon S3 by using batch loading. Use the new file system as the shared storage for the duration of the job. Delete the file system when the job is complete.

upvoted 1 times

 **rxhan** 9 months, 1 week ago

Selected Answer: A

A benefit of FSx for Lustre.

Integrates seamlessly with Amazon S3 (connect your S3 data sets to your FSx for Lustre file system, run your analyses, write results back to S3, and delete your file system) ...

upvoted 2 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: A

A?

C would load unneeded data.

The only potential issue with A is that lazy loading may impact high performance access, which is also requirement

upvoted 1 times

Question #24

Topic 1

A company is developing a new service that will be accessed using TCP on a static port. A solutions architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name my.service.com, which is publicly accessible. The service must use fixed address assignments so other companies can add the addresses to their allow lists. Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?

- A. Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer (NLB) and expose the static TCP port. Register EC2 instances with the NLB. Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.
- B. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer (NLB) and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.
- C. Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone. Create a Network Load Balancer (NLB) and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB. Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set.
- D. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster. Create an Application Load Balancer (ALB) and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

Correct Answer: C

Community vote distribution

C (100%)

 **God_Is_Love**  1 year, 1 month ago

Logical answer : Non http port like TCP should hint to NLB immediately.(ALB does not fit here) Sharing IP address of EC2 is not apt whether it is from individual EC2 instances or those from ECS cluster.this eliminates A,B,D, infact the NLB's address which stays in front of / associates to ec2 instances need to be shared. So, only solution is C

upvoted 9 times

 **masetromain**  1 year, 2 months ago

Selected Answer: C

A more appropriate solution would be option C. Create an Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone. Create a Network Load Balancer (NLB) and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB. Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set. As it uses the NLB as the resource in the A-record, traffic will be routed through the NLB, and it will automatically route the traffic to the healthy instances based on the health checks and also it provides the fixed address assignments as the other companies can add the NLB's Elastic IP addresses to their allow lists.

upvoted 5 times

 **gofavad926**  3 weeks, 3 days ago

Selected Answer: C

C: NLB with elastic IPs

upvoted 1 times

 **mosotaw39** 1 month, 2 weeks ago

The practice questions on ITEXAMSLAB helped me to better prepare for the SAP-C02 exam: <https://www.itexamslab.com/amazon/sap-c02-dumps.html>

upvoted 1 times

 **Vaibs099** 2 months, 1 week ago

C is the right answer - Few key points - TCP static Port (go with NLB), IP Whitelisting required which can only be done with NLB. ALB doesn't support static IPs. And sharing Static (Elastic) IPs of instances of no use when using NLB. We need to share NLB Elastic IPs from Multi AZs and create DNS record for NLB Domain Name to Domain entry.

upvoted 1 times

 **sammyhaj** 3 months ago

<https://repost.aws/knowledge-center/elb-attach-elastic-ip-to-public-nlb>

upvoted 1 times

Simon523 7 months, 1 week ago

Selected Answer: C

Other option haven't mention multi AZ

upvoted 1 times

Christina666 9 months, 1 week ago

Selected Answer: C

Static IP-> NLB

upvoted 1 times

NikkyDicky 9 months, 2 weeks ago

Selected Answer: C

I suppose C, although you can't do this with A record, only alias

upvoted 1 times

GilbertJorge 9 months, 3 weeks ago

If you are preparing for the AWS SAP-C02 exam, I recommend studying the official AWS certification guide, attending training courses, gaining hands-on experience with AWS services, utilizing practice exams, and seeking additional study resources specifically designed for the AWS Solutions Architect - Professional certification.

"<https://www.passin1day.com/SAP-C02-dumps.html>

upvoted 1 times

SkyZeroZx 9 months, 3 weeks ago

Selected Answer: C

Create one Elastic IP address for each Availability Zone.

upvoted 2 times

AWS_Sam 11 months ago

C is the only option that talks about more than one AZ.

upvoted 1 times

mfsec 1 year ago

Selected Answer: C

Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone.

upvoted 2 times

kiran15789 1 year, 1 month ago

Selected Answer: C

IP address using NLB

upvoted 1 times

saurabh1805 1 year, 1 month ago

Selected Answer: C

C looks correct.

upvoted 2 times

zozza2023 1 year, 2 months ago

Selected Answer: C

C. NLB with one Elastic IP per AZ to handle TCP traffic. Alias record set named my.service.com.

<https://www.examtopics.com/discussions/amazon/view/28045-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

Musk 1 year, 2 months ago

Selected Answer: C

C looks correct. I did not read the rest.

upvoted 1 times

Question #25

Topic 1

A company uses an on-premises data analytics platform. The system is highly available in a fully redundant configuration across 12 servers in the company's data center.

The system runs scheduled jobs, both hourly and daily, in addition to one-time requests from users. Scheduled jobs can take between 20 minutes and 2 hours to finish running and have tight SLAs. The scheduled jobs account for 65% of the system usage. User jobs typically finish running in less than 5 minutes and have no SLA. The user jobs account for 35% of system usage. During system failures, scheduled jobs must continue to meet SLAs. However, user jobs can be delayed.

A solutions architect needs to move the system to Amazon EC2 instances and adopt a consumption-based model to reduce costs with no long-term commitments. The solution must maintain high availability and must not affect the SLAs.

Which solution will meet these requirements MOST cost-effectively?

- A. Split the 12 instances across two Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run four instances in each Availability Zone as Spot Instances.
- B. Split the 12 instances across three Availability Zones in the chosen AWS Region. In one of the Availability Zones, run all four instances as On-Demand Instances with Capacity Reservations. Run the remaining instances as Spot Instances.
- C. Split the 12 instances across three Availability Zones in the chosen AWS Region. Run two instances in each Availability Zone as On-Demand Instances with a Savings Plan. Run two instances in each Availability Zone as Spot Instances.
- D.** Split the 12 instances across three Availability Zones in the chosen AWS Region. Run three instances in each Availability Zone as On-Demand Instances with Capacity Reservations. Run one instance in each Availability Zone as a Spot Instance.

Correct Answer: C

Community vote distribution



lasco Highly Voted 1 year, 1 month ago

Selected Answer: D

Voted D because of the 65% / 35% proportion. C seems to be good but with only 50% instances available we break the SLA
upvoted 21 times

joefromnc Highly Voted 7 months, 2 weeks ago

Can not be C because Savings Plans requirement long term commitment.
upvoted 6 times

gofavad926 Most Recent 3 weeks, 3 days ago

Selected Answer: D

D is more cost-effective than C
upvoted 1 times

atirado 3 months, 3 weeks ago

Selected Answer: D

Option A - This option might not work: it might not provide sufficient processing capacity for the batch jobs to meet the SLAs during outages. Moreover, 4 servers will not provide sufficient capacity to meet the SLAs of batch jobs

Option B - This option might not work: In case of an outage affecting the On-Demand instances there might not be enough processing capacity to meet batch job SLAs

Option C - This option will not meet the requirement not to make any long-term commitments

Option D - This option will work: There is enough sufficient processing capacity to meet the SLAs of batch jobs and keep processing One-off jobs

upvoted 1 times

subupro 4 months ago

D would be perfect, because it requires more cpu usage, we should have more capacity CPU .
upvoted 1 times

edder 4 months, 2 weeks ago

Selected Answer: D

The answer is D.

Since it originally had a completely redundant configuration, it is thought that scheduled tasks are executed on 4 machines and user tasks are executed on 2 machines.

A,B: Requirements cannot be met when a specific region falls.

C: No Savings Plan required.

D: Even if a specific region goes down, 6 machines will be maintained, so service can be maintained.

upvoted 1 times

✉ **Russ99** 8 months, 1 week ago

Selected Answer: D

About 65% or about 8 instances have to run at the same time to meet the SLA.

upvoted 3 times

✉ **ggrodsckiy** 8 months, 1 week ago

Correct C.

Option D is incorrect because running three instances in each Availability Zone as On-Demand Instances with Capacity Reservations will increase the cost of the solution without providing any additional benefit. Capacity Reservations are not necessary when using a Savings Plan, as they both offer guaranteed capacity at a discounted price <https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/amazon-ec2.html>. Also, running only one instance in each Availability Zone as a Spot Instance will not provide enough capacity for the user jobs that account for 35% of system usage.

upvoted 4 times

✉ **joefromnc** 7 months, 2 weeks ago

Can't be C it says it can't require long term commitment. Savings plans like reserved instance require long term commitments with a contract.

upvoted 3 times

✉ **awsrd2023** 9 months, 1 week ago

Selected Answer: D

D. 3 AZ (Redundancy), 3 EC2 in each AZ as on demand and 1 spot (addresses SLA in 65/35 ratio)

Ruling out Factors:

- A. Only 2 AZ (low redundancy), all EC2 in capacity reservation (Not Cost effective as SLA requirement is in 65/35 ratio).
- B. All 4 on-demand in 1 AZ (low redundancy), rest spot (Will effect tight SLA - is actually 35/65 instead of 65/35).
- C. Savings Plan (Against no long term commitments requirement).

upvoted 3 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: D

D

- 1 - need capacity reservation
- 2 - need to cover 65% with HA

upvoted 1 times

✉ **aca1** 10 months, 3 weeks ago

Selected Answer: D

Just D is the right one. We need to guarantee 65% (about 8 instances of 12) of capacity for the SLA, so 9 can do it and then let the others as spot. Another point Saving Plans need commitment "Savings Plans are a flexible pricing model that offer low prices on Amazon EC2, AWS Lambda, and AWS Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term" - <https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 3 times

✉ **gameoflove** 11 months ago

Selected Answer: C

Voted C, the reason for this option is Spot Instance which is truly cost saving when we are performing Batch jobs and if you plan the cost properly this is best solution

upvoted 1 times

✉ **Maria2023** 11 months, 3 weeks ago

Selected Answer: D

65% SLA can be reached only on answer D. Yeah - 9 instances are a bit too much but that's the only answer that meets the SLA

upvoted 1 times

✉ **rxhan** 11 months, 3 weeks ago

Selected Answer: D

Option D splits the 12 instances across three AZs and runs three instances in each AZ as On-Demand Instances with Capacity Reservations, and one instance in each AZ as a Spot Instance. This option can provide better redundancy and capacity for scheduled jobs while still providing some cost savings through Spot Instances. Additionally, the user jobs can be easily absorbed by the available Spot Instances during On-Demand Instance failures.

upvoted 4 times

✉ **asifjanjua88** 1 year ago

Option C as per ChatGPT

upvoted 2 times

✉ **rxhan** 11 months, 3 weeks ago

ChatGPT gave me option D

upvoted 3 times

✉ **fig** 5 months, 1 week ago

This is proof that ChatGPT does make mistakes! Savings plans are 1 year or 3 year commitments. So C is incorrect.

upvoted 1 times

 **Amac1979** 1 year ago

Selected Answer: D

12 nodes in redundant configuration ..Means 6 nodes can handle load at any given time.

Out of 6 nodes, 65 % is SLA driven (~4nodes) and 35% load can be paused.

This lead to 4 nodes with single point of failure. D- If one -az down you still have 4 nodes available.

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: D

...Run one instance in each Availability Zone as a Spot Instance.

upvoted 2 times

Question #26

Topic 1

A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:

The database must use strong, randomly generated passwords stored in a secure AWS managed service.

The application resources must be deployed through AWS CloudFormation.

The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- B. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- C. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

Correct Answer: B

Community vote distribution

A (100%)

✉ **Untamables** Highly Voted 1 year, 3 months ago

Selected Answer: A

A

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/cloudformation.html>

Option B is wrong. The ParameterStore::RotationSchedule resource does not exist in CloudFormation.

Option C is wrong. It does not meet the requirement because it does not use CloudFormation.

Option D is wrong. The AWS::AppSync::DataSource resource is what to create data sources for resolvers in AWS AppSync to connect to.

upvoted 14 times

✉ **OnePunchExam** 1 year ago

Agree with A but I want to nitpick on this reply "The ParameterStore::RotationSchedule resource does not exist in CloudFormation". It is technically more correct to say ParameterStore does not support automated rotation of secrets instead of saying ParameterStore::RotationSchedule is not supported by CF.

upvoted 7 times

✉ **karma4moksha** Highly Voted 11 months ago

Ans A but answer is badly phrased. Why is the Lambda needed ?

Refer docs: Some services offer managed rotation, where the service configures and manages rotation for you. With managed rotation, you don't use an AWS Lambda function to update the secret and the credentials in the database. The following services offer managed rotation:

Amazon RDS offers managed rotation for master user credentials. For more information, see Password management with Amazon RDS and AWS Secrets Manager in the Amazon RDS User Guide.

upvoted 11 times

✉ **ftaws** 2 months, 3 weeks ago

I agree with you. Secret Manager support to rotate credentials.

upvoted 2 times

✉ **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: A

A is the correct answer

upvoted 1 times

✉ **8608f25** 2 months ago

Selected Answer: A

Option A is the most straightforward and provides the least amount of operational overhead because it leverages AWS Secrets Manager's native capabilities for secret rotation. This eliminates the need for custom rotation logic or external triggers for rotation, unlike the other options that

either rely on AWS Systems Manager Parameter Store (which does not have built-in secret rotation capabilities like Secrets Manager) or require additional resources such as Amazon EventBridge or AWS AppSync for triggering rotations, which complicates the architecture and increases operational overhead.

Therefore, Option A is the correct choice as it directly addresses all the specified requirements using the intended features of AWS services, ensuring security and efficiency with minimal operational complexity.

upvoted 1 times

✉ **AimarLeo** 2 months ago

OK.. A ..but.. lambda to rotate for Secret Managers ? it does rotation natively ! why is that

upvoted 2 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: A

Option A - This option will work: This option takes advantage of the Automatic Rotation feature in Secrets Manager which reduces operational overhead during secret rotation, i.e. CloudTrail will show a secret was rotated

Option B - This option will not work: Parameter Store does not have a feature called RotationSchedule

Option C - This option might work but increases overhead: Rotation will be triggered on the 90 day schedule but more work will be necessary to validate the secret was rotated and tested, i.e. CloudTrail logs will only show a lambda function was triggered

Option D - This option will not work: Parameter Store does not have a feature called RotationSchedule

upvoted 2 times

✉ **shaaam80** 4 months, 1 week ago

Selected Answer: A

Answer A. Password rotation -> Secrets Manager

upvoted 1 times

✉ **whenthan** 7 months, 1 week ago

Selected Answer: A

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

use <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-secretsmanager-rotationschedule.html>

upvoted 1 times

✉ **SK_Tyagi** 7 months, 3 weeks ago

All - I feel the answer is A but why does it says Correct Answer "B" - What is the rationale behind B, can anyone explain. I am so confused??

upvoted 2 times

✉ **SuperDuperPooperScooper** 5 months, 1 week ago

The answers shown as correct are almost never the right ones on these test dumps, just pay attention to what was most voted and the discussions in the comments

upvoted 4 times

✉ **chico2023** 8 months, 1 week ago

Selected Answer: A

Answer: A

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: A

it's n A

upvoted 1 times

✉ **rtguru** 10 months, 3 weeks ago

A poorly phrased but seems to be the best option in this scenario

upvoted 1 times

✉ **gameoflove** 11 months ago

Selected Answer: A

AWS Secret Manager is the best option for Password safety and option fulfill all the requirement

upvoted 1 times

✉ **chiplyti** 11 months, 2 weeks ago

Selected Answer: A

A correct

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

Secrets Manager RotationSchedule resource

upvoted 1 times

✉️  **kiran15789** 1 year, 1 month ago

Selected Answer: A

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_managed.html

upvoted 1 times

✉️  **_lasco_** 1 year, 1 month ago

Selected Answer: A

voted A, rotation with secrets manager:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_managed.html

upvoted 1 times

Question #27

Topic 1

A company is storing data in several Amazon DynamoDB tables. A solutions architect must use a serverless architecture to make the data accessible publicly through a simple API over HTTPS. The solution must scale automatically in response to demand. Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon API Gateway REST API. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.
- B. Create an Amazon API Gateway HTTP API. Configure this API with direct integrations to Dynamo DB by using API Gateway's AWS integration type.
- C. Create an Amazon API Gateway HTTP API. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.
- D. Create an accelerator in AWS Global Accelerator. Configure this accelerator with AWS Lambda@Edge function integrations that return data from the DynamoDB tables.
- E. Create a Network Load Balancer. Configure listener rules to forward requests to the appropriate AWS Lambda functions.

Correct Answer: CD

Community vote distribution



✉️ **Untamables** 1 year, 3 months ago

Selected Answer: AC

A and C.

API Gateway REST API can invoke DynamoDB directly.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-overview-developer-experience.html>

upvoted 25 times

✉️ **ixdb** 3 months, 4 weeks ago

CD is right.

While this option A works for private access, it does not support public access as DynamoDB tables are not publicly accessible by default.

upvoted 1 times

✉️ **Impromptu** 3 months, 3 weeks ago

Option A has the ability to specify an execution role. This IAM role should have the GetItem/PutItem permissions for the given DynamoDB table. That way you can have access to your private table via the DynamoDB API while your API Gateway is publicly available.

So I agree with A and C

upvoted 2 times

✉️ **jpa8300** 3 months, 1 week ago

You cannot choose A and C, you choose A OR C, one excludes the other. When a question says to choose two answers, one shall complement the other.

I agree that the API can integrate directly with DynamoDB, but if I have to choose two answers that complement each other, the A option cannot go with any of the others.

Saying that, the only possible choices should be C and D, you create the Lambda functions to integrate with Dynamodb and then deploy them at Edge, as extra to improve performance and latency you use Global Accelerator. Yes, it is true that this is not a requirement, but it is good to have.

upvoted 2 times

✉️ **atirado** 3 months, 3 weeks ago

Selected Answer: AC

Option A - This option might work: REST APIs can run over HTTPS and the integration type DynamoDB is possible

Option B - This option will not work: HTTP APIs do not support integration types for DynamoDB

Option C - This option will work: HTTP APIs support integration with Lambda functions

Option D - This option will not work: Lambda@Edge is a function of CloudFront

Option E - This option will not work: NLB Target groups can target Lambda functions however NLBs are not a Serverless solution (They are deployed on VPCs).

upvoted 5 times

✉️ **gofavad926** 3 weeks, 3 days ago

Selected Answer: AC

A and C

upvoted 1 times

✉ **Russ99** 3 weeks, 3 days ago

Selected Answer: CD

The solutions that meet the requirements of using a serverless architecture to make the data accessible publicly through a simple API over HTTPS and scaling automatically in response to demand are: C AND D

upvoted 1 times

✉ **Russ99** 3 weeks, 3 days ago

Actually, Option D is out, reason: you cannot use AWS Lambda@Edge with Global accelerator

upvoted 1 times

✉ **JOKERO** 1 month ago

a, c

<https://medium.com/brlink/rest-api-just-with-apigateway-and-dynamodb-8a9b0cd76b7a>

upvoted 1 times

✉ **anubha.agrahari** 1 month ago

Selected Answer: A

API Gateway REST API can invoke DynamoDB directly.

upvoted 1 times

✉ **DmitriKonnovNN** 1 month, 4 weeks ago

Sometimes when multiple answers are required, they're supposed to complement each other, but sometimes these have to be just 2 valid but independent solutions... Well API GW with Rest endpoint is a valid solution, since it's had DynamoDB proxy integration lately. We use it in production, and it's a good fit, if you want to have a lot of control and features in your API GW and no lambda functions in between, reason being VTL supports a big set of mutations which is enough to us.

On the flip side, since we're forced to use a combination, then CD is the right answer.

In terms of simplicity, it is the question, what you consider simple. API GW REST endpoint is considered simple, because it provides caching, api keys, usage plans, rate limiting, authorization, deployment stages etc. out of the box. So the plethora of out-of-the-box features is rather simple than implementing them oneself.

upvoted 1 times

✉ **ninomfr64** 3 months, 3 weeks ago

Selected Answer: BC

Not E as I think NLB listener rules don't provide the required capability to forward requests to the appropriate Lambda (you need to have an ALB)

Not D as Lambda@Edge is a CloudFront feature

A, B and C they all work here however the question requires "a simple API over HTTPS". Both REST APIs and HTTP APIs are RESTful API products. REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price. Thus I would go for B and C

upvoted 1 times

✉ **ninomfr64** 3 months, 3 weeks ago

My answer is wrong, double check that DynamoDB is not supported as first-class integration with API Gateway as per doc <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrations-aws-services-reference.html>

Thus the correct answer is A and C

upvoted 1 times

✉ **subupro** 4 months ago

C and D is the correct option

1) C- Need server less architecture so need to use lambda function instead of REST API

2) D - Global accelerator work with lambda edge would be best the option compare to NLB for auto scale up and down. It has static address and fixed entry point if we deploy multiple region.

upvoted 2 times

✉ **Hit1979** 4 months, 1 week ago

Selected Answer: CE

REST API - is not simple and limitation around scalability. NLB with listener rules can be used to forward request based on specified conditions to appropriate AWS lambda function

upvoted 1 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: AC

lambda can have https endpoints available

upvoted 1 times

✉ **rodrod** 6 months, 3 weeks ago

Selected Answer: BC

I've read similar questions previously, keyword is "simple API".

REST API adds more features than HTTP API and is considered "more" complex.

So it has to be HTTP just for that reason.

You can use API Gateway (HTTP)->dynamodb:

<https://aws.amazon.com/fr/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/>

so B and C

upvoted 3 times

 **sonyaws** 4 months, 2 weeks ago

BC

HTTP API support AWS Integrations + Simple

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

upvoted 2 times

 **bur4an** 7 months, 1 week ago

Selected Answer: BC

B. Create an Amazon API Gateway HTTP API. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.

C. Create an Amazon API Gateway HTTP API. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.

Options A, D, and E do not align with the requirements as well:

A. Amazon API Gateway REST API with Direct DynamoDB Integration: While REST APIs could work, HTTP APIs are generally more lightweight and cost-effective. Also, direct integration with DynamoDB using REST APIs could be more complex to set up compared to HTTP APIs.

upvoted 3 times

 **Russ99** 8 months, 1 week ago

Selected Answer: AB

Option C suggests configuring an Amazon API Gateway HTTP API with integrations to AWS Lambda functions that return data from the DynamoDB tables. However, this approach would introduce unnecessary complexity and additional steps since it involves using AWS Lambda as a middle layer to fetch data from DynamoDB

upvoted 1 times

 **chico2023** 8 months, 1 week ago

Selected Answer: AC

Answer: A and C

upvoted 1 times

 **pupsik** 8 months, 3 weeks ago

Selected Answer: AB

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>

upvoted 1 times

 **pupsik** 8 months, 3 weeks ago

Oops, it's AC

DynamoDb is not one of the supported services for HTTP API.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrations-aws-services-reference.html>

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: AC

AC

B is not supported by HTTP API GWY

upvoted 1 times

Question #28

Topic 1

A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JSON document. All DNS records are managed by Amazon Route 53.

A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.

Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)

- A. Create a dynamic webpage that runs on an Amazon EC2 instance. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
- B. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
- C. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
- D. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
- E. Create an Amazon CloudFront distribution. Deploy a Lambda@Edge function.
- F. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.

Correct Answer: BCF

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: CEF

C: By creating an AWS Lambda function, the solution architect can use the JSON document to look up the target URLs for each domain and respond with the appropriate redirect URL. This way, the solution does not need to rely on a web server to handle the redirects, which reduces operational effort.

E: By creating an Amazon CloudFront distribution, the solution architect can deploy a Lambda@Edge function that can look up the target URLs for each domain and respond with the appropriate redirect URL. This way, CloudFront can handle the redirection, which reduces operational effort.

F: By creating an SSL certificate with ACM and including the domains as Subject Alternative Names, the solution architect can ensure that the redirect service can handle both HTTP and HTTPS requests, which is required by the company.

upvoted 31 times

✉️ **Shahul75** 1 year, 2 months ago

SAN cannot handle redirects. We need to do http - https

upvoted 1 times

✉️ **masetromain** 1 year, 2 months ago

A and B are not the right answer because they would require configuring and maintaining a web server to handle the redirects, which would increase operational effort.

D is not the right answer because it would require creating an API Gateway API, which increases operational effort.

upvoted 6 times

✉️ **Arnaud92** 1 year ago

Wrong for B, Lambda can be an ALB target, you do not need web server

upvoted 7 times

✉️ **chathur** 10 months, 2 weeks ago

Selected Answer: BCF

If you go with a Cloudfront what is the origin? Lambda@edge is not origin. The function mentioned in C is Lambda and in E it says about Lambda@edge, which are two things. If you handle redirect from the Lambda@edge in CF there is no need of the Lambda you wrote in Answer C.

MY Answer:

Create an ALB with HTTP and HTTPS listeners (B), Use the TLS cert created in F for the HTTPS listener. As the backend for the ALB write a Lambda with endpoint mapping JSON (C)

Is this full serverless? No, but you do not have to worry about scaling or operational overhead, AWS Handles everything for us.

upvoted 21 times

✉️ **dubyaF** 3 months, 2 weeks ago

This is the only answer that is completed by using all three options selected BCF. F is mandatory to resolve the marketing domains URLs that are HTTPS. So B and C then work together to redirect to those URLs as a full solution like <https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-http-s-redirects-and-certificate-management-at-scale/>

E may have partial potential to do something, but you have no origin with it - and what would the origin be?

With BCF you hit the ALB get a redirect as a result of the Marketing URL and your done-- its a complete redirect solution which is what the whole requirement is.

upvoted 2 times

 **Dgix** Most Recent 2 weeks, 5 days ago

Selected Answer: CEF

CEF is the correct combination.

upvoted 1 times

 **24Gel** 3 weeks, 5 days ago

E is a bit blur, it seems like an unifished sentence to me

upvoted 1 times

 **atirado** 3 months, 2 weeks ago

Selected Answer: BCF

Option A - This option could work but it increases operational overhead: Deploying an EC2 instance requires building a VPC with one public subnet. Moreover, the architect will need to write an application to process the event.

Option B - This option could work and it reduces operational overhead: An ALB helps expose the solution and respond to HTTP/S requests; a VPC will needed. It can target EC2 instances and Lambda functions

Option C - This option could work and minimizes operational overhead: The architect can focus on writing the code to process the event. A VPC is not necessarily needed to deploy a Lambda function

Option D - This option might not work: AWS Gateway APIs only respond to HTTPS

Option E - This option might not work: It can respond to HTTP/S requests and send events to API Gateway as an origin. However, this would remove the need to deploy a Lambda@Edge function

Option F - This option will contribute to the solution: It enables HTTPS for the 10 domains

upvoted 3 times

 **jainparag1** 4 months, 2 weeks ago

Selected Answer: BEF

Lambda@Edge allows you to execute custom business logic closer to the viewer. This capability enables intelligent/programmable processing of HTTP requests at locations that are closer (for the purpose of latency) to your viewer. In this case the Lambda@Edge function can be written so that it redirects viewers based on information in the request based on domain and path.

To accept multiple custom domains on the CloudFront distribution a certificate can be created in ACM that includes multiple subject alternative names. These names can then be used in Route 53 records pointing to the distribution.

The ALB may will need to be configured with both an HTTP and an HTTPS listener. The HTTPS listener will also require a certificate, and this could use the same certificate used in the CloudFront distribution or it could be a separate certificate.

upvoted 3 times

 **jainparag1** 4 months, 2 weeks ago

INCORRECT: "Create a dynamic webpage and host it on an Amazon EC2 instance. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL" is incorrect. While designing such a solution, serverless should be utilized and hence EC2 isn't an appropriate use case for this scenario.

INCORRECT: "Create an AWS Lambda function that uses the event message and specified JSON document to look up and respond with a redirect URL" is incorrect. With this solution, Lambda would need a change every time config file changes and would increase effort, hence this is not an efficient option.

INCORRECT: "Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function" is incorrect. With this option as well, for each domain addition or change, API gateway stages would have to be re deployed hence this is again an ineffective choice.

upvoted 2 times

 **jainparag1** 4 months, 2 weeks ago

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-to-another-domain-with-alb/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-edge-how-it-works-tutorial.html>

Save time with our AWS cheat sheets:

<https://digitalcloud.training/amazon-cloudfront/>

upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: CEF

as they fit each other

upvoted 1 times

 **Jay_2pt0_1** 5 months ago

B, E, F - Lambda@Edge will allow for processing before directing to ALB

upvoted 1 times

 **rif** 6 months ago

BCF. We need to choose the solution with three steps and here is the blog with same situation with old possible scenario with limited scale (S3, cloudfront without lambda@edge)
<https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-http-s-redirects-and-certificate-management-at-scale/>

upvoted 3 times

 **vjp_training** 6 months, 3 weeks ago

Selected Answer: BEF

trust me

upvoted 4 times

 **Simon523** 7 months ago

Selected Answer: CEF

E is correct, cause Lambda@Edge can redirect to a different URI.

<https://aws.amazon.com/tw/blogs/networking-and-content-delivery/handling-redirectsedge-part1/>

upvoted 2 times

 **Greyeye** 7 months, 3 weeks ago

I thought about it, but I would pick C E F,

so, lambda edge over ALB

For ALB, you will have to have 10 rules created, each mapping to the Lambda as a trigger.

For Cloudfront Lambda@edge, you just need to set up a distribution, point R53 to it, and let Lambda@Edge handle all the redirects.

upvoted 2 times

 **chico2023** 8 months, 1 week ago

Selected Answer: BCF

Answer: B, C and F.

upvoted 2 times

 **ggrodsckiy** 8 months, 1 week ago

Correct BCF.

Option E is incorrect because using an Amazon CloudFront distribution and a Lambda@Edge function is not suitable for this scenario. CloudFront is a content delivery network (CDN) that caches content at edge locations for faster delivery. Lambda@Edge allows you to run Lambda functions at the edge locations to customize the content delivery. However, in this case, you do not need to cache or customize any content, but simply redirect requests based on a JSON document. Using CloudFront and Lambda@Edge may add latency and cost to your solution.

upvoted 4 times

 **softarts** 8 months, 1 week ago

Selected Answer: BEF

correct answer is BEF

explained in neal's practice test6,Q28

upvoted 3 times

 **softarts** 8 months, 1 week ago

Lambda@Edge allows you to execute custom business logic closer to the viewer. This capability enables intelligent/programmable processing of HTTP requests at locations that are closer (for the purpose of latency) to your viewer. In this case the Lambda@Edge function can be written so that it redirects viewers based on information in the request based on domain and path.

upvoted 2 times

 **softarts** 8 months, 1 week ago

To accept multiple custom domains on the CloudFront distribution a certificate can be created in ACM that includes multiple subject alternative names. These names can then be used in Route 53 records pointing to the distribution.

The ALB may will need to be configured with both an HTTP and an HTTPS listener. The HTTPS listener will also require a certificate, and this could use the same certificate used in the CloudFront distribution or it could be a separate certificate.

upvoted 2 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: BCF

CEF . although BCF seems workable and low ope overhead too

upvoted 1 times

 **Parimal1983** 9 months, 2 weeks ago

Selected Answer: BCF

ALB can support Lambda as a target, with SSL can support HTTPS along with HTTP, so these options make more logical and make sense. To process JSON document, we are using option C so option E will not be applicable.

upvoted 1 times

Question #29

Topic 1

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers.

The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value or "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- B. In the member accounts of the organization, activate the costCenter user-defined tag. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- C. In the member accounts of the organization activate the costCenter user-defined tag. From the management account, schedule a monthly AWS Cost and Usage Report. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- D. Create a custom report in the organization view in AWS Trusted Advisor. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

Correct Answer: A

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: A

Answer A : because we do not depend on the users, I prefer management account

Option C or A would be the correct answer. In option C, the solution architect would activate the costCenter user-defined tag in the member accounts of the organization, and then schedule a monthly AWS Cost and Usage Report from the management account to retrieve the reports and calculate the total cost for the costCenter tagged resources. In option A, the management account of the organization would activate the costCenter user-defined tag and configure monthly AWS Cost and Usage Reports to be saved to an Amazon S3 bucket in the management account. Then, use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources. Both options would allow the company to accurately identify the cost of the security tools running on the EC2 instances and charge the compliance team's AWS account.

upvoted 17 times

✉️ **dkx** 9 months, 2 weeks ago

Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 10 times

✉️ **chathur** 10 months, 2 weeks ago

User-defined tags can not be allowed from management accounts in AWS Organization. It must done from the management Account.
upvoted 2 times

✉️ **Untamables** 1 year, 3 months ago

Selected Answer: A

I vote A.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/configurecostallocreport.html>

upvoted 6 times

✉️ **gofavad926** 3 weeks, 3 days ago

Selected Answer: A

A is correct

upvoted 1 times

✉️ **subbupro** 4 months ago

A is correct, we need to login to management account to create

upvoted 1 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: A

yes, you need to activate cost allocation tags before using, you can do this the same place where you would like to see your reports - management account

upvoted 2 times

✉ **whenthan** 5 months, 3 weeks ago

Selected Answer: C

lines up correctly

activate tag in member accounts and generating AWS CUR from management account (has ability to see costs across all member accounts) and Tag breakdown in report

upvoted 1 times

✉ **imvb88** 6 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html>

"For tags to appear on your billing reports, you must activate them."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

"Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console."

-> eliminate B,C. D is not relevant

upvoted 2 times

✉ **whenthan** 7 months, 1 week ago

Selected Answer: A

<https://docs.aws.amazon.com/whitepapers/latest/tagging-best-practices/building-a-cost-allocation-strategy.html>

upvoted 1 times

✉ **bur4an** 7 months, 1 week ago

Selected Answer: A

Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console.

upvoted 3 times

✉ **NikkyDicky** 9 months, 2 weeks ago

it's an A

upvoted 1 times

✉ **rtguru** 10 months, 3 weeks ago

I go with D

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

Cost center tag int he management account.

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: A

Management account for reports

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: A

Answer A

upvoted 2 times

✉ **yimicc** 1 year, 3 months ago

Selected Answer: C

Should be a C

upvoted 1 times

✉ **yimicc** 1 year, 3 months ago

Change to A, the activation of user tag for billing can only be done by management account

upvoted 5 times

✉ **tman22** 1 year, 3 months ago

A. You want the cost information across all accounts - So you use the management account.

upvoted 4 times

 **masetromain** 1 year, 3 months ago

I want to answer C

upvoted 1 times

Question #30

Topic 1

A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

Which combination of steps will meet these requirements? (Choose two.)

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager.
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP.
- C. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
- D. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- E. From the management account, share the transit gateway with member accounts by using AWS Service Catalog.

Correct Answer: AC

Community vote distribution

AC (100%)

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: AC

Option A is sharing the transit gateway with member accounts by using AWS Resource Access Manager, which allows the management account to share resources with member accounts. Option C is launching an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account, and associates the attachment with the transit gateway in the management account by using the transit gateway ID. This automation of creating a new VPC and transit gateway attachment in new member accounts can help to streamline the process and reduce operational effort.

upvoted 17 times

✉️  **jainparag1** 4 months, 2 weeks ago

Precisely!

upvoted 1 times

✉️  **gofavad926**  3 weeks, 3 days ago

Selected Answer: AC

AC are correct

upvoted 1 times

✉️  **kmstan** 4 months ago

Selected Answer: AC

I am working on a project doing the exact same thing :D

upvoted 1 times

✉️  **rif** 6 months ago

AC.

<https://aws.amazon.com/ko/blogs/networking-and-content-delivery/automating-aws-transit-gateway-attachments-to-a-transit-gateway-in-a-central-account/>

<https://cloudjourney.medium.com/aws-ram-and-transit-gateway-8ac230f298e8>

upvoted 1 times

✉️  **Simon523** 7 months, 1 week ago

Selected Answer: AC

You can use AWS Resource Access Manager (RAM) to share a transit gateway for VPC attachments across accounts or across your organization in AWS Organizations.

upvoted 1 times

✉️  **NikkyDicky** 9 months, 2 weeks ago

AC of course

upvoted 1 times

✉️  **mfsec** 1 year ago

Selected Answer: AC

AC are my choice.

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: AC

A and C are the answer for me

upvoted 2 times

 **Untamables** 1 year, 3 months ago

Selected Answer: AC

A & C

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-transitgatewayattachment.html>

upvoted 2 times

 **masetromain** 1 year, 3 months ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/60090-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 3 times

Question #31

Topic 1

An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

Correct Answer: D

Community vote distribution

C (91%)

9%

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: C

The most efficient way to design an architecture to meet these requirements is option C. By creating an IAM role named procurement-manager-role in all the shared services accounts in the organization and adding the AWSPrivateMarketplaceAdminFullAccess managed policy to the role, the procurement managers will have the necessary permissions to administer Private Marketplace. Then, by creating an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role and another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization, the company can restrict access to Private Marketplace administrative access to only the procurement managers.

upvoted 13 times

✉️  **SK_Tyagi** 7 months, 3 weeks ago

The catch is the "Create an organization root-level SCP to deny permissions". I'd refrain from creating a root-level SCP

upvoted 3 times

✉️  **anubha.agrahari**  1 month ago

Selected Answer: C

C, D doesn't make sense.

upvoted 1 times

✉️  **ninomfr64** 3 months, 3 weeks ago

Selected Answer: C

Not A as it does not implement the requirement to enforce procurement managers to use the shared services account in each organizational unit
Not B as this would allow developers to administer private market place
not D as this would allow developers to administer private market place

C is correct as it configures the required role (with required permission) only in the shared service account, uses an SCP to deny private market place management to everyone except the role named procurement-manager-role and another SCP to prevent creating a role named procurement-manager-role

upvoted 2 times

✉️  **ninomfr64** 3 months, 3 weeks ago

Actually D would do the job, but creating a role in every account is not strictly necessary and would cause more work

upvoted 1 times

 **subupro** 4 months ago

C is the better one than D . because we need to apply scp to the root level with deny policy is the best practices. create the role and apply to each account is not a correct way and it is overhead to the administrator.

upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: C

look on whenthans answer

upvoted 1 times

 **whenthan** 5 months, 3 weeks ago

Selected Answer: C

creation of role in all shared services

adding required policy to the role

creation of org root-level to guardrail who can have those privileges

creation of SCP to close out workaround of creation of another role with same access

upvoted 2 times

 **Tarun4b7** 6 months, 2 weeks ago

Selected Answer: D

C and D options are most relevant. Once you create a role, you cannot create another role with same name. So option C doesn't make sense. So my answer Option D

upvoted 2 times

 **_Jassybang_** 2 months ago

i am on same page

upvoted 1 times

 **_Jassybang_** 2 months ago

its C - the role should be in shared service accounts and not all accounts

upvoted 1 times

 **qxy** 7 months, 1 week ago

Selected Answer: C

Clearly, it's C.

upvoted 1 times

 **Karamen** 7 months, 4 weeks ago

Selected answer: C

option D: "Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers", the procurement-manager-role is used by manager not used by developers

upvoted 2 times

 **alicewsm** 5 months, 3 weeks ago

the first sentence "An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace."

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

Developers has to ask procurement manager and not purchase by themselves.

upvoted 1 times

 **SorenBendixen** 8 months ago

Selected Answer: D

Its D - According to this : <https://aws.amazon.com/blogs/awsmarketplace/controlling-access-to-a-well-architected-private-marketplace-using-iam-and-aws-organizations/>

upvoted 2 times

 **SorenBendixen** 8 months ago

Its C. D is wrong - missed : "procurement-manager-role in all AWS accounts that will be used by DEVELOPERS"

upvoted 2 times

 **NikkyDicky** 9 months ago

Selected Answer: C

Its a C

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

Selected Answer: C

C is correct-

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: C

D is a distractor since the developers do not need to administer the private marketplace. Plus that the procurement team acts only in the shared accounts. That leaves C as the only option

upvoted 4 times

✉ **Jackhemo** 9 months, 3 weeks ago

Selected Answer: C

From olabiba.ai:

The MOST efficient way to design an architecture to meet these requirements is option C.

Explanation:

- Create an IAM role named procurement-manager-role in all the shared services accounts in the organization.
- Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role.
- Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.
- Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.

This approach ensures that only the procurement managers, who assume the procurement-manager-role, have administrative access to Private Marketplace. Other IAM users, groups, roles, and account administrators in the company are denied access to Private Marketplace administrative functions.

upvoted 3 times

✉ **rtguru** 10 months, 3 weeks ago

Correct answer is D

upvoted 1 times

✉ **chikorita** 10 months, 2 weeks ago

answer without proper justifications won't add up

additionally, the 4th option does not mention "root" level which in-turn is most efficient way of solving the problem

so the correct answer is C

the correct answe

upvoted 2 times

✉ **Sarutobi** 11 months, 4 weeks ago

Selected Answer: C

Very similar to this blog <https://aws.amazon.com/blogs/awsmarketplace/controlling-access-to-a-well-architected-private-marketplace-using-iam-and-aws-organizations/>. In here there are more details.

upvoted 3 times

✉ **mfsec** 1 year ago

Selected Answer: C

Create an IAM role named procurement-manager-role in all the shared services accounts in the organization.

upvoted 1 times

Question #32

Topic 1

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3, and Amazon DynamoDB. The developers account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

When this policy is deployed, IAM users in the developers account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained.
- B. Remove the FullAWSAccess SCP from the developers account's OU.
- C. Modify the FullAWSAccess SCP to explicitly deny all services.
- D. Add an explicit deny statement using a wildcard to the end of the SCP.

Correct Answer: A

Community vote distribution

B (72%)	D (21%)	6%
---------	---------	----

✉  **zhangyu20000**  1 year, 3 months ago

B is correct because default FullAWSAccess SCP is applied
upvoted 15 times

✉  **Six_Fingered_Jose**  6 months, 3 weeks ago

Selected Answer: B

If you go to AWS management console and look up how SCP works, you will find that by default FullAWSAccess policy is attached to all OUs by default if you have SCP enabled.
upvoted 7 times

✉  **jainparag1** 4 months, 2 weeks ago

That's correct. You can disable AWSFullAccess SCP from member accounts as long as you are replacing it with another policy with specific permissions required.
upvoted 2 times

✉  **Dgix**  4 weeks, 1 day ago

Selected Answer: D

D - the alternative doesn't mention an ASG which must be taken as implied.

The other solutions are simply absurd:

A: The operational overhead is ENORMOUS. To those who think that "operational overhead" is only day-to-day maintenance: it is not. It encompasses ALL CHANGES to the infrastructure.

B: Kubernetes is the very definition of operational overhead. Always avoid unless there is an absolutely compelling reason to use it.

C: And what do you people think the function of the Lambda is? None.

D: This works and is the most straightforward as soon as you realise that the ASG is implied.

In the final analysis, this is another example of how AWS exam questions leave out information in order to trip you up.

upvoted 1 times

 **Dafukubai** 1 month, 3 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html

FullAWSAccess NOT inherited. It must be set at every OU layer.

B is the most inadvisable choice because target account will get a explicitly DENY for all AWS services including EC2 etc if delete FullAWSAccess at it OU.

upvoted 1 times

 **8608f25** 2 months ago

Selected Answer: D

To eliminate the developers' ability to use AWS services outside the scope of Amazon EC2, Amazon S3, and Amazon DynamoDB, the solutions architect should:

* D. Add an explicit deny statement using a wildcard to the end of the SCP.

This action effectively restricts access to only the specified services by explicitly denying access to all other AWS services. The corrected Service Control Policy (SCP) would look something like this:

```
{
  "Sid": "ExplicitDenyAllOtherServices",
  "Effect": "Deny",
  "NotAction": [
    "ec2:",
    "dynamodb:",
    "s3:"
  ],
  "Resource": "*"
}
```

upvoted 2 times

 **8608f25** 2 months ago

Full SCP:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:",
      "Resource": "*"
    },
    {
      "Sid": "ExplicitDenyAllOtherServices",
      "Effect": "Deny",
      "NotAction": [
        "ec2:",
        "dynamodb:",
        "s3:"
      ],
      "Resource": "*"
    }
  ]
}
```

upvoted 1 times

 **8608f25** 2 months ago

Explanation:

- * Option A is less efficient because creating an explicit deny statement for each AWS service except EC2, S3, and DynamoDB would be impractical given the large number of services AWS offers.
- * Option B suggests removing the FullAWSAccess SCP from the developers account's OU. While removing FullAWSAccess could potentially restrict access, it's not as direct or effective as implementing an explicit deny. The FullAWSAccess SCP allows all actions on all resources within the account or OU it's applied to, and simply removing it doesn't automatically restrict access to only the specified services.
- * Option C suggests modifying the FullAWSAccess SCP to explicitly deny all services. However, the FullAWSAccess SCP is a default SCP applied by AWS Organizations and should generally be left as is. Custom SCPs should be created to enforce specific policies.
- * Option D is the most direct and effective approach.

upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

Selected Answer: B

ignore my previous comment

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

Selected Answer: A

By default, FullAWSAccess is applied at the root, so all member accounts in all OUs will inherit this policy. Removing FullAWSAccess SCP from a specific OU isn't enough. Answer is A.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

Ahh, thanks to @gustori99 for pointing out my incorrect understanding. SCPs are not inherited. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

The answer is B.

upvoted 1 times

 **Vaibs099** 2 months, 1 week ago

A is correct - Removing FullAWSAccess SCP from the developer account only is not going to help. As FullAWSAccess allowing all is also being inherited from the root and Parent OUs. When SCP is enable FullAWSAccess is enabled by default.

One option is replacing FullAWSAccess on root and all Parent OUs and developer account to the SCP mentioned in question allowing only three service.

If we are only removing FullAWSAccess SCP from developer's account then we will have to explicitly deny all other services not required.

upvoted 1 times

 **gustori99** 2 months, 1 week ago

Selected Answer: A

It seems that almost no one understands how SCPs are evaluated:

From the documentation: For a permission to be allowed for a specific account, there must be an explicit Allow statement at every level from the root through each OU in the direct path to the account (including the target account itself).

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html

So FullAWSAccess at the root level is NOT inherited. It must be present at ALL levels.

B is wrong because when you remove FullAWSAccess at the OU level and do not replace it with an allow list of the permitted services, ALL services will be denied even if you have an allow list on account level.

C and D does't make sense.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

The question states clearly that 3 services are permitted by the new SCP attached to the developer OU. The answer is B.

upvoted 1 times

 **gustori99** 1 month, 2 weeks ago

The question states "the solutions architect has implemented the following SCP on the developers account". In my understanding the SCP is attached on the developers account not on the OU level.

If SCP is attached on OU level then B is correct. If it is attached on the account B cannot be correct.

upvoted 1 times

 **TheHowesHold** 2 months, 2 weeks ago

Selected Answer: B

B -AWS Organizations attaches an AWS managed SCP policy named FullAWSAccess which allows all services and actions. If this policy is removed and not replaced at any level of the organization, all OUs and accounts under that level would be blocked from taking any actions.

upvoted 1 times

 **ele** 3 months, 1 week ago

Selected Answer: D

Right answer is D.

D: explicit deny will override any allow inherited from root. AWS doc:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html#how_scps_deny
not A as it is not efficient.

not B as it will not help if root still has FullAccess

not C as it is not possible to modify

upvoted 1 times

✉ **ninomfr64** 3 months, 3 weeks ago

Selected Answer: B

Services are implicitly denied and you allow services with SCP (or explicitly deny). In this scenario an SCP applied to higher level is allowing more services thus B

upvoted 1 times

✉ **subbupro** 4 months ago

Best approach - apply the deny in the root level - it is a must one best practices. When you create the organization we need to first create the below statement,

Create an explicit default deny statement for each AWS service that should be constrained.

upvoted 1 times

✉ **eurriola10** 4 months, 1 week ago

Selected Answer: B

B is correct. Review this link under Sandbox OU Scenario 2

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html#strategy_using_scps

upvoted 2 times

✉ **edder** 4 months, 2 weeks ago

Selected Answer: B

The answer is B.

When I actually tried it, except for A, the behavior was as follows.

B: Services outside the scope of the policy cannot be used.

C: All services are unavailable.

D: All services are unavailable.

upvoted 2 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: B

B, they are able to access, hence all current SCPs including parent ones have explicit allow. Removing explicit allow from the current OU will be enough to deny access.

upvoted 1 times

✉ **AMohanty** 7 months ago

A

SCP is a DENY statement, its NOT designed to PERMIT/ALLOW service access.

upvoted 1 times

Question #33

Topic 1

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases to traffic. The app has not been able to keep up with the traffic.

A solutions architect needs to implement a solution so that the app can handle the new and varying load.

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

- A. Separate the API into individual AWS Lambda functions. Configure an Amazon API Gateway REST API with Lambda integration for the backend. Update the Route 53 record to point to the API Gateway API.
- B. Containerize the API logic. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingress. Update the Route 53 record to point to the Kubernetes ingress.
- C. Create an Auto Scaling group. Place all the EC2 instances in the Auto Scaling group. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilization. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- D. Create an Application Load Balancer (ALB) in front of the API. Move the EC2 instances to private subnets in the VPC. Add the EC2 instances as targets for the ALB. Update the Route 53 record to point to the ALB.

Correct Answer: D*Community vote distribution*

EricZhang Highly Voted 1 year, 3 months ago

Selected Answer: A

Serverless requires least operational effort.

upvoted 29 times

Ikyixoayffasdrlaqd 1 year, 1 month ago

How can this be the answer ?? It says: Separate the API into individual AWS Lambda functions. Can you calculate the operational overhead to do that?

upvoted 14 times

scuzzy2010 12 months ago

Separating would be development overhead, but once done, the operational overhead (operational = ongoing day-to-day) will be the least.

upvoted 12 times

24Gel 3 weeks, 5 days ago

disagree, ASG in Option D, after set up, operational is not overheat as well

upvoted 1 times

24Gel 3 weeks, 5 days ago

i mean Option C not D

upvoted 1 times

24Gel 3 weeks, 5 days ago

never mind, A is simpler than C

upvoted 1 times

Jay_2pt0_1 10 months, 3 weeks ago

From any type of real-world perspective, this just can't be the answer IMHO. Surely AWS takes "real world" into account.

upvoted 1 times

dqwswwwtgxwkvgcvc 7 months, 3 weeks ago

I guess multivalue answer routing in Route53 is not proper load balancing so replacing multivalue answer routing with ALB would proper balance the load (with minimal effort)

upvoted 1 times

jooncco Highly Voted 1 year, 2 months ago

Selected Answer: C

Suppose there are a 100 REST APIs (Since this application is monolithic, it's quite common).

Are you still going to copy and paste all those API codes into lambda?

What if business logic changes?

This is not MINIMAL. I would go with C.

upvoted 19 times

✉ **chathur** 10 months, 2 weeks ago

"Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record. " This does not make any sense, why do you need to change R53 records using a Lambda?

upvoted 1 times

✉ **Vesla** 8 months ago

Because if you have 4 ec2 in your ASG you need to have 4 records in domain name if ASG scale up to 6 for example you need 2 add 2 records more in domain name

upvoted 3 times

✉ **liquen14** 1 month, 1 week ago

Too contrived in my opinion, and what about DNS caches in the clients?. You coul get stuck for a while with the previous list of servers. I think it's has to be A (but it would involve a considerable development effort) or D which is extremely easy to implement but and the same time it sounds a little bit fishy because they don't mention anything about ASG or scaling

I hate this kind of questions and I don't understand what kind of useful insight they provide unless they want us to become masters of the art of dealing with ambiguity

upvoted 1 times

✉ **scuzzy2010** 1 year, 1 month ago

It says "a monolithic REST-based API " - hence only 1 API. Initially I thought C, but I'll go with A as it says least operation overhead (not least implementation effort). Lambda has virtually no operation overhead compared to EC2.

upvoted 8 times

✉ **aviathor** 9 months, 1 week ago

Answer A says "Separate the API into individual AWS Lambda functions." Makes me think there may be many APIs.

However, we are looking to minimize operational effort, not development effort...

upvoted 1 times

✉ **Jay_2pt0_1** 11 months, 2 weeks ago

A monolithic REST api likely has a gazillion individual APIs. This refactor would not be a small one.

upvoted 5 times

✉ **jainparag1** 4 months, 2 weeks ago

Dealing with business logic change is applicable to existing solution or any solution based on the complexity. Rather it's easier to deal when these are microservices. You shouldn't hesitate to refactor your application by putting one time effort (dev overhead) to save significant operational overhead on daily basis. AWS is pushing for serverless only for this.

upvoted 1 times

✉ **lasithasilva709** Most Recent 5 days, 2 hours ago

Selected Answer: C

I choose C.

A,B may need significant development effort to refactor

D doesn't address the major issue which is scaling

upvoted 1 times

✉ **Smart** 1 week, 2 days ago

Selected Answer: A

There is a difference between development burden of refactoring and operational burden.

upvoted 1 times

✉ **43c89f4** 1 week, 2 days ago

A. partial correct - because monolithic application, if EC2 are not handle i dont think Lamda can handle the traffic.

i can go for D.

- because of Multi-value, ALB, TG,ASG

upvoted 1 times

✉ **VerRi** 2 weeks ago

Selected Answer: D

A will work, but not the least operational overhead.

upvoted 1 times

✉ **mav3r1ck** 2 weeks, 4 days ago

Selected Answer: D

Choosing option A — separating the API into individual AWS Lambda functions and configuring an Amazon API Gateway REST API with Lambda integration — does present a modern, highly scalable solution that could theoretically handle new and varying loads with potentially lower operational overhead once implemented.

upvoted 1 times

✉ **mav3r1ck** 2 weeks, 4 days ago

There are several reasons why it might not be considered the best option with the "least" operational overhead in this specific scenario:
 Refactoring Effort: Transforming a monolithic application into a set of microservices or serverless functions can be a significant undertaking. It requires a thorough analysis of the existing application architecture, identifying logical separations between different parts of the application, and then implementing those separations. This process can be time-consuming and requires careful planning to ensure that the application continues to function correctly as a set of more granular services.

upvoted 1 times

 **mav3r1ck** 2 weeks, 4 days ago

Testing and Debugging Challenges: Serverless applications, due to their distributed nature, can present unique challenges for testing and debugging. Ensuring that the application behaves correctly as a collection of independently deployed functions requires comprehensive integration testing. Debugging issues can also be more complex compared to a monolithic architecture, where the application components are more tightly coupled.

upvoted 1 times

 **mav3r1ck** 2 weeks, 4 days ago

Development and Deployment Overhead: Initially, moving to AWS Lambda and API Gateway involves a different approach to application development, deployment, and monitoring. Teams may need to familiarize themselves with serverless architectures, adapt deployment pipelines, and implement new monitoring and logging solutions suitable for serverless environments. This learning curve and setup can introduce additional overhead before the benefits of reduced operational management are realized.

upvoted 1 times

 **mav3r1ck** 2 weeks, 4 days ago

In contrast, option D — creating an Application Load Balancer (ALB) in front of the API and updating the infrastructure to better manage traffic through scaling and health checks — offers a balance between reducing operational overhead and implementing the solution with minimal changes to the existing application architecture. It provides an immediate solution to the problem of handling varying loads without the significant upfront investment in refactoring the application or the learning curve associated with adopting serverless technologies.

upvoted 1 times

 **red_panda** 2 weeks, 5 days ago

Selected Answer: C

For me it's C.

Answer A it's impossible. Can you imagine how much time do we need to refactor the application into n API/functions?

Answer B and C make no sense.

The only one is C, for me.

upvoted 1 times

 **kz407** 3 weeks, 3 days ago

Selected Answer: D

Problem I have with A, is the overhead of rearchitecting the application code. Monolithic REST API into Lambda means time and money spent on redesigning, development, testing and deployment. That's also "operational overhead" IMHO.

Option D on the other hand is quite straightforward. Only thing missing for that to be the obvious go-to is that it doesn't mention EC2 autoscaling.

As far as the current set up is concerned, given that the only form of load balancing available is the multivalue DNS responses, it's quite possible that always the top most IP in the list gets the most hits. When quite a high traffic hits the target, it goes down (no replacement is spun up either) resulting in the IP of that EC2 is not included in the subsequent DNS responses. Eventually, you are gonna exhaust the entire set of EC2 instance. With this behaviour being more likely than not, trying to revamp the monolith into AWS Lambda would be overkill, and it brings way too much operational overhead as well.

upvoted 1 times

 **Dgix** 1 month, 1 week ago

The correct answer is D, believe it or not. "LEAST OPERATIONAL OVERHEAD", remember? Refactoring the monolith constitutes substantial overhead. The reason D isn't immediately apparent as the correct solution is that D doesn't mention that autoscaling _can_ be used, but the operational overhead is practically zero. This is just another "fine" example of AWS wording their questions and replies in an incomplete, ambiguous manner (which we all hate) :).

upvoted 1 times

 **JOKERO** 1 month ago

but have you answered this request : implement a solution so that the app can handle the new and varying load. !!

upvoted 1 times

 **_Jassybanga_** 2 months ago

I will go with A - may be complex development with simple operations overhead as we are going full serverless here. The option D does not make sense , we are putting the API as target group for ALB but at the same time we want to point the EC2 Ip to the ALB.. not clear to be honest .

upvoted 1 times

 **_Jassybanga_** 2 months ago

Sorry I read it wrong - answer can be D as well, Route53 - ALB - Ec2 - Least changes needs to be done and is a fine working solution

upvoted 1 times

 **_Jassybanga_** 2 months ago

Actually the answer should be D as the main problem is load balancing which is achieved by using ALB. In A the load balancing is still not happening

upvoted 2 times

 **AWSPro1234** 2 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 3 times

✉ **GabrielShiao** 3 months ago

Selected Answer: D

D is least effort, no code change, auto scaling, HA. Changing code is not easy. Even if C is workable but it is not so load balancing since multivalue answer can return 8 records at maximum which is not a good choice

upvoted 2 times

✉ **grire974** 2 months, 4 weeks ago

Yeh but D doesn't mention autoscaling; I almost wrote D; but I think it's A. Just because the load is balanced doesn't mean it can handle excess demand. Ordinarily and ALB would be attached to an ASG; but an ASG isn't mentioned. And and ALB can connect to EC2 without an ASG.

upvoted 2 times

✉ **learnwithaniket** 3 months, 1 week ago

Selected Answer: D

Least operational overhead is D. Since they already have EC2 instances running.

Creating API Gateway and Lambda requires efforts.

upvoted 2 times

✉ **jpa8300** 3 months, 1 week ago

this is the kind of questions where the answers are divided. Reading the explanations in this discussion I would also choose option A, because it is the one that will cause least overhead in the day by day work, but I also agree with people that say that converting a monolithic app into a Lambda function is not easy. Options C and D are also correct and they are both a good choice and one complements the other. If you have several EC2 and you need to scale out and in, you must have a ASG. On the other hand the ALB is needed to spread the load between the EC2. So in summary it is not easy to choose the correct answer here, but I still go to A, because of the requirement 'LEAST' overhead.

upvoted 2 times

✉ **ninomfr64** 3 months, 3 weeks ago

Selected Answer: A

Not B as EKS and EC2 requires a lot of work

Not C as EC2 requires work and the lambda to update R53 upon scale out requires more work (and it is cumbersome)

Not D as EC2 requires more work than Lambda

A because R53, API GW and Lambda are all serverless and managed services

upvoted 1 times

✉ **subupro** 4 months ago

A and B are operation overhead, we need to do the rearchitecture, and D is not having any scope for auto scaling just using an ALB and Route 53. So C would be best

upvoted 1 times

✉ **grire974** 2 months, 4 weeks ago

Route53 can only return a max of 8 healthy values; so there's an upper limit on how this could scale:

<https://aws.amazon.com/route53/faqs/#:~:text=If%20you%20want%20to%20route,each%20DNS%20query.> ignoring the fact that it's also quite unorthodox.

upvoted 1 times

Question #34

Topic 1

A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts.

A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts.

Which solution meets these requirements?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

Correct Answer: B

Community vote distribution

B (96%) 4%

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: B

B is the correct answer. The solution would be to create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. This would allow the management account to view the usage costs across all the member accounts, and the teams can visualize the CUR through an Amazon QuickSight dashboard. This allows the organization to have a centralized place to view the cost breakdown and the teams to access the cost breakdown in an easy way.

upvoted 15 times

 **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: B

B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.

upvoted 1 times

 **Rajarshi** 1 month, 2 weeks ago

C

As target is to design a solution so that each OU can view a breakdown of usage costs across its AWS accounts

upvoted 1 times

 **acordovam** 2 months ago

Selected Answer: A

The question specifies that each OU should only view their own AWS accounts, not all accounts in the organization. While creating the solution in the management account might offer a centralized approach, it violates this crucial requirement.

upvoted 1 times

 **acordovam** 2 months ago

Sorry, I'm wrong, RAM can't create a Cost Report.

upvoted 1 times

 **abeb** 4 months, 2 weeks ago

B From management account of each account

upvoted 1 times

 **daz2023** 6 months, 1 week ago

AWS Resource Access Manager has nothing to do with creating CUR.

Answer B is correct. Use AWS Organization management account

upvoted 1 times

 **duriselvan** 7 months, 4 weeks ago

<https://aws.amazon.com/blogs/mt/visualize-and-gain-insights-into-your-aws-cost-and-usage-with-cloud-intelligence-dashboards-using-amazon-quicksight/>

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

B by elimination
upvoted 1 times

 **gameoflove** 11 months ago

Selected Answer: B
B As AWS Organizations Management account is only correct option
upvoted 1 times

 **leehjworking** 11 months, 3 weeks ago
Can anyone explain why A is wrong? Thank you.
upvoted 1 times

 **scuzzy2010** 11 months, 2 weeks ago
AWS Resource Access Manager has nothing to do with creating CURs. It's for sharing resources with other accounts.
upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: B
B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account.
upvoted 2 times

 **masetromain** 1 year, 3 months ago

Selected Answer: B
<https://www.examtopics.com/discussions/amazon/view/71951-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 3 times

Question #35

Topic 1

A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily. The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS. Which data migration strategy should the company use?

- A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
- B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
- C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
- D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).

Correct Answer: B

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: B

B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS) are also valid options. They both use DataSync to schedule a daily task to replicate the data between on-premises and cloud, the main difference is the type of file system in the cloud, Amazon FSx or Amazon Elastic File System (Amazon EFS).

upvoted 13 times

✉️ **rbm2023** 11 months, 1 week ago

EFS only support Linux FS. this is why we need to go for FSx . option B

upvoted 17 times

✉️ **Karamen** 7 months, 4 weeks ago

thanks for this explaination.

> EFS only support Linux FS. this is why we need to go for FSx . option B

upvoted 1 times

✉️ **victorHugo** 7 months, 1 week ago

Selected Answer: A

For an and b we need FSx. Data Sync is useful for a batch and is able to process large data volumes. in (a) the data is also accessible from on prem. The data volume is quite small (5 GB) per day therefore (a) is feasible. In my opinion, the key requirement is "data to be available on a file system in the cloud" and ",, migrating workloads" and I think this includes that it can be accessed from servers on prem. In addition (a) replaces only a Windows File server and not the overall windows landscape in AWS. There I vote for (a), AWS Data Sync.

See <https://tutorialsdojo.com/aws-datasync-vs-storage-gateway/> for a comparison

upvoted 8 times

✉️ **swadeey** 4 months, 2 weeks ago

Correct point here is migration not daily sync and replication.

upvoted 1 times

✉️ **vn_thanh tung** 7 months, 1 week ago

needs the data to be available on a file system in the cloud

upvoted 1 times

✉️ **Vongolatt** 1 week, 1 day ago

Selected Answer: B

A is not the data migration

upvoted 1 times

✉️ **mav3r1ck** 2 weeks, 4 days ago

Selected Answer: B

option B is the most suitable data migration strategy for the company. It leverages AWS DataSync to automate the replication of daily data increments from the on-premises Windows file server to Amazon FSx for Windows File Server. This approach provides a seamless integration for Windows-based workloads with minimal disruption and supports the company's needs for a cloud-native file system that is fully managed and integrates well with AWS services.

upvoted 1 times

✉ mav3r1ck 2 weeks, 4 days ago

Selected Answer: B

This option is particularly suitable for the company's requirements because it allows for scheduled daily tasks to efficiently replicate the 5 GB of new data to Amazon FSx, providing a cloud-native file system that integrates well with Windows-based workloads.

upvoted 1 times

✉ gofavad926 3 weeks, 3 days ago

Selected Answer: B

B is the answer

upvoted 1 times

✉ a54b16f 1 month, 1 week ago

Selected Answer: B

B is right, but, I wish they change "FSx" to "FSx for windows file server"

upvoted 1 times

✉ Dgix 1 month, 1 week ago

The key here is the word "migration". This suggests DataSync. If the objective was to set up a permanent hybrid solution, then AWS Storage Gateway would be the solution. Again an example where the entire question hinges on one single word.

upvoted 1 times

✉ djeong95 1 month, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html>

upvoted 1 times

✉ 8608f25 2 months ago

Selected Answer: B

The most appropriate data migration strategy for the company, considering the need for the data to be available on a file system in the cloud and the existing AWS Direct Connect connection, is:

* B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
Option B is the best choice because AWS DataSync is a data transfer service designed to make it easy to move large amounts of data online between on-premises storage systems and AWS storage services. Amazon FSx provides fully managed Windows file servers in the cloud, offering native Windows file system capabilities, making it an ideal target for Windows-based workloads that the company has migrated to AWS. Using DataSync to automate the daily replication of data ensures the new data produced is consistently available in the cloud with minimal manual effort.

upvoted 1 times

✉ Vaibs099 2 months, 1 week ago

company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. -> This line is key here, they have already moved part of Windows workload and require data to be available on another file system in the cloud. This is possible by Data Sync migrating data to FSx for Windows Server (SMB supporting file server).

File Gateway - would for connection to S3 and hardware compliance locally will give illusion of File Server. This is good for DR, Backup and migration to cheaper storage. But doesn't solve the purpose of moving data and creating another file share in Cloud.

upvoted 1 times

✉ tmlong18 2 months, 4 weeks ago

Selected Answer: A

B incorrect. Since you created a DX between AWS and on-premises, you can mount FSx in your local server directly. It doesn't make sense to schedule a daily task.

upvoted 1 times

✉ e4bc18e 1 month ago

This is wrong look at what the question actually asks, it says what is a proper MIGRATION strategy, File Gateway only lets you access data but does not migrate data from on premises.

upvoted 1 times

✉ 0c118eb 3 months, 3 weeks ago

Selected Answer: B

Anyone saying A has never used file gateway before. You can't "point the existing file share to the new file gateway". That's not how file gateways work.

upvoted 2 times

✉ ninomfr64 3 months, 3 weeks ago

Selected Answer: A

Windows workload thus C and D are ruled out (EFS is for NFS only).

B is precisely stated pointing to FSx for Windows, while A to work we need to imply we are using FSx for Windows File Gateway which is not (clearly stated). Assuming it is FSx for Windows File Gateway, A is more versatile as is quicker in synching data (B once a day)

upvoted 3 times

 **shaaam80** 4 months, 1 week ago

Selected Answer: B

Answer B. Company is looking for a migration strategy. With AWS Direct Connect in place, Datasync replication is the way to go. 5GB of new data is would be replicated in no time.

upvoted 2 times

 **swadeey** 4 months, 2 weeks ago

Aren't we talking about migration not sync. Migration means move data and use on solution. So if we use option B it says schedule daily task to replicate. That means we have on premise working and then replication to cloud. Shouldn't migration means migrate to one file system that is either cloud gateway or keep on server

upvoted 1 times

 **trap** 4 months, 2 weeks ago

Correct: A

<https://aws.amazon.com/storagegateway/file/fsx/>

upvoted 2 times

 **trap** 4 months, 2 weeks ago

<https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html>

<https://docs.aws.amazon.com/filegateway/latest/filefsxw/file-gateway-fsx-concepts.html>

upvoted 2 times

Question #36

Topic 1

A company's solutions architect is reviewing a web application that runs on AWS. The application references static assets in an Amazon S3 bucket in the us-east-1 Region. The company needs resiliency across multiple AWS Regions. The company already has created an S3 bucket in a second Region.

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

- A. Configure the application to write each object to both S3 buckets. Set up an Amazon Route 53 public hosted zone with a record set by using a weighted routing policy for each S3 bucket. Configure the application to reference the objects by using the Route 53 DNS name.
- B. Create an AWS Lambda function to copy objects from the S3 bucket in us-east-1 to the S3 bucket in the second Region. Invoke the Lambda function each time an object is written to the S3 bucket in us-east-1. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- C. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. Set up an Amazon CloudFront distribution with an origin group that contains the two S3 buckets as origins.
- D. Configure replication on the S3 bucket in us-east-1 to replicate objects to the S3 bucket in the second Region. If failover is required, update the application code to load S3 objects from the S3 bucket in the second Region.

Correct Answer: D

Community vote distribution



✉ **zhangyu20000** Highly Voted 1 year, 3 months ago

C is correct.

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

upvoted 13 times

✉ **gofavad926** Most Recent 3 weeks, 3 days ago

Selected Answer: C

C is correct

upvoted 1 times

✉ **VerRi** 1 month, 2 weeks ago

Selected Answer: C

Straightforward

upvoted 1 times

✉ **8608f25** 2 months ago

Selected Answer: C

Option C is the most efficient solution because it leverages S3's built-in replication feature to automatically replicate objects to a second bucket in another Region, ensuring that the data is resiliently stored across multiple Regions. By using Amazon CloudFront with an origin group containing both S3 buckets, the application benefits from CloudFront's global content delivery network, which improves load times and provides a built-in failover mechanism. This setup minimizes operational overhead while achieving the desired resiliency and performance improvements. Option C provides a seamless, automated solution for achieving resiliency across multiple AWS Regions with minimal operational effort, leveraging AWS services designed for replication, content delivery, and failover.

upvoted 1 times

✉ **Vaibs099** 2 months, 1 week ago

C is correct because,

You can serve Dynamic Websites with Static Content with CDN by having origins for both and in your webserver app refer to DNS for s3 origin from CF to deliver static content. For webserver on EC2 (Custom Origins can be used).

So in above scenario, if you would like to have resiliency. Add another S3 Origin with bucket in different region. Create Origin Group with both S3 Origins. Set priority on Origins and select 4XX and 5XX error codes for failover. You can use DNS returned for Origin Group from Cloud front in your web app and that would do automatic failover with least overheads.

D also solves the purpose, but you will need to build failover mechanism in your app. However, with above Cloudfront Origin group is taking care of that for you.

upvoted 1 times

✉ **ninomfr64** 3 months, 3 weeks ago

Selected Answer: C

All options does the job, but:

A would require code maintenance and managing public hosted zone -> No

B would require Lambda and CloudFront operations -> No

C would require only CloudFront operations -> Yes
D requires a lot of work for failover that appears to be manual -> No
upvoted 2 times

subupro 4 months ago
C is mostly correct, A is not correct - B and D required the code changes. C will take care of the cloud front orgin failover.
upvoted 1 times

abeb 4 months, 2 weeks ago
C is good
upvoted 1 times

severlight 4 months, 4 weeks ago

Selected Answer: C

obvious
upvoted 1 times

totten 6 months, 1 week ago

Selected Answer: C

Here's why Option C is the most suitable choice:

Replication: Amazon S3 Cross-Region replication is designed to replicate objects from one S3 bucket to another in a different Region. This ensures data resiliency across Regions with minimal operational overhead. Once configured, replication happens automatically.

CloudFront: Setting up an Amazon CloudFront distribution with an origin group containing the two S3 buckets allows you to use a single CloudFront distribution to serve content from both Regions. CloudFront provides low-latency access to your content, and using an origin group allows for failover if one of the S3 buckets becomes unavailable.

upvoted 3 times

totten 6 months, 1 week ago

Option A suggests configuring the application to write each object to both S3 buckets, which can result in higher operational overhead and may not provide immediate failover capabilities.

Option B involves creating a Lambda function to copy objects, which adds complexity and requires code maintenance for each object written to the S3 bucket in us-east-1.

Option D relies on manual updates to the application code for failover, which is less automated and could result in higher operational overhead.

Therefore, Option C is the most efficient and operationally streamlined solution to achieve data resiliency and availability across multiple AWS Regions.

upvoted 1 times

Simon523 7 months ago

Selected Answer: C

C, LEAST operational overhead
upvoted 1 times

TWOCATS 7 months, 2 weeks ago

Selected Answer: C

C should incur the least operational cost while D still requires the cx to update the code in whatever way they deem as appropriate
upvoted 1 times

Karamen 7 months, 4 weeks ago

Selected Answer: C
upvoted 1 times

xplusfb 8 months ago

Selected Answer: C

Its completely asking CRR Right one is C
upvoted 1 times

Brightalw 8 months ago

Selected Answer: D

EB support .Net. and from question, it was ordered to move the app from on-premises to AWS. EB is more appropriated for this case.
upvoted 1 times

Jonalb 9 months ago

Selected Answer: C

CCCCCCCCCC
upvoted 1 times

Jonalb 9 months, 1 week ago

Selected Answer: C

its a C correct ans...
104/402

upvoted 1 times

Question #37

Topic 1

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.
- C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- D. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

Correct Answer: C*Community vote distribution*

robertohyena Highly Voted 1 year, 3 months ago

Selected Answer: B

Agree with B.

Not A: we will not use NLB for web app

Not C: Beanstalk is region service. It CANNOT "automatically scaling web server environment that spans two separate Regions"

Not D: spot instances cant meet 'highly available'

upvoted 24 times

kz407 3 weeks, 3 days ago

I don't think ASGs are cross-region either. This answer in SO gives a serious perspective on this regard.

<https://stackoverflow.com/a/12907101/3126973>

upvoted 1 times

masetromain 1 year, 2 months ago

That's correct, option C is not a valid solution because AWS Elastic Beanstalk is a region-specific service, it cannot span multiple regions. Option B is a valid solution that uses CloudFormation to launch a stack with an Application Load Balancer in front of an Auto Scaling group, a Multi-AZ Aurora MySQL cluster and Route 53 to route traffic to the load balancer, it meets the requirements of scalability and high availability with a good performance and with less operational overhead.

upvoted 6 times

Perkuns 10 months ago

if I am not mistaken you can deploy the same EB to a different region. why does that eliminate C? it further increases your availability with geolocation weighted routing, as well as you having DR which even further increases availability along with low RPO and RTO

upvoted 4 times

jpa8300 3 months, 1 week ago

I agree with you, that's the best option, two EBs, one in each region to deploy, manage and monitor all the environment.

upvoted 1 times

masetromain Highly Voted 1 year, 2 months ago

Selected Answer: B

B is correct. The solution architect should use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

This solution provides scalability and high availability for the web application by using an Application Load Balancer and an Auto Scaling group in multiple availability zones, which can automatically scale in and out based on traffic demand. The use of a Multi-AZ Amazon Aurora MySQL DB cluster provides high availability for the database layer and the Retain deletion policy ensures the data is retained even if the DB instance is deleted. Additionally, the use of Route 53 with an alias record ensures traffic is routed to the correct location.

upvoted 8 times

 **TonytheTiger** Most Recent 1 week ago

Selected Answer: C

Option C: The only AWS documentation I found that support .NET application migration is for Elastic Beanstalk, it said " EB is the fastest and simplest way to deploy .NET applications on AWS" Many suggestion is selection option "B", the question is not asking about cost or least operational overhead, just scalable and highly available for the migration for a .NET application. Also, I can see why so many people are selecting option "B".

<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/aws-elastic-beanstalk.html>
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.design.html>

upvoted 1 times

 **kz407** 3 weeks, 3 days ago

Selected Answer: B

B however is not a highly available solution IMO because it is restricted to a region. By any chance if the region goes down, the webapp goes down as well.

A is out of the picture because it involves an NLB.

D is out of the picture because it involves spot instances which is not the choice for HA requirements.

C, everything is good except the mention of "Elastic Beanstalk environment that spans across regions". This is wrong. EB environments are a region construct. You can't have them spanning cross region. You can however have EB in multiple regions.

upvoted 1 times

 **bjexamprep** 2 months, 3 weeks ago

Selected Answer: B

Guessing the question designer prefers B. But it is wrong. When talking about R53 Alias record, it is wrong. Cause Alias record points to IP address while ALB endpoint is not an IP address.

A has flaw. The question says 3-tier web application. AWS question designers often mess up the definition of 3-tier application, which means there isn't a very clear definition of 3 tier: browser/application server/database is one definition, another one is WebServer/Application Server/database. Looks like A means the latter. Then, if the Elastic Beanstalk is hosting a web server, what are the ASG hosting? And why the R53 is pointing to the NLB which is pointing to the ASG?

C is wrong, cause Elastic Beanstalk cannot span regions.

D is wrong because spot instance is not HA.

Weighting the flaws of different answers, B has the least flaw.

upvoted 1 times

 **ninomfr64** 3 months, 3 weeks ago

Selected Answer: B

Not C as we do not need to span multiple Region (DR, global reach, ...), also cross-Region read replica does not fail-over automatically (you need to promote it to primary). Finally from the wording it seems that this imply having a single environment that spans two separate Regions which is not supported (you need two separate environments)

Not D as we have a single RDS DB instance, no HA

Both A and B does the job, but B provides better scalability as it make use of Aurora Multi-AZ that allows secondary (reader) instance(s) to be accessed for reads, while RDS Multi-AZ instance does not allow standby instance endpoint to be accessed. This could be circumvented by using Multi-AZ DB cluster deployment that provides 2 readable standby instance

upvoted 1 times

 **ayadmawla** 4 months ago

Selected Answer: C

Answer is C

The best way to migrate a .NET application to AWS is via Beanstalk (see: <https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/aws-elastic-beanstalk.html>)

I think that the question regarding spanning a deployment across two regions has triggered some to reject based on the multi-region but if you continue you will notice the separate regional deployments based on two ALBs etc. Just my two pennie :)

upvoted 1 times

 **subbupro** 4 months ago

B is the correct,

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

Selected Answer: B

Answer B

upvoted 1 times

 **abeb** 4 months, 2 weeks ago

B is good

upvoted 1 times

 **totten** 6 months, 1 week ago

Selected Answer: B

Here's why Option B is the best choice:

High Availability: The use of an Application Load Balancer (ALB) and Amazon Aurora Multi-AZ deployment ensures high availability and fault

tolerance for the web application and the MySQL database. The Multi-AZ setup for Aurora provides automatic failover.

Scalability: Using an EC2 Auto Scaling group across multiple Availability Zones allows the application to automatically scale to meet traffic demands. This is crucial for handling the surge in traffic from 200,000 daily users.

Deletion Policy: The Retain deletion policy for the Aurora MySQL DB cluster ensures that even if the CloudFormation stack is deleted, the database is retained, which is important for data preservation and recovery.

Route 53 Routing: Route 53 with an alias record provides efficient DNS routing, directing traffic to the ALB, which then distributes it to the EC2 instances. This ensures that users can access the application reliably.

upvoted 1 times

 **totten** 6 months, 1 week ago

Option C introduces unnecessary complexity by spanning two separate Regions and using geoproximity routing. This is typically used for disaster recovery and global deployments, which may not be necessary here.

upvoted 1 times

 **Simon523** 7 months ago

Selected Answer: B

The question required to "design a scalable and highly available solution". Cause the different between Beanstalk and CloudFormation is, Beanstalk is PaaS (platform as a service) while CloudFormation is IaC (infrastructure as code). So I go for Answer B, as it is related to infrastructure.

upvoted 1 times

 **victorHugo** 7 months, 1 week ago

Selected Answer: C

"web server environment" doesn't require a single instance to spawns multiple regions, multiple AWS Beanstalks for each region are also feasible. With geoproximity routing it is guaranteed the requests are routed to the same region. In addition the requirement is "highly available", which can be achieve with a multi region architecture

upvoted 1 times

 **aviathor** 7 months, 1 week ago

Selected Answer: B

- A. I do not quite understand the choice of NLB for this, but Multi-AZ DB instance, EC2 auto-scaling in multiple AZ sure sounds good.
- C. Elastic Beanstalk does not "span multiple regions". Geoproximity routing does not sound right for a disaster recovery scenario.
- B. I like CloudFormation, and I like the Retain deletion policy. In order to switch to the other region, one will need to update the Route 53 alias...
- D. I do not like the Snapshot deletion policy... The DB is not Multi-AZ, nor has a read-replica in the fail-over region. Spot instance is not great for HA.

upvoted 1 times

 **chico2023** 8 months, 1 week ago

Selected Answer: B

C is incorrect. If it wasn't "to create an automatically scaling web server environment that spans two separate Regions" I would also go with that.

upvoted 1 times

 **Jonalb** 9 months ago

Selected Answer: B

bbbbbbbbbbbbb

upvoted 1 times

 **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

Its a B

upvoted 1 times

Question #38

Topic 1

A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- A. Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
- B. Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
- C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
- D. Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

Correct Answer: C -

Community vote distribution

C (100%)

≡  **masetromain**  1 year, 2 months ago

Selected Answer: C

The best solution is C, because it involves creating the stack set in the management account of the organization, which is the central point of control for all the member accounts. This allows the solutions architect to manage the deployment of the stack set across all member accounts from a single location. Service-managed permissions are used, which allows the CloudFormation service to deploy the stack set to all member accounts. The deployment options are set to deploy to the organization and automatic deployment is enabled, which ensures that the stack set is automatically deployed to all member accounts as soon as it is created in the management account.

upvoted 19 times

≡  **masetromain**  1 year, 3 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/47723-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 5 times

≡  **Vaibs099**  2 months, 1 week ago

C. Create a stack set in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.

C is more suitable as Enable CloudFormation StackSets automatic deployment will take care of any new account in the Org. Set deployment options to deploy to the organization helps deploying Stack Instances to targeted account in Org. Use service-managed permissions is hassle free as it takes care or roles for you.

D. Create stacks in the Organizations management account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

D is good option too as StackSets drift detection is a good option to have but not a requirement. It only saves from future troubleshooting of drift scenarios.

upvoted 1 times

≡  **nharaz** 2 months, 2 weeks ago

Selected Answer: C

D is wrong - Drift Detection identifies unmanaged changes (Outside CloudFormation)

upvoted 1 times

≡  **jainparag1** 4 months, 2 weeks ago

Selected Answer: C

I'll go with C since it satisfies all the requirements with minimum operational overhead. But wondering if "Stack Sets drift detection" is just a distractor here. Can someone throw some light on this?

upvoted 2 times

≡  **ninomfr64** 3 months, 3 weeks ago

I am not an expert, just sharing my thoughts:

"Stack Sets drift detection" is a feature of stack set, however this is not needed according to the scenario.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-drift.html>.

D is a no-go for me because it deploys in each managed account without making use of stack sets, so you cannot then use stack sets drift detection.

upvoted 1 times

✉️ **daz2023** 6 months, 1 week ago

Selected Answer: C

C is the right answer

upvoted 1 times

✉️ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: C

C no brainer

upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: C

Create a stack set in the Organizations management account.

upvoted 2 times

✉️ **spd** 1 year, 1 month ago

Selected Answer: C

Stack Set in Mgmt account

upvoted 2 times

✉️ **Atila50** 1 year, 3 months ago

I THINK I SHOULD BE A

upvoted 1 times

Question #39

Topic 1

A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes, and network connections of its on-premises workloads. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs.
- C. Group servers into applications for migration by using AWS Systems Manager Application Manager.
- D. Group servers into applications for migration by using AWS Migration Hub.
- E. Generate recommended instance types and associated costs by using AWS Migration Hub.
- F. Import data about server sizes into AWS Trusted Advisor. Follow the recommendations for cost optimization.

Correct Answer: BDE

Community vote distribution

bititan Highly Voted 1 year, 2 months ago

Selected Answer: ADE

trusted advisor doesn't have option to upload data, so option F is irrelevant

upvoted 20 times

gofavad926 Most Recent 3 weeks, 3 days ago

Selected Answer: ADE

ADE is correct

upvoted 1 times

8608f25 2 months ago

Selected Answer: ADE

The correct answers are:

- * A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs. The AWS Application Discovery Service helps gather detailed information about on-premises data centers, including servers, network dependencies, and performance metrics.
- * D. Group servers into applications for migration by using AWS Migration Hub. AWS Migration Hub provides a centralized location to track the progress of application migrations across multiple AWS and partner solutions. It allows grouping discovered servers into applications, which simplifies the organization of migration tasks.
- * E. Generate recommended instance types and associated costs by using AWS Migration Hub. After servers are discovered and grouped into applications, AWS Migration Hub can analyze the collected data to recommend suitable Amazon EC2 instance types. This ensures that the migrated applications are hosted on the most cost-effective resources.

upvoted 2 times

ninomfr64 3 months, 3 weeks ago

Selected Answer: ADE

A vs B -> A because we need to use AWS Application Discovery and it provides its own agent

<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html>

C vs D -> D because AWS Application Discovery is integrated with AWS Migration Hub and it can be used to group servers into applications

<https://aws.amazon.com/migration-hub/faqs/#:~:text=How%20do%20I%20group%20servers%20into%20an%20application%3F>

E vs. F -> E as AWS Migration Hub allows to generate recommendation for instance types

<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

upvoted 3 times

Simon523 7 months ago

Selected Answer: ADE

<https://aws.amazon.com/tw/blogs/mt/using-aws-migration-hub-network-visualization-to-overcome-application-and-server-dependency-challenges/>

upvoted 2 times

NikkyDicky 9 months, 2 weeks ago

Selected Answer: ADE

ADE no brainer
upvoted 1 times

ZK000001qws 10 months, 1 week ago

B is incorrect as System Manager doesn't do discovery however, SSM Agent makes it possible for Systems Manager to update, manage, and configure the resources in AWS as well as on-premises. ADE

upvoted 3 times

asifjanjua88 1 year ago

ADE is correct answer.
upvoted 1 times

Jacky_exam 1 year ago

Selected Answer: ADE

<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html>
<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

upvoted 2 times

hgc2023 1 year ago

B is incorrect because the servers are on prem.
upvoted 1 times

ninomfr64 3 months, 3 weeks ago

SSM can be installed on on-premise server. This is not the point for not picking B
upvoted 1 times

dev112233xx 1 year ago

Selected Answer: ADE

ADE no doubts

upvoted 1 times

God_Is_Love 1 year, 1 month ago

Logical answer : Falls under the domain "Accelerate Workload Migration and Modernization"
promoting MigrationHub

Step 1 - Identify the apps

Step 2 - Group them

Step 3 - Before hand, find out what instance types would need to be in when
actual migration happens

https://d1.awsstatic.com/Product-Page-Diagram_AWS-Migration-Hub-Orchestrator%402x.0c34c9483d13ebd26cf9072193384a58531624f3.png

For OnPremises migrations, first phase is Discovery which can be done with

Discovery agent , A

https://d1.awsstatic.com/products/application-discovery-service/Product-Page-Diagram_AWS-Application-Discovery-Service%201.9d81c27f3de50349a9406b8def61b8eb914e2930.png

I wont go with Trusted Advisor although it advises how cost can be advised because-

This applies for already aws available environment. Here, about to get migrated into

AWS and Architects need to discover lot of info before hand to plan alot. So I choose E between E and F. My answer - A,D,E

upvoted 2 times

aws0909 1 year, 1 month ago

Why Option C Group servers into applications for migration by using AWS Systems Manager Application Manager is incorrect?
upvoted 1 times

sambb 1 year, 1 month ago

AWS SSM Application Manager is used for existing resources deployed to AWS
upvoted 1 times

moota 1 year, 1 month ago

Selected Answer: ADE

A is better than B.

> Agent-based discovery can be performed by deploying the AWS Application Discovery Agent on each of your VMs and physical servers. The agent installer is available for Windows and Linux operating systems. It collects static configuration data, detailed time-series system-performance information, inbound and outbound network connections, and processes that are running.

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 1 times

boomx 1 year, 2 months ago

BDE. Trusted Advisor is not for onprem assessments. Migration hub does EC2 ones
upvoted 1 times

zhangyu20000 1 year, 2 months ago

ADE is my answer

upvoted 3 times

 **masetromain** 1 year, 2 months ago

Selected Answer: ADF

in order to meet the requirements of capturing details about the system configuration, system performance, running processes, and network connections of on-premises workloads, the company should install the AWS Application Discovery Agent on the physical machines and VMs. This will allow the company to assess the existing applications and gather information about their system configurations, performance, and network connections.

To group servers into applications for migration, the company should use the AWS Migration Hub. This will allow the company to organize their servers and applications in a way that makes migration to AWS more manageable and efficient.

upvoted 2 times

 **masetromain** 1 year, 2 months ago

In order to generate recommended instance types and associated costs, the company should use AWS Trusted Advisor. Trusted Advisor can analyze the data collected by the Application Discovery Agent and provide recommendations for cost-optimized EC2 instances that will be suitable for the company's workloads. This will allow the company to run their workloads on AWS in the most cost-effective manner.

Option E, which involves generating recommended instance types and associated costs using AWS Migration Hub, is not the best choice for cost optimization. Trusted Advisor is a service that analyzes the resources in your AWS environment and provides recommendations to help you save money, improve system performance, or close security gaps.

upvoted 1 times

 **shputhan** 1 year, 2 months ago

I think option E is correct. Considering the fact Trusted Advisor provides suggestion based on utilization of resources which is already deployed in AWS. Whereas Migration Hub can suggest recommended EC2 instances.

<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

upvoted 7 times

 **ZwAi777** 6 months, 2 weeks ago

E should have mentioned Migration Evaluator since ME provides cost evaluation and right sizing info.

My thoughts

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Hey Maestro, appreciate your responses man..but you are wrong in this question. E is correct because this is for on premises requirement. F is correct in aws environment. ADE should be correct. I gave detailed logical answer as well if you are interested in other comments area

upvoted 3 times

Question #40

Topic 1

A company is hosting an image-processing service on AWS in a VPC. The VPC extends across two Availability Zones. Each Availability Zone contains one public subnet and one private subnet.

The service runs on Amazon EC2 instances in the private subnets. An Application Load Balancer in the public subnets is in front of the service. The service needs to communicate with the internet and does so through two NAT gateways. The service uses Amazon S3 for image storage. The EC2 instances retrieve approximately 1 TB of data from an S3 bucket each day.

The company has promoted the service as highly secure. A solutions architect must reduce cloud expenditures as much as possible without compromising the service's security posture or increasing the time spent on ongoing operations.

Which solution will meet these requirements?

- A. Replace the NAT gateways with NAT instances. In the VPC route table, create a route from the private subnets to the NAT instances.
- B. Move the EC2 instances to the public subnets. Remove the NAT gateways.
- C. Set up an S3 gateway VPC endpoint in the VPAttach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
- D. Attach an Amazon Elastic File System (Amazon EFS) volume to the EC2 instances. Host the images on the EFS volume.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: C

C. Setting up an S3 gateway VPC endpoint in the VPC and attaching an endpoint policy to the endpoint will allow the EC2 instances to securely access the S3 bucket for image storage without the need for NAT gateways, reducing costs without compromising security or increasing ongoing operations. This option reduces the costs associated with the NAT gateways and allows for faster data retrieval from the S3 bucket as traffic does not have to go through the internet gateway.

upvoted 13 times

 **God_Is_Love**  1 year, 1 month ago

The only reason for C is - Gateway endpoints are not Billed and so cost effective (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>) If the question changes from single region to across region, the answer would be B (overhead of NAT gateways and traversing TBs of data across NAT is expensive) because gateway endpoints are region specific

upvoted 7 times

 **anita_student** 1 year, 1 month ago

B wouldn't be highly secure and data transfer would also be slower

upvoted 1 times

 **8608f25**  2 months ago

Selected Answer: C

Option C is the most cost-effective solution that maintains the service's security posture. An S3 gateway VPC endpoint allows private connections between the VPC and S3 without requiring traffic to go through the internet or NAT gateways. This eliminates the need for NAT gateways when accessing S3, which can significantly reduce costs, especially considering the 1 TB of data retrieved daily from S3. Endpoint policies ensure that the security posture is not compromised by allowing only the required actions on the specific S3 bucket.

upvoted 1 times

 **grire974** 2 months, 4 weeks ago

Any chance someone could fix the typo in the correct answer; "VPC. Attach..." instead of VPAttach; terribly misleading.

upvoted 1 times

 **daz2023** 6 months, 1 week ago

Selected Answer: C

C for using an endpoint.

upvoted 2 times

 **NikkyDicky** 9 months, 2 weeks ago

C of course

upvoted 1 times

 **gameoflove** 11 months ago

Selected Answer: C

C is the Correct option as S3 Gateway will reduce the cost for NAT gateway
upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: C

Set up an S3 gateway VPC endpoint
upvoted 3 times

 **dev112233xx** 1 year ago

Selected Answer: C

C - easy one 
upvoted 3 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: C

C for sure
upvoted 4 times

Question #41

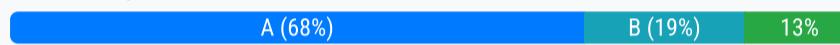
Topic 1

A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load for the rest of the week. The access pattern includes many more writes to the table than reads of the table.

A solutions architect needs to implement a solution to minimize the cost of the table.

Which solution will meet these requirements?

- A. Use AWS Application Auto Scaling to increase capacity during the peak period. Purchase reserved RCUs and WCUs to match the average load.
- B. Configure on-demand capacity mode for the table.
- C. Configure DynamoDB Accelerator (DAX) in front of the table. Reduce the provisioned read capacity to match the new peak load on the table.
- D. Configure DynamoDB Accelerator (DAX) in front of the table. Configure on-demand capacity mode for the table.

Correct Answer: D
Community vote distribution


zhangyu20000 Highly Voted 1 year, 2 months ago

A is correct. On demand mode is for unknown load pattern, auto scaling is for known burst pattern
upvoted 24 times

AimarLeo 2 months ago

But the pattern here is known.. 4 hours peak time etc.. not sure if that would be the write answer
upvoted 1 times

dqwsrnwwvtgxwkvvcv 7 months, 3 weeks ago

How AWS Application Auto Scaling scale the read/write performance of DynamoDB?
upvoted 1 times

tanh 7 months ago

You can scale DynamoDB tables and global secondary indexes using target tracking scaling policies and scheduled scaling.
<https://docs.aws.amazon.com/autoscaling/application/userguide/services-that-can-integrate-dynamodb.html>
upvoted 1 times

ccort Highly Voted 1 year, 2 months ago

Selected Answer: A

A

on-demand prices can be 7 times higher, given the options it is better to have reserved WCU and RCU and auto scale in the given schedule
upvoted 15 times

mav3r1ck Most Recent 2 weeks, 4 days ago

Selected Answer: B

Considering the application's need to handle a peak load that is double the average and the fact that the workload is write-heavy, option B (Configure on-demand capacity mode for the table) is the most suitable solution. It directly addresses the variability in workload without requiring upfront capacity planning or additional management overhead, thus likely providing the best cost optimization for this scenario. On-demand capacity mode eliminates the need to scale resources manually or through Auto Scaling and ensures that you only pay for the write and read throughput you consume.

upvoted 1 times

mav3r1ck 2 weeks, 4 days ago

A. AWS Application Auto Scaling with Reserved Capacity

Pros: Auto Scaling allows you to automatically adjust the provisioned throughput to meet demand, and purchasing reserved RCUs and WCUs can reduce costs for the capacity you know you'll consistently use.

Cons: This option might not be as cost-effective for workloads with significant variability and a high write-to-read ratio, especially if the peak load is much higher than the average load. Reserved capacity benefits consistent usage patterns, but the peak load being double the average may not be fully optimized here.

upvoted 1 times

mav3r1ck 2 weeks, 4 days ago

B. On-demand Capacity Mode

Pros: On-demand capacity mode is ideal for unpredictable workloads because it automatically scales to accommodate the load without

provisioning. You pay for what you use without managing capacity planning. This mode is particularly suitable for the described scenario where the load spikes significantly and unpredictably.

Cons: While potentially more expensive per unit than provisioned capacity with auto-scaling, it eliminates the risk of over-provisioning or under-provisioning.

upvoted 1 times

kz407 3 weeks, 2 days ago

Selected Answer: A

A is badly worded however, because it says "application" autoscaling. We are not talking about that here. Either it should be reworded as "DynamoDB autoscaling" for the answer to be correct.

On-demand capacity mode is for unknown read/write patterns. Since the load change patterns are known, anything that involves on-demand capacity modes can be eliminated (hence not B).

DAX is a caching service deployed in front of DynamoDB. It is geared towards "performance at scale". Problem in the use case, is to optimize table costs. Using DAX will incur additional costs. Hence anything that involves DAX (C and D) can also be eliminated.

upvoted 1 times

anubha.agrahari 1 month ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/#:~:text=You%20can%20approximate%20a%20blend,save%20money%20as%20reserved%20capacity>

upvoted 1 times

8608f25 2 months ago

Selected Answer: B

Option B is the most cost-effective solution for workloads with significant fluctuations and unpredictable access patterns. The on-demand capacity mode automatically adjusts the table's throughput capacity as needed in response to actual traffic, eliminating the need to manually configure or manage capacity. This mode is ideal for applications with irregular traffic patterns, such as a significant peak once a week, because you only pay for the read and write requests your application performs, without having to provision throughput in advance. Option B directly addresses the requirement to minimize costs associated with fluctuating loads, especially when the load significantly exceeds the average only during a brief period, by leveraging DynamoDB's on-demand capacity mode to automatically scale and pay only for what is used.

upvoted 1 times

igor12ghsj577 2 months, 1 week ago

Selected Answer: A

I think there is mistake in answer A, and it should be DynamoDb auto scaling instead of application autos calling. Or application and dynamoDB auto scaling.

upvoted 1 times

igor12ghsj577 2 months, 1 week ago

Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

upvoted 1 times

jpa8300 3 months, 1 week ago

Selected Answer: D

I choose option D, because DAX is not only an accelerator for the Reads, it also cache releasing a lot of load from the DB.

upvoted 1 times

ninomfr64 3 months, 3 weeks ago

Selected Answer: A

A -> You can scale DynamoDB tables and global secondary indexes using target tracking scaling policies and scheduled scaling. In this I would go for scheduled scaling.

<https://docs.aws.amazon.com/autoscaling/application/userguide/services-that-can-integrate-dynamodb.html>

B -> on-demand capacity mode is for unknown workload, this is not the case

C -> DAX come with costs and it helps with reads, while here we have a more write-bound workload

D -> See B and C comments

upvoted 2 times

severlight 4 months, 4 weeks ago

Selected Answer: A

we use scheduled scaling here

upvoted 1 times

whenthan 5 months, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/#:~:text=You%20can%20approximate%20a%20blend,save%20money%20as%20reserved%20capacity>

upvoted 1 times

Simon523 7 months ago

Selected Answer: A

Reserved capacity is available for single-Region, provisioned read and write capacity units (RCU and WCU) on DynamoDB tables including global and local secondary indexes. You cannot purchase reserved capacity for replicated WCUs (rWCUs).

upvoted 2 times

✉ **awsent** 7 months ago

Correct Answer: A

Application auto scaling can be used for scheduled scaling for DynamoDB tables and GSIs

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>

upvoted 1 times

✉ **sontis** 7 months, 2 weeks ago

aababasdasdasdasd

upvoted 1 times

✉ **venvig** 7 months, 3 weeks ago

Selected Answer: A

Refer <https://aws.amazon.com/dynamodb/reserved-capacity/>

Reserved capacity is a great option to reduce DynamoDB costs for workloads with steady usage and predictable growth over time

Reserved capacity mode might be best if you:

Have predictable application traffic.

Run applications whose traffic is consistent or ramps gradually.

Can forecast capacity requirements to control costs.

upvoted 2 times

✉ **uC6rW1aB** 7 months, 3 weeks ago

Selected Answer: B

A. This approach takes into account peak and average loads, but it might lead to unnecessary costs since you have to pay for reserved RCU and WCU, even during off-peak times.

B. The on-demand capacity mode can adjust dynamically based on actual demand, making it a suitable option, especially considering the peak lasts only for 4 hours.

C. DAX is designed to accelerate read operations, but the problem description indicates the access pattern is primarily write-focused. Therefore, this option might not be the best choice.

D. This option combines DAX with the on-demand capacity mode, but as mentioned, DAX might not be necessary.

Conclusion: Option B (configuring the table for on-demand capacity mode) seems to be the most appropriate choice, as it allows for dynamic capacity scaling during peaks and only pays for the required capacity costs during off-peak times.

upvoted 3 times

✉ **dqwsmwwvtgxwkgcvc** 7 months, 3 weeks ago

Yes I am also not sure about option B & D

upvoted 1 times

✉ **subbupro** 4 months ago

A is correct, reserved is only for average load which is less than ondemand . So A is correct

upvoted 2 times

✉ **grire974** 2 months, 4 weeks ago

Yeh B is listed as correct in Neal's udemy exam set says for this question. However if performance isn't mentioned (Dynamo throttling can occur with reserved capacity); I think A is best if there's a known average & the reserved amount is for the average. Man it would be great if there was some consensus among mock exam providers. FML.

upvoted 1 times

✉ **ggrodsckiy** 8 months, 1 week ago

Correct B.

Option A uses AWS Application Auto Scaling, which is a service that helps you adjust provisioned capacity automatically in response to actual traffic patterns. However, this option requires you to purchase reserved RCUs and WCUs, which are commitments to pay for a minimum amount of capacity for a specific term. This option can be more expensive and less flexible than on-demand capacity mode.<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/>

upvoted 2 times

✉ **b3llman** 8 months ago

If you already know the usage patterns, you save \$\$ by purchasing reserved RCUs and WCUs. It is what you want to do to save \$\$ because you will definitely use the reserved units, and what goes beyond that is what autoscaling is for.

upvoted 1 times

Question #42

Topic 1

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

- A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
- B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
- C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
- D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket.

Correct Answer: D

Community vote distribution

D (96%) 2%

masetromain Highly Voted 1 year, 2 months ago

Selected Answer: D

The correct answer would be option D.

This option suggests creating a queue using Amazon SQS, configuring the existing web server to publish to the new queue, and using EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. The EC2 instances can be scaled based on the SQS queue length, which ensures that the resources are available during peak usage times and reduces costs during non-peak times.

Option A is not correct because it suggests using AWS Lambda which has a maximum execution time of 15 minutes.
 Option B is not correct because it suggests creating a new EC2 instance for each message in the queue, which is not cost-effective.
 Option C is not correct because it suggests using Amazon EFS, which is not a suitable option for long-term storage of large files.
 upvoted 18 times

ninomfr64 Highly Voted 3 months, 2 weeks ago

Selected Answer: D

Not A - Lambda max execution time is 15 minutes, image processing can take up to 1 hour
 Not B - Amazon MQ is not needed (more expensive than SQS) and EFS is more expensive than S3
 Not C - Amazon MQ is not needed (more expensive than SQS) and Lambda max execution time is 15 minutes, image processing can take up to 1 hour

D does the job with the lower cost thanks to SQS, S3 and EC2 Auto Scaling Group

upvoted 5 times

mav3r1ck Most Recent 2 weeks, 4 days ago

Selected Answer: D

Given the need to process files that can take up to 1 hour each and the variability in workload, option D (Amazon SQS, EC2 Auto Scaling, and S3) appears to be the most cost-effective and practical solution. It leverages SQS for queue management, enabling efficient handling of the processing queue's variability. EC2 Auto Scaling allows for flexible and cost-effective scaling of processing capacity, ramping up during high-demand periods and scaling down when demand wanes, thus optimizing costs. Finally, Amazon S3 offers a highly durable and cost-effective solution for storing the processed media files. This option provides the necessary flexibility for long processing tasks while efficiently managing the variable demand and optimizing storage costs.

upvoted 1 times

Simon523 7 months ago

Selected Answer: D

Simple Queuing Service
 SQS is based on pull model. Here are some of the important features:

Reliable, scalable, fully-managed message queuing service
 High availability
 Unlimited scaling

Auto scale to process billions of messages per day

Low cost (Pay for use)

upvoted 1 times

✉ **aviathor** 7 months, 1 week ago

Selected Answer: D

This is quite simple. Any answer (A and C) consisting of using Lambda for processing the files is out because of the 15 minutes limit on Lambda processes.

B is out because using EFS is expensive and it does not specify how to launch and terminate the EC2 instances. Amazon MQ is not required either.

This leaves D which uses SQS, Auto Scaling Groups and publishes the resulting files to S3.

upvoted 2 times

✉ **chico2023** 8 months, 1 week ago

Selected Answer: D

Answer: D

You can eliminate A and C right in the beginning: Lambda functions can run up to 15 minutes.

B won't help much as you need to create new EC2 instances (manually, apparently) and EFS is more expensive than S3.

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: D

d for sure

upvoted 1 times

✉ **ailves** 9 months, 4 weeks ago

Selected Answer: D

Because of "Each media file can take up to 1 hour to process" and we know Lambda has a limit in 15 minutes, The correct answer is D

upvoted 1 times

✉ **EricZhang** 10 months, 2 weeks ago

D - <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

upvoted 1 times

✉ **huanaws088** 12 months ago

Selected Answer: B

I sure is B , because

1. SQS , SNS are " cloud - native " services : proprietary protocols from AWS
2. Traditional applications running from on - premises may use open protocols such as : MQTT , AMQP ,... so When migrating to the cloud , instead of re-engineering the application to use SQS and SNS will very expensive, we can use Amazon MQ.
3. Amazon MQ doesn't " scale " as much as SQS / SNS Amazon MQ runs on servers but Amazon MQ has both queue feature (~ SQS) and topic features (~ SNS)

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-difference-from-amazon-mq-sns.html>

upvoted 1 times

✉ **hexie** 9 months, 1 week ago

In terms of cost (which is a point on the question), Amazon SQS is generally more cost-effective compared to Amazon MQ for this specific use case. SQS pricing is based on the number of requests and message data transfer, whereas Amazon MQ pricing includes additional costs associated with broker instances and data transfer.

upvoted 1 times

✉ **takecoffee** 1 year ago

Selected Answer: D

SQS and autoscaling no doubt answer is D

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: D

SQS and Auto Scaling

upvoted 2 times

✉ **dev112233xx** 1 year ago

Selected Answer: D

D - makes sense.. Lambda can't run more than 15m.

And Amazon MQ is only recommended when migrating existing message brokers that rely on compatibility with APIs such as JMS or protocols such as AMQP, MQTT, OpenWire, and STOMP.. in the question there is no mention for these services ..

upvoted 4 times

✉ **God_Is_Love** 1 year, 1 month ago

A and C are out because lambda does not support more than 15 min. B says, to create an EC2 for each new message which is certainly not cost effective and bad design as well. So answer is D

upvoted 2 times

 **c73bf38** 1 year, 1 month ago

Selected Answer: D

The most cost-effective migration recommendation to handle peak loads during business hours is to use Amazon SQS to create a queue, configure the existing web server to publish to the new queue, and use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. The EC2 instances should be scaled based on the SQS queue length. Storing the processed files in an Amazon S3 bucket will help in reducing the storage cost. This approach is scalable and can handle peak loads during business hours, while still being cost-effective during non-business hours. Option A is also a possible solution, but using EC2 instances in an EC2 Auto Scaling group is a more scalable and cost-effective solution. Options B and C involve using Amazon EFS, which can be more expensive than Amazon S3.

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: D

D is the right answer

upvoted 2 times

 **Musk** 1 year, 2 months ago

Selected Answer: D

Because A is not valid due to time

upvoted 2 times

Question #43

Topic 1

A company is using Amazon OpenSearch Service to analyze data. The company loads data into an OpenSearch Service cluster with 10 data nodes from an Amazon S3 bucket that uses S3 Standard storage. The data resides in the cluster for 1 month for read-only analysis. After 1 month, the company deletes the index that contains the data from the cluster. For compliance purposes, the company must retain a copy of all input data.

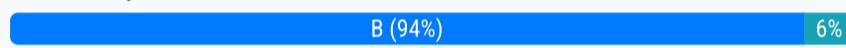
The company is concerned about ongoing costs and asks a solutions architect to recommend a new solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Replace all the data nodes with UltraWarm nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.
- B. Reduce the number of data nodes in the cluster to 2 Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Transition the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy.
- C. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data. Add cold storage nodes to the cluster Transition the indexes from UltraWarm to cold storage. Delete the input data from the S3 bucket after 1 month by using an S3 Lifecycle policy.
- D. Reduce the number of data nodes in the cluster to 2. Add instance-backed data nodes to handle the expected capacity. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.

Correct Answer: B

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: B

B is the most cost-effective solution as it reduces the number of data nodes in the cluster to 2 and adds UltraWarm nodes to handle the expected capacity. By configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data, the company can take advantage of the lower storage costs of UltraWarm. Additionally, by transitioning the input data to S3 Glacier Deep Archive after 1 month using an S3 Lifecycle policy, the company can further reduce costs by using the lower storage costs of S3 Glacier Deep Archive for long-term data retention.

upvoted 19 times

✉️ **masetromain** 1 year, 2 months ago

Option C can meet the requirements of reducing the number of data nodes in the cluster and using UltraWarm and cold storage nodes to handle the expected capacity and moving the data to lower cost storage after 1 month. However, it may not be the most cost-effective solution as it involves additional complexity in configuring the indexes to transition between different storage tiers, and may also require additional management and maintenance of the cold storage nodes. Option B, where the data is transitioned from S3 Standard to S3 Glacier Deep Archive using an S3 Lifecycle policy is simpler and more cost-effective as it eliminates the need for additional storage tiers and management.

upvoted 3 times

✉️ **God_Is_Love** 1 year, 1 month ago

B says to delete but question asks for saving on compliance purposes.

upvoted 4 times

✉️ **God_Is_Love** 1 year, 1 month ago

* I meant C says..

upvoted 5 times

✉️ **ninomfr64** 3 months, 2 weeks ago

I need help here:

To use UltraWarm storage, domains must have dedicated master nodes as per doc <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ultrawarm.html>

The scenario mentions "an OpenSearch Service cluster with 10 data nodes". Assuming you only have these nodes in the cluster, in all answers you need to add dedicated master node(s). Assuming we also have dedicated master node why not replacing all data nodes with UltraWarm nodes?

upvoted 1 times

✉️ **ninomfr64** 3 months, 2 weeks ago

I think I got it, UltraWarm is for read-only data. Thus you still need to have at least a data node

upvoted 1 times

✉ **venvig** 7 months, 3 weeks ago

Selected Answer: B

Option A says to replace all Data Nodes with ultra warm nodes. But this is NOT possible. There has to be atleast one data node
upvoted 2 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

B I think :/

upvoted 2 times

✉ **Damijo** 1 year ago

Selected Answer: A

If you look at the IAM documentation here, you can see that the ec2:AuthorizeSecurityGroupIngress action doesn't have any conditions that would allow you to specify the ip addresses in the inbound/outbound rules.https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonec2.html

upvoted 2 times

✉ **Jesuisleon** 10 months ago

I think you are referring All AWS Certified Solutions Architect - Professional SAP-C02 Questions, question 44. yes, I changed from D to A after reading this link.

upvoted 1 times

✉ **eddylynx** 9 months, 1 week ago

You can specify the IP address with the CIDR parameter

[https://ec2.amazonaws.com/?Action=AuthorizeSecurityGroupIngress&GroupId=sg-112233&IpPermissions.1.IpProtocol=tcp&IpPermissions.1.FromPort=3389&IpPermissions.1.ToPort=3389&IpPermissions.1.IpRanges.1.CidrIp=192.0.2.0/24&IpPermissions.1.IpRanges.1.Description=Access from New York office](https://ec2.amazonaws.com/?Action=AuthorizeSecurityGroupIngress&GroupId=sg-112233&IpPermissions.1.IpProtocol=tcp&IpPermissions.1.FromPort=3389&IpPermissions.1.ToPort=3389&IpPermissions.1.IpRanges.1.CidrIp=192.0.2.0/24&IpPermissions.1.IpRanges.1.Description=Access%20from%20New%20York%20office)

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_AuthorizeSecurityGroupIngress.html

upvoted 1 times

✉ **dev112233xx** 1 year ago

Selected Answer: B

B - makes more sense

upvoted 4 times

✉ **Ajani** 1 year, 1 month ago

UltraWarm provides a cost-effective way to store large amounts of read-only data on Amazon OpenSearch Service. Standard data nodes use "hot" storage, which takes the form of instance stores or Amazon EBS volumes attached to each node. Hot storage provides the fastest possible performance for indexing and searching new data.

upvoted 2 times

✉ **moota** 1 year, 1 month ago

I asked ChatGPT. Can I use all UltraWarm nodes in AWS OpenSearch instead of data nodes? :)

No, UltraWarm nodes in AWS OpenSearch are designed for storage and retrieval of infrequently accessed data, while data nodes are optimized for faster indexing and searching of data. While UltraWarm nodes can be used as a complement to data nodes, they are not a replacement for them.

upvoted 2 times

✉ **hobokabobo** 1 year, 1 month ago

This eliminates option A

upvoted 2 times

✉ **Musk** 1 year, 2 months ago

Selected Answer: B

Option B is the most cost-effective solution that meets the requirements. Reducing the number of data nodes in the cluster and adding UltraWarm nodes will help to reduce the ongoing costs of running the OpenSearch Service cluster. Configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data will further reduce costs. Additionally, transitioning the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy will lower the storage costs of retaining the input data for compliance purposes.

upvoted 4 times

Question #44

Topic 1

A company has 10 accounts that are part of an organization in AWS Organizations. AWS Config is configured in each account. All accounts belong to either the Prod OU or the NonProd OU.

The company has set up an Amazon EventBridge rule in each AWS account to notify an Amazon Simple Notification Service (Amazon SNS) topic when an Amazon EC2 security group inbound rule is created with 0.0.0.0/0 as the source. The company's security team is subscribed to the SNS topic.

For all accounts in the NonProd OU, the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source.

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

- A. Modify the EventBridge rule to invoke an AWS Lambda function to remove the security group inbound rule and to publish to the SNS topic. Deploy the updated rule to the NonProd OU.
- B. Add the vpc-sg-open-only-to-authorized-ports AWS Config managed rule to the NonProd OU.
- C. Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is not 0.0.0.0/0. Apply the SCP to the NonProd OU.
- D. Configure an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is 0.0.0.0/0. Apply the SCP to the NonProd OU.

Correct Answer: C

Community vote distribution



✉ **masetromain** 1 year, 2 months ago

Selected Answer: D

The solution that meets this requirement with the LEAST operational overhead is D. Configuring an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is 0.0.0.0/0, and applying the SCP to the NonProd OU. This solution would prevent the security group inbound rule from being created in the first place and will not require any additional steps or actions to be taken in order to remove the rule. This is less operationally intensive than modifying the EventBridge rule to invoke an AWS Lambda function, adding a Config rule or allowing the ec2:AuthorizeSecurityGroupIngress action with a specific IP.

upvoted 47 times

✉ **masetromain** 1 year, 2 months ago

Option C does not meet the requirement that the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source. It only allows the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is not 0.0.0.0/0. It does not prevent the creation of a security group inbound rule that includes 0.0.0.0/0 as the source, it only allows for the ingress action on non-0.0.0.0/0 IPs.

Option D is the best solution as it denies the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is 0.0.0.0/0. This will prevent the creation of any security group inbound rule that includes 0.0.0.0/0 as the source.

upvoted 6 times

✉ **MikelH93** 10 months, 3 weeks ago

the answer can't be C or D because aws:Sourcelp condition key don't exist with SCP.
So answer is A

upvoted 2 times

✉ **b3llman** 8 months ago

have you actually tested it? if you haven't, please do it and then comment.
upvoted 3 times

✉ **aokaddaoc** 4 months, 3 weeks ago

I think the reason why C is wrong is not because C does not meet the requirement but simply because it is too strong: All users can do is to set ingress rule in SG and all other actions are all blocked. Both C and D results the same which users can no longer able to open port to 0.0.0.0/0, but D is more precise without blocking other actions.

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

Selected Answer: D

I literally just created the SCP and it works. I saw some comments that "ec2:AuthorizeSecurityGroupIngress action doesn't have any conditions" - that is not correct. This is my scp :
{

```

"Sid": "Statement1",
"Effect": "Deny",
>Action": [
"ec2:AuthorizeSecurityGroupIngress"
],
"Resource": [
"**"
],
"Condition": {
"IpAddress": {
"aws:SourcelP": [
"0.0.0.0/0"
]
}
}
}
}

upvoted 26 times

```

 **b3llman** 8 months ago

Tested and confirmed!
upvoted 4 times

 **dqwsmtwwtgxwkvvcv** 7 months, 3 weeks ago

I guess proving D works doesn't show C is incorrect. I feel that both C and D could be correct because as CuteRunRun mentioned, the SCP deny is default.

Just have one more question, what is the ec2:AuthorizeSecurityGroupIngress if the SourcelP is not 0.0.0.0/0?

upvoted 1 times

 **vn_thanhung** 7 months, 1 week ago

For all accounts in the NonProd OU, the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source.
you think C can "remove the ability to create" carry ? SCP allow all by default?
upvoted 1 times

 **vn_thanhung** 7 months, 1 week ago

Sorry typo.
you think C can "remove the ability to create" crazy ? SCP allow all by default
upvoted 1 times

 **longns** 6 months, 1 week ago

This will deny all action create a inbound rule not only Inbound rule which have source ip "0.0.0.0/0"
upvoted 2 times

 **mav3r1ck** Most Recent 2 weeks, 4 days ago

Selected Answer: D

The goal is to prevent the creation of Amazon EC2 security group inbound rules that include 0.0.0.0/0 as the source for all accounts in the NonProd Organizational Unit (OU) with the least operational overhead.
Option D is the most straightforward and effective solution to meet the requirement with the least operational overhead. By configuring a Service Control Policy (SCP) to deny the ec2:AuthorizeSecurityGroupIngress action when the aws:SourcelP condition key is 0.0.0.0/0 and applying this policy to the NonProd OU, the company can ensure that no account within this OU can create security group inbound rules that expose resources to the entire internet. This approach leverages AWS Organizations' capability to apply governance and compliance policies at scale, thereby reducing the need for individual resource monitoring or post-creation remediation.

upvoted 1 times

 **gofavad926** 3 weeks, 3 days ago

Selected Answer: D

D is going to avoid to create the rule. A is not going to prevent, is going to remediate it...
upvoted 1 times

 **Dgix** 1 month, 1 week ago

A is out because creation of the SG is allowed albeit briefly before being updated
B is noise
C is out because SCPs don't allow
D is the correct answer
upvoted 2 times

 **Dafukubai** 1 month, 3 weeks ago

Selected Answer: A

To everyone who claimed tested D,
plz try create inbound rules other than 0.0.0.0/0.
D will deny all AuthorizeSecurityGroupIngress operation from your IP. that's why D is "worked"
upvoted 3 times

 **8608f25** 2 months ago

Selected Answer: D

Option D is the most direct and efficient solution. By creating an SCP that explicitly denies the ec2:AuthorizeSecurityGroupIngress action when the source IP is 0.0.0.0/0, it prevents users in all accounts under the NonProd OU from creating such open security group rules. This enforcement happens at the API level, blocking the action before the rule is created, which aligns with the goal of reducing operational overhead and proactively enforcing security best practices.

It is not option C because, Option C mentions configuring a Service Control Policy (SCP) to allow the ec2:AuthorizeSecurityGroupIngress action except when the source IP is 0.0.0.0/0. While the intention is correct, SCPs do not support allow-listing in this manner; they are designed to explicitly allow or deny actions across accounts in an AWS Organization.

upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

Selected Answer: A

Read the most recent comments to understand why it isn't B, C or D.

upvoted 1 times

 **Vaibs099** 2 months, 1 week ago

It has to be A,

In option C and D, aws:Sourcelp

Use this key to compare the requester's IP address with the IP address that you specify in the policy.

This is the condition not available for ec2:AuthorizeSecurityGroupIngress. It is condition to be used with Properties of the network.

Option is B is just a config rule for unauthorized port.

Only A can remove ingress rule out of these options.

Below confirming this condition is not available for ec2:AuthorizeSecurityGroupIngress

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_AuthorizeSecurityGroupIngress.html

Below confirming use of aws:Sourcelp -

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html#condition-keys-sourceip

upvoted 1 times

 **gustori99** 2 months, 1 week ago

Selected Answer: A

Everybody who voted D. Just test it yourself and you will see that it does not work.

Please understand the meaning of aws:sourcelp. From the AWS documentation: "The aws:Sourcelp condition key resolves to the IP address that the request originates from".

The aws:sourcelp condition checks the IP address of the requestor and has nothing to do with the security group sourcelp configuration.

The comment from Maria2023 who claims to have tested it is wrong because her suggested SCP denies all inbound rule creation even if you try to configure a specific IP address in the inbound rule.

Although I disagree with the wording from option A "Deploy the updated rule to the NonProd OU", A is the only possible answer.

upvoted 4 times

 **master9** 2 months, 2 weeks ago

Selected Answer: C

"C" is the right answer as in the statement it is written "NOT" which will revert the allow condition.

"Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:Sourcelp condition key is not 0.0.0.0/0. Apply the SCP to the NonProd OU".

upvoted 1 times

 **ninomfr64** 3 months, 2 weeks ago

Selected Answer: A

Not B - the vpc-sg-open-only-to-authorized-ports AWS Config managed rule checks if security groups allowing unrestricted incoming traffic ('0.0.0.0/0' or '::/0') only allow inbound TCP or UDP connections on authorized ports. The rule is NON_COMPLIANT if such security groups do not have ports specified in the rule parameters. The scenario is about unrestricted ip address and does not about port.

Not C and D - aws:Sourcelp key is used to compare the API client requester's IP address with the IP address that you specify in the policy. The aws:Sourcelp condition key can only be used for public IP address ranges.

Thus A is the right answer as it does the job (even if it requires some work)

upvoted 2 times

 **ayadmaawla** 4 months ago

Selected Answer: D

"remove the ability to create" - is not the same as removing an SG after it has been created.

upvoted 4 times

 **shaaam80** 4 months, 1 week ago

Selected Answer: D

Answer D.

Regarding A, isn't it a reactive approach?

upvoted 1 times

 **edder** 4 months, 2 weeks ago

Selected Answer: A

The correct answer is A.

I actually tried it and verified it.

B: Unsuitable because it controls TCP or UDP connections.

C,D: Even after applying the created SCP, the default SCP FullAWSAccess is still applied, so rules can be created. Even if you delete FullAWSAccess, you will not be able to access the security group with an implicit Deny.

A: This is the answer by process of elimination.

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

Selected Answer: A

I believe they are asking for a reactive approach here. They are allowing it to happen and at the same time handling it along with notification. Either C or D won't allow it to happen in the first place.

upvoted 1 times

 **NOZOMI** 4 months, 3 weeks ago

Choosing d in this problem is evidence of underestimating IAM on a regular basis. It is not befitting of a specialist. The condition key in d indicates the source IP of the API, and is not related to the control of security groups.

upvoted 2 times

Question #45

Topic 1

A company hosts a Git repository in an on-premises data center. The company uses webhooks to invoke functionality that runs in the AWS Cloud. The company hosts the webhook logic on a set of Amazon EC2 instances in an Auto Scaling group that the company set as a target for an Application Load Balancer (ALB). The Git server calls the ALB for the configured webhooks. The company wants to move the solution to a serverless architecture.

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

- A. For each webhook, create and configure an AWS Lambda function URL. Update the Git servers to call the individual Lambda function URLs.
- B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint.
- C. Deploy the webhook logic to AWS App Runner. Create an ALB, and set App Runner as the target. Update the Git servers to call the ALB endpoint.
- D. Containerize the webhook logic. Create an Amazon Elastic Container Service (Amazon ECS) cluster, and run the webhook logic in AWS Fargate. Create an Amazon API Gateway REST API, and set Fargate as the target. Update the Git servers to call the API Gateway endpoint.

Correct Answer: C*Community vote distribution*

masetromain Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Create an Amazon API Gateway HTTP API. Implement each webhook logic in a separate AWS Lambda function. Update the Git servers to call the API Gateway endpoint. This solution will provide low operational overhead as it utilizes the serverless capabilities of AWS Lambda and API Gateway, which automatically scales and manages the underlying infrastructure and resources. It also allows for the webhook logic to be easily managed and updated through the API Gateway interface.

The answer should be B because it is the best solution in terms of operational overhead.

upvoted 19 times

masetromain 1 year, 2 months ago

Option A would require updating the Git servers to call individual Lambda function URLs for each webhook, which would be more complex and time-consuming than calling a single API Gateway endpoint.

Option C would require deploying the webhook logic to AWS App Runner, which would also be more complex and time-consuming than using an API Gateway.

Option D would also require containerizing the webhook logic and creating an ECS cluster and Fargate, which would also add complexity and operational overhead compared to using an API Gateway.

upvoted 6 times

hobokabobo 1 year, 1 month ago

I do agree with B.

However on Git server side it does make no difference if one calls aws or do a rest call via gateway.

Eg. if you use Python it makes no difference if you use boto(call Lambda) or request(rest api) module.

If one implements via shell it makes no difference if one uses aws-cli(invokes Lambda directly) or curl(do a rest call).

Similar for other implementations.

upvoted 2 times

hobokabobo 1 year, 1 month ago

As addition why B is still better: it hides the implementation details and decouples by introducing a interface.

With that a team for Aws may change what ever it needs to change to implement the interface. On the other hand on git side can use whatever deems necessary without caring about implementation details.

upvoted 2 times

SmileyCloud Highly Voted 9 months, 1 week ago

Selected Answer: B

API GW and Lambda. Here is your architecture: <https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/>

upvoted 5 times

kz407 Most Recent 3 weeks, 2 days ago

Selected Answer: B

Given the current answers, I think B is the only possible option with least overhead.

C would have been a better candidate over B, if it mentioned to include the App Runner in a Target Group TG and assign TG as the target for the API Gateway. As it stands now, C is not correct because App Runner app can't be directly assigned as a target for API Gateway.

upvoted 1 times

 **gofavad926** 3 weeks, 3 days ago

Selected Answer: A

A, because is the solution with less operational overhead. Also option B also will create new lambda functions per webhook, and you have to define the specific path in the apigateway and integrate it with your specific lambda...

upvoted 1 times

 **bjexamprep** 1 month ago

Selected Answer: B

Lambda function is the easiest way to implement the webhook logic. App Runner and ECS all requires more ops overhead. So the answer is between A and B. Someone argue that using A introduces ops overhead of mapping every Lambda function to the webhooks, but actually with B, users don't need to map Lambda function in git webhooks, but move the Lambda function mapping ops to API gateway. The mapping need to be done, that's an ops overhead that cannot be ignored.

I'm guessing the question designer prefers to use API GW, because the description "Update the Git servers to call the individual Lambda function URLs." doesn't look good. While, in reality, the repo developers create the Lambda function, and they know the URL, it's very easy to launch the Lambda function from the web hook. No additional API GW is required.

upvoted 1 times

 **master9** 2 months, 2 weeks ago

Selected Answer: C

You can set App Runner as a target for ALB.

AWS App Runner can use your code. You can use AWS App Runner to create and manage services based on two fundamentally different service sources: source code and source image. App Runner starts, runs, scales, and balances your service regardless of the source type. You can use the CI/CD capability of App Runner to track changes to your source image or code. When App Runner discovers a change, it automatically builds (for source code) and deploys the new version to your App Runner service

upvoted 1 times

 **djeong95** 1 month, 1 week ago

Looks like App Runner is built more for deploying web applications rather than hosting webhook logics.

upvoted 1 times

 **uas99** 3 months, 1 week ago

A. is the right answer as no need to introduce gateway here

upvoted 2 times

 **ninomfr64** 3 months, 2 weeks ago

Selected Answer: A

I need help here: what's wrong with Lambda Function URL?

With A I just need to handle my Lambda functions, updates go through updating my aliases pointing to a new version. Here I am just missing all the capabilities provided by API Gateway that seems not to be requested (transformations, throttling, quotas, cache, api keys, auth, OpenAPI, ...). With B I still need to implement each webhook logic in a separate AWS Lambda function and update git server + I need to operate API Gateway.

Any other option requires 2 or more services thus generating more operations, also:

Not C as app runner is not a target for ALB (private IP, ECS, EC2 instance, Lambda)

Not D as you cannot set Fargate as API Gateway target (while you can use ECS as target)

Can you help me understand why B requires less operations overhead?

upvoted 5 times

 **subupro** 4 months ago

Least operations is the key. App runner is a AWS managed one and can deploy it easily, A and B we need to create lambda for each webhook it is very complex. So C would be correct

upvoted 1 times

 **jpa8300** 3 months, 1 week ago

ninomfr64 says that App runner cannot be a target for ALB, so that's the reason you cannot select C.

upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: B

Don't see the exact reasons to not choose A for now, but B will work for sure.

upvoted 1 times

 **severlight** 4 months, 4 weeks ago

UPD: Don't see the exact reasons why A won't work for now, but B will work for sure.

upvoted 1 times

 **whenthan** 5 months, 3 weeks ago

Selected Answer: B

reducing operational overhead!

upvoted 1 times

✉ **Andy97229** 5 months, 4 weeks ago

Selected Answer: C

B vs C. Looking at App Runner C makes more sense.

upvoted 1 times

✉ **sam_cao** 6 months, 2 weeks ago

Selected Answer: C

The comments below supported Option B are only focusing on how Lambda + API Gateway can help reduce operational overhead. Thinking of the scenario in the question that we have already had the source code, wouldn't it be easier if we only specify the code repo on App Runner and let it process and finish the task? Implement all logic again would consume a lot more time.

upvoted 1 times

✉ **SuperDuperPooperScooper** 5 months ago

Watch this video from AWS. At 4:05 he says Apprunner is serverless, and also there are no load balancers. Since the answer mentions load balancers it is incorrect.

<https://www.youtube.com/watch?v=HJsULvSJWes>

I found the video from this AWS post

<https://aws.amazon.com/blogs/containers/introducing-aws-app-runner/>

upvoted 3 times

✉ **CuteRunRun** 8 months, 1 week ago

Selected Answer: B

I prefer B

upvoted 1 times

✉ **NikkyDicky** 9 months, 2 weeks ago

Selected Answer: B

B makes sense

upvoted 1 times

✉ **emiliocb4** 10 months, 1 week ago

Selected Answer: C

to accomplish the least operational requirement i will go with C.

B seems to be too much disruptive to implement "each logic" in a separate lambda

upvoted 3 times

✉ **sam_cao** 6 months, 2 weeks ago

I agree. We don't have any coding if we choose C.

upvoted 1 times

✉ **Sarutobi** 11 months ago

Interesting that there is no more debate here about option A. I still think B is the way to go because AWS recommends integrating with GitLab with <https://aws-quickstart.github.io/quickstart-git2s3/> and that is what we use. But if option A works, it would be the "LEAST operational overhead." I think masetromain talked about it, but I see it differently, basically, it can be a single Lambda function that reads the payload of the webhook to continue the pipeline, basically the same idea but without API-GW in front.

upvoted 1 times

✉ **b3llman** 8 months ago

Option A works for sure, but managing API gateway is easier than managing function URLs in every single lambda function.

upvoted 1 times

Question #46

Topic 1

A company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select.
- B. Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight.
- C. Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console.
- D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

Correct Answer: C

Community vote distribution



masetromain 1 year, 2 months ago

Selected Answer: D

The correct answer is D: Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3.

Here is why the other choices are not correct:

A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises hosts. Configure Data Exploration in AWS Migration Hub. Use AWS Glue to perform an ETL job against the data. Query the data by using Amazon S3 Select. - AWS Agentless Discovery Connector will help in discovering and inventory servers but it does not provide the same level of detailed metrics as the AWS Application Discovery Agent, it also does not cover process information.

upvoted 40 times

masetromain 1 year, 2 months ago

B. Export only the VM performance information from the on-premises hosts. Directly import the required data into AWS Migration Hub. Update any missing information in Migration Hub. Query the data by using Amazon QuickSight. - It does not cover process information and it's not the best way to collect the required data, it's not efficient and it might miss some important information.

C. Create a script to automatically gather the server information from the on-premises hosts. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub. Query the data directly in the Migration Hub console. - this solution might not be very reliable and it does not cover process information, also it does not provide a way to query and analyze the data.

upvoted 5 times

masetromain 1 year, 2 months ago

D. Deploy the AWS Application Discovery Agent to each on-premises server. Configure Data Exploration in AWS Migration Hub. Use Amazon Athena to run predefined queries against the data in Amazon S3. - This is the correct answer as it covers all the requirements mentioned in the question, it will allow collecting the detailed metrics, including process information and it provides a way to query and analyze the data using Amazon Athena.

upvoted 4 times

icassp 1 year, 2 months ago

Selected Answer: D

Choosing between A and D. For A, how can S3 select query?

upvoted 6 times

oatif 1 year, 2 months ago

I think A is a better solution because the Agentless discovery connector is custom-made for the VMware environment. It will save us time and collect all the necessary data we need. Installing a Discovery agent in every server would be very time-consuming. S3 select allows simple select operations against your raw data. I don't think we need athena for

upvoted 2 times

djeong95 1 month, 1 week ago

As written by jainparag1, S3 Select is definitely the wrong solution here. As you said, it only allows for very simple select operations. Athena is a better way to go once you have configured the Migration hub settings correctly.

upvoted 1 times

✉ **jainparag1** 4 months, 2 weeks ago

A is horrible. You can write only simple SQLs using S3 select. But here you need a sophisticated solution to query these special metrics. D is satisfying all the requirements.

upvoted 2 times

✉ **gofavad926** **Most Recent** 3 weeks, 3 days ago

Selected Answer: D

D is correct

upvoted 1 times

✉ **whichonce** 1 month, 1 week ago

Selected Answer: A

Definitely A

<https://docs.aws.amazon.com/application-discovery/latest/userguide/agentless-collector-data-collected-vmware.html>

Vmware supports agentless connector with AWS, and data can be imported ove Migration Hub

upvoted 1 times

✉ **8608f25** 2 months ago

Selected Answer: D

Option D is the most efficient and streamlined solution for the requirements. Deploying the AWS Application Discovery Agent on each on-premises server allows for detailed collection of server metrics, including CPU usage, RAM usage, operating system details, and running processes. By configuring Data Exploration in AWS Migration Hub, the collected data can be analyzed and queried effectively. Using Amazon Athena for querying enables powerful SQL-based exploration of the data stored in Amazon S3, offering a flexible and scalable way to analyze the migration readiness and planning data.

It is not option C because, Option C involves creating a custom script to gather server information and using the AWS CLI to store data in AWS Migration Hub. While this approach could potentially work, it requires significant manual effort to develop, deploy, and maintain the scripts across 1,000 servers, which is not ideal for minimizing operational overhead.

upvoted 1 times

✉ **ninomfr64** 3 months, 2 weeks ago

Selected Answer: D

Not A - as AWS Agentless Discovery Connector does not provide processes visibility

Not B - as Migration Hub Import functionality does not support process data <https://docs.aws.amazon.com/cli/latest/reference/mgh/put-resource-attributes.html>, also I do not see how to query with QuickSight as there is not direct integration with Migration Hub to my knowledge

Not C - as it seems that put-resource-attributes command does not support process data

<https://docs.aws.amazon.com/cli/latest/reference/mgh/put-resource-attributes.html>

D is correct as Discovery Agent collects the required data including processes, Data Exploration in Migration Hub allows to use Amazon Athena and comes with pre-defined queries as well. <https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

upvoted 1 times

✉ **edder** 4 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

upvoted 1 times

✉ **punkbuster** 8 months ago

Selected Answer: D

The agent-based collector can collect data related to running processes which is not available to the Agentless Collector.

Check out for yourself in the FAQs:

<https://aws.amazon.com/application-discovery/faqs/>

upvoted 1 times

✉ **xplusfb** 8 months ago

Selected Answer: A

As far as i learned for VM based envs we can go with agentless. And we can use a OVA image via collect the metrics and so on. im going with A . <https://docs.aws.amazon.com/application-discovery/latest/userguide/agentless-data-collected.html>

upvoted 1 times

✉ **chico2023** 8 months, 1 week ago

Selected Answer: D

Answer: D

The requirement: "the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes."

From <https://aws.amazon.com/application-discovery/faqs/>:

== AWS Application Discovery Service Discovery Agent

Q: What data does the AWS Application Discovery Service Discovery Agent capture?

The Discovery Agent captures system configuration, system performance, running processes, and details of the network connections between systems.

upvoted 1 times

 **chico2023** 8 months, 1 week ago

==== Agentless Collector

Q: What data does the Agentless Collector capture?

The Agentless Collector is delivered as an Open Virtual Appliance (OVA) package that can be deployed to a VMware host. The type of data collected will depend on the capabilities that you configure. If the credentials are provided to connect to vCenter, the Agentless Collector will collect VM inventory, configuration, and performance history data such as CPU, memory, and disk usage. If credentials are provided to connect to databases such as Oracle, SQL Server, MySQL, or PostgreSQL, the Agentless Collector will collect version, edition, and schema data. Server and database information is uploaded to the Application Discovery Service data store. Database information can be sent to AWS DMS Fleet Advisor for analysis.

upvoted 1 times

 **CuteRunRun** 8 months, 1 week ago

Selected Answer: D

I prefer D

upvoted 1 times

 **ggrodsckiy** 8 months, 1 week ago

Correct A.

D uses agent-based discovery, which requires installing an agent on each on-premises server. This can be cumbersome and intrusive for a large number of servers. It also does not explain how to use AWS Glue to perform an ETL job against the data.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

it's a D

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: D

Initially, I went for A but the Discovery Connector only seems to collect information from the hypervisor, which excludes memory usage, processes etc. So I end up with D. Note to myself and a reminder to everyone - read the questions carefully, this is not associate exam.

upvoted 4 times

 **bcx** 9 months, 3 weeks ago

Selected Answer: A

The key is the VMWare environment, for that the obvious solution is A. IMHO.

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: D

D is the answer because agentless cant grab everything

upvoted 2 times

 **dev112233xx** 1 year ago

Selected Answer: D

A is wrong.. because Agentless can't collect processes .. only CPU/RAM and disk IO

upvoted 4 times

Question #47

Topic 1

A company is building a serverless application that runs on an AWS Lambda function that is attached to a VPC. The company needs to integrate the application with a new service from an external provider. The external provider supports only requests that come from public IPv4 addresses that are in an allow list.

The company must provide a single public IP address to the external provider before the application can start using the new service.

Which solution will give the application the ability to access the new service?

- A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.
- B. Deploy an egress-only internet gateway. Associate an Elastic IP address with the egress-only internet gateway. Configure the elastic network interface on the Lambda function to use the egress-only internet gateway.
- C. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the Lambda function to use the internet gateway.
- D. Deploy an internet gateway. Associate an Elastic IP address with the internet gateway. Configure the default route in the public VPC route table to use the internet gateway.

Correct Answer: C

Community vote distribution

A (96%) 3%

 **masetromain**  1 year, 2 months ago

Selected Answer: A

A. Deploy a NAT gateway. Associate an Elastic IP address with the NAT gateway. Configure the VPC to use the NAT gateway.

This solution will give the Lambda function access to the internet by routing its outbound traffic through the NAT gateway, which has a public Elastic IP address. This will allow the external provider to whitelist the single public IP address associated with the NAT gateway, and enable the application to access the new service.

upvoted 26 times

 **Jacky_exam** 1 year ago

Options A are not appropriate solutions because they involve deploying a NAT gateway or an egress-only internet gateway, which are used for different purposes, such as allowing resources in a private subnet to access the internet while using a static public IP address. These options will not provide the Lambda function with a single public IP address to be used for external requests.

upvoted 5 times

 **ninomfr64** 3 months, 1 week ago

The question includes "The external provider supports only requests that come from public IPv4 addresses that are in an allow list" this imply the Lambda needs to call the external provider

upvoted 1 times

 **JMAN1** 3 months, 2 weeks ago

Big Thank to you. masetromain.

upvoted 2 times

 **vvahe**  1 year ago

A

<https://docs.aws.amazon.com/lambda/latest/operatorguide/networking-vpc.html>

"By default, Lambda functions have access to the public internet. This is not the case after they have been configured with access to one of your VPCs. If you continue to need access to resources on the internet, set up a NAT instance or Amazon NAT Gateway. Alternatively, you can also use VPC endpoints to enable private communications between your VPC and supported AWS services."

upvoted 7 times

 **kz407**  3 weeks, 2 days ago

Selected Answer: A

Option A will be the only solution that matches the given requirements.

The problem with any solution that involves IGw is that IGw DOES NOT perform NAT. In fact, it does not alter the source IP field at all, meaning that we don't really have a mechanism of having a static public IP address set to the outbound traffic, while ensuring security. So, the only practical solution is to go with the NAT option.

upvoted 1 times

✉  **gofavad926** 3 weeks, 3 days ago

Selected Answer: A

A, deploy nat gateway and associate an elastic ip

upvoted 1 times

✉  **Dgix** 1 month, 1 week ago

Can an admin please take a look at _all_ the "correct answers" in this exam? They really cannot be trusted and reduce the usefulness of ExamTopics altogether. As things are, you should always just disregard the correct answer as it so often is insane.

The correct answer is of course A.

upvoted 1 times

✉  **Vsos_in29** 1 month, 2 weeks ago

A is correct option, Other approach to enable internet access

<https://www.linkedin.com/pulse/aws-lambda-accessing-private-vpc-resources-internet-without-vokhmin-pyxbe/>

upvoted 1 times

✉  **8608f25** 2 months ago

Selected Answer: A

The solution that enables the Lambda function in a VPC to access an external service that requires requests to come from a specific public IPv4 address, and to provide a single public IP address for allow listing, is:

* Option A is correct because a NAT (Network Address Translation) gateway allows instances or AWS Lambda functions in a private subnet of a VPC to initiate outbound traffic to the internet (or external services) while preventing unsolicited inbound traffic from the internet. By associating an Elastic IP address with the NAT gateway, all outbound traffic from the Lambda function routed through the NAT gateway will appear to come from this single public IP address, which can be provided to the external provider for allow listing.

upvoted 1 times

✉  **8608f25** 2 months ago

It is not option C because, Option C describes deploying an internet gateway and associating an Elastic IP address with it. However, Lambda functions cannot be directly associated with Elastic IP addresses, and internet gateways are used to route traffic between a VPC and the internet, not to provide a static public IP address for outbound traffic.

upvoted 1 times

✉  **ninomfr64** 3 months, 1 week ago

Selected Answer: A

Not B. egress-only internet gateway is IPv6 only, the question is about IPv6

Not C. you cannot associate Elastic IP to IGW also Lambda deployed in VPC cannot egress to internet via IGW, you need a NAT Gateway / NAT Instance

Not D. same as C.

A is the right solution (even if it is not well explained in my opinion)

upvoted 1 times

✉  **cgsoft** 3 months, 4 weeks ago

Selected Answer: A

As per <https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>, "To access private resources, connect your function to private subnets. If your function needs internet access, use network address translation (NAT). Connecting a function to a public subnet doesn't give it internet access or a public IP address."

upvoted 1 times

✉  **enk** 4 months, 2 weeks ago

Selected Answer: A

Just to clarify...If the Lambda function is already attached to a VPC, it's implied that it's in a private subnet since Lambda functions can't be directly placed in public subnets. So C and D are out.

upvoted 2 times

✉  **Pupu86** 5 months ago

Selected Answer: A

Option B is definitely out as egress-only internet gateway is applicable solely for IPv6 traffic.

upvoted 2 times

✉  **whenthan** 5 months, 3 weeks ago

Selected Answer: A

internet gateway - can't assign elastic IP to internet gateway

upvoted 1 times

✉  **TWOCATS** 7 months, 1 week ago

Selected Answer: A

Option B is fundamentally wrong as Egress-only internet gateway only supports IPv6, which is basically the IPv6 equivalent of NAT gateway. Please check document [1] Enable outbound IPv6 traffic using an egress-only internet gateway -

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

upvoted 1 times

✉  **vjp_training** 7 months, 3 weeks ago

Selected Answer: A

A is the best solution

<https://repost.aws/knowledge-center/internet-access-lambda-function>

upvoted 1 times

✉ **Russ99** 7 months, 3 weeks ago

Selected Answer: B

considering all these points, the best answer is B

A NAT gateway allows private subnets in a VPC to access the internet by providing them a public IP address. However, the Lambda function in this case is already in a public subnet, so a NAT gateway is not needed.

A NAT gateway only allows outbound internet access from the private subnets. It does not provide a stable public IP address that can be whitelisted by the external provider.

An internet gateway allows bi-directional internet access, which exposes the Lambda function and VPC to unsolicited inbound traffic from the internet. This is more access than what is required.

The requirement is to provide the Lambda function with outbound internet access only, and provide the external provider with a single public IP address to whitelist.

An egress-only internet gateway satisfies these requirements exactly. It allows outbound access only, and an Elastic IP can be associated with it to provide a stable whitelistable IP address.

upvoted 1 times

✉ **b3llman** 8 months ago

Selected Answer: A

IGW allows instances with public IPs to access the internet.

NGW allows instances with no public IPs to access the internet.

Since the lambda function does not have a public IP and it is in a private subnet, we need a NGW with connectivity type of "public" to access the internet and NGW has a public static IP. IGW by itself does not work for this case.

upvoted 4 times

✉ **chico2023** 8 months, 1 week ago

Selected Answer: A

This post explains way better than I could: <https://matthewleak.medium.com/aws-lambda-functions-with-a-static-ip-89a3ada0b471>

upvoted 2 times

Question #48

Topic 1

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

Which actions should the solutions architect take to meet these requirements? (Choose two.)

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

Correct Answer: BD

Community vote distribution

BD (98%)

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: BD

The correct answer is B and D.

B. Using RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database can help improve the performance of the application by reducing the number of connections opened to the database. RDS Proxy manages the connection pool and routes incoming connections to the available read replicas, which can help with connection management and reduce the number of connections that need to be opened and closed.

D. Moving the code for opening the database connection in the Lambda function outside of the event handler can help to improve the performance of the application by allowing the database connection to be reused across multiple requests. This avoids the need to open and close a new connection for each request, which can be time-consuming and resource-intensive.

upvoted 38 times

✉️  **masetromain** 1 year, 2 months ago

A. Using the cluster endpoint of the Aurora database instead of the reader endpoint would not help improve performance in this case, because the solution architect is already using read replicas to offload read traffic from the primary instance.

C. Using the Lambda Provisioned Concurrency feature would not help improve performance in this case, as the problem is related to the number of connections to the database, not the number of instances running the Lambda function.

E. Changing the API Gateway endpoint to an edge-optimized endpoint would not help improve performance in this case, as the problem is related to the number of connections to the database, not the location of the API Gateway endpoint.

upvoted 10 times

✉️  **gofavad926**  3 weeks, 3 days ago

Selected Answer: BD

B and D

upvoted 1 times

✉️  **totten** 6 months, 1 week ago

Selected Answer: BD

B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.

RDS Proxy helps manage and efficiently pool database connections, reducing the number of database connections required by the application. It helps improve performance and reduces the load on the database.

D. Move the code for opening the database connection in the Lambda function outside of the event handler.

By reusing database connections, you can reduce the overhead of opening and closing connections for each Lambda invocation. You can use the Lambda execution context to keep the database connection open and reuse it across multiple requests within the same execution context.

upvoted 2 times

✉️  **NikkyDicky** 9 months, 1 week ago

Selected Answer: BD

BD for sure

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: BD

RDS proxy + Lambda function

upvoted 3 times

✉ **dev112233xx** 1 year ago

Selected Answer: BD

RDX proxy & connecting outside the handler method is up to 5 times faster than connecting inside.

upvoted 3 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: BD

he Lambda function only queries an Amazon Aurora MySQL database- so i would reject option C

upvoted 2 times

✉ **God_Is_Love** 1 year, 1 month ago

This may be too logical answer :-) - Setting up RDS proxy will help connection pooling, So B is one answer. Now C vs D

This question focuses on serverless solutions and best practices of lambda. and question hints that lambda only contains simple code.so lambda concurrency improvements may not be the cause for performance issues detected while testing, and guess what - app is still in testing phase. so code might have a flaw can be reviewed and changed as per lambda best practices - <https://docs.aws.amazon.com/lambda/latest/dg/best-practices.html>. I choose B and D

upvoted 2 times

✉ **moota** 1 year, 1 month ago

Selected Answer: BD

According to ChatGPT,

By reusing the same database connection across multiple invocations of the function, you can reduce the number of database connections that are opened and closed, which can help conserve resources and reduce the risk of running into database connection limits.

upvoted 2 times

✉ **Amac1979** 1 year, 2 months ago

BD

<https://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler-method-to-improve-performance-en/>

upvoted 4 times

✉ **masssa** 1 year, 2 months ago

B/C

lambda provisioned concurrency and RDS proxy are mentioned in same page.

<https://quintagroup.com/blog/aws-lambda-provisioned-concurrency>

upvoted 1 times

✉ **Untamables** 1 year, 2 months ago

Selected Answer: BC

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.howitworks.html>

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>

upvoted 1 times

✉ **jhonivy** 1 year, 2 months ago

B/C

Provisioned Concurrency needed: https://www.reddit.com/r/aws/comments/gcwtqt/lambda_provisioned_concurrency_with_aurora/

With connection Pool, no to worry D

upvoted 1 times

Question #49

Topic 1

A company is planning to host a web application on AWS and wants to load balance the traffic across a group of Amazon EC2 instances. One of the security requirements is to enable end-to-end encryption in transit between the client and the web server.

Which solution will meet this requirement?

- A. Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Export the SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- B. Associate the EC2 instances with a target group. Provision an SSL certificate using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution and configure it to use the SSL certificate. Set CloudFront to use the target group as the origin server.
- C. Place the EC2 instances behind an Application Load Balancer (ALB). Provision an SSL certificate using AWS Certificate Manager (ACM), and associate the SSL certificate with the ALB. Provision a third-party SSL certificate and install it on each EC2 instance. Configure the ALB to listen on port 443 and to forward traffic to port 443 on the instances.
- D. Place the EC2 instances behind a Network Load Balancer (NLB). Provision a third-party SSL certificate and install it on the NLB and on each EC2 instance. Configure the NLB to listen on port 443 and to forward traffic to port 443 on the instances.

Correct Answer: C

Community vote distribution



✉ **pitakk** 1 year, 2 months ago

Selected Answer: C

Amazon-issued public certificates can't be installed on an EC2 instance. To enable end-to-end encryption, you must use a third-party SSL certificate. <https://aws.amazon.com/premiumsupport/knowledge-center/acm-ssl-certificate-ec2-elb/> so it's C or D. I choose C as it's ALB
upvoted 41 times

✉ **_Jassybang_** 1 month, 3 weeks ago

in C , the encryption will terminate at ALB so its not an end-2-end encryption , for e2e end encryption need NLB
upvoted 1 times

✉ **hobokabobo** 1 year, 1 month ago

correct, but then you would use that ordered certificate for the alb as well. The other reason to order certificates is because some clients cannot verify ACM certificates which is not acceptable for a productive public service.

Between ALB and EC2 a self signed certificate is sufficient as alb does no verification of the EC2's certificate at all.

upvoted 2 times

✉ **bjexamprep** 6 days, 5 hours ago

that means you are decrypting the data on ALB and encrypt it again to send it to EC2. Does that sound E2E?
upvoted 1 times

✉ **Untamables** 1 year, 2 months ago

Selected Answer: D

Vote D.

If you need to pass encrypted traffic to targets without the load balancer decrypting it, you can create a Network Load Balancer or Classic Load Balancer with a TCP listener on port 443.

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

upvoted 30 times

✉ **hobokabobo** 1 year, 1 month ago

coorect. but they want to upload the the certificate to the NLB for unknown reasons.
upvoted 4 times

✉ **Arnaud92** 1 year ago

You can use NLB with ACM cert on it. NLB can do TLS termination (<https://aws.amazon.com/blogs/aws/new-tls-termination-for-network-load-balancers/>) and re-encrypt to target

upvoted 2 times

✉ **Ikyixoayffasdrlaqd** 1 year, 1 month ago

how can this be true? Option D says to install on NLB.
You say bypass the NLB. If you bypass the NLB why are you installing the cert?
upvoted 11 times

 EmmanuelPR Most Recent 3 weeks ago

Selected Answer: A. Public Certificates: You can request Amazon-issued public certificates from ACM. ACM manages the renewal and deployment of public certificates that are used with ACM-integrated services, including Amazon CloudFront, Elastic Load Balancing, and Amazon API Gateway. <https://aws.amazon.com/es/certificate-manager/faqs/>

upvoted 2 times

 gofavad926 3 weeks, 3 days ago

Selected Answer: C
C: use ACM in the ALB and third-party SSL certificate in the EC2 instances

upvoted 1 times

 Dgix 4 weeks, 1 day ago

Selected Answer: D
The only solution that encrypts all the way is D.

upvoted 1 times

 bjexamprep 1 month ago

Selected Answer: D
The different opinions are mainly on C or D. Both C and D are good for end to end encryption “in transit”. But actually the data is unencrypted on the ALB, and then encrypted again. Technically speaking, the ALB should be considered as part of the “transit”. This is a flaw of C. And it is complicated to introduce another certificate.

The flaws of answer D are:

- mentioning installing SSL certificate to the NLB, which is not necessary.
- It doesn't mention which listener is used. TLS listener does SSL termination while TCP listener does not.

upvoted 1 times

 marszalekm 1 month, 1 week ago

<https://aws.amazon.com/blogs/aws/mutual-authentication-for-application-load-balancer-to-reliably-verify-certificate-based-client-identities/>
upvoted 1 times

 ninomfr64 3 months, 1 week ago

Selected Answer: D
Not A. You cannot export ACM certificate <https://repost.aws/knowledge-center/configure-acm-certificates-ec2>
Not B. You cannot set CloudFront to use the target group as the origin server, you need to set the ELB the target group is assigned
Not C. This terminates SSL in the load balancer and then re-encrypt, while the question asks for end-to-end encryption in transit between the client and the web server. <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

NLB configured with TCP listener on port 443 is the right option. This answer is misleading as it mention to install the SSL certificate on the NLB, this is not needed if you do not use a TLS listener.

upvoted 2 times

 subupro 4 months ago

D would be fine transport level security. No need any encrypt and decrypt.
upvoted 1 times

 sonyaws 4 months, 2 weeks ago

Selected Answer: D
Application Load Balancers do not support mutual TLS authentication (mTLS). For mTLS support, create a TCP listener using a Network Load Balancer or a Classic Load Balancer and implement mTLS on the target.
Ref: 4th paragraph of <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>
upvoted 1 times

 aokaddaoc 4 months, 3 weeks ago

Selected Answer: D
Note that if you need to pass encrypted traffic to the targets without the load balancer decrypting it, create a TCP listener on port 443 instead of creating a TLS listener. The load balancer passes the request to the target as is, without decrypting it.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

Must be D. C will decrypt request once for sure

upvoted 2 times

 heatblur 4 months, 3 weeks ago

Selected Answer: C
C is the best choice.

Similar to Option A, but with the use of a third-party SSL certificate installed on each EC2 instance. This approach would indeed ensure end-to-end encryption, with the ALB handling the SSL termination from the client and the third-party SSL certificate securing the connection from the ALB to the EC2 instances. This option is technically feasible and meets the requirement of end-to-end encryption.

upvoted 2 times

 PAUGURU 4 months, 3 weeks ago

This question is clearly wrong and no option is correct. In my world, end-to-end means there is no decryption from source to target (server). If you decrypt it on an NLB or ALB and then re-encrypt it, Amazon could read the traffic in clear if they want to, so the encryption is NEVER end-to-end with these choices.

upvoted 1 times

✉ **PAUGURU** 4 months, 1 week ago

Change to D, the only one who lets encrypted traffic pass through;
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

upvoted 1 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: C

C and D will work, but for web applications, C is preferred.

upvoted 1 times

✉ **Russs99** 5 months ago

Selected Answer: A

I originally picked C, but, you cannot use a third-party SSL certificate with an Application Load Balancer (ALB). An ALB only supports SSL certificates that are provisioned by AWS Certificate Manager (ACM) or imported into ACM. Remember this for the exam

upvoted 1 times

✉ **rainrafa** 2 months, 2 weeks ago

While you're doing that, also remember you can't export ACM certs. So definitely don't go for A.

upvoted 2 times

✉ **SuperDuperPooperScooper** 5 months ago

Selected Answer: D

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

upvoted 2 times

✉ **Pupu86** 5 months ago

Selected Answer: C

Both NLB and ALB can handle SSL/TLS offloading/termination but I would choose C cause the crux here is pointing towards web traffic (HTTP) and ALB handles web traffic while NLB handles TCP traffic.

upvoted 1 times

Question #50

Topic 1

A company wants to migrate its data analytics environment from on premises to AWS. The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run, some of the load jobs fail to run correctly.

The company must resolve the data loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the NLB.
- B. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- D. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

Correct Answer: C
Community vote distribution

C (95%)	5%
---------	----

OCHT 11 months, 4 weeks ago

Selected Answer: C

Option A, B and D have some similarities with Option C but also have some key differences:

Option A uses a Network Load Balancer (NLB) instead of an Application Load Balancer (ALB) and does not use AWS Database Migration Service (AWS DMS) for continuous data replication. Instead, it sets up the Aurora MySQL database as a replication target for the on-premises database. Option B does use AWS DMS for continuous data replication and sets up collection endpoints behind an ALB as Amazon EC2 instances in an Auto Scaling group. However, it does not create an Aurora Replica for the Aurora MySQL database or use Amazon RDS Proxy to write to the Aurora MySQL database.

Option D does not use AWS DMS for continuous data replication or set up collection endpoints behind an ALB. Instead, it sets up collection endpoints as an Amazon Kinesis data stream and uses Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database.

upvoted 15 times

ninomfr64 3 months, 1 week ago

Selected Answer: C

Not A. not clear how the on-premises database is replicated on the Aurora MySQL, also you cannot place Lambda behind NLB as NLB only supports private IPs, instances and ALB <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html>
 Not B. this will keep executing the aggregation job and the load on the same database instance and this will not resolve loading issues
 Not D. using Kinesis Data Firehose to replicate the database is not recommended, the solution should involve DMS. also moving to Kinesis Data Stream for data load requires some changes on the customer side which is not part of the request.

C is the right solution: use DMS to migrate on-premise database, move the aggregation job to the read replica, using Lambda (that supports node.js) behind ALB will not impact client side

upvoted 2 times

shaaam80 4 months, 1 week ago

Selected Answer: C

Answer C

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

It's a c

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: C

Keywords = DMS & RDS Proxy

Then C

upvoted 2 times

✉ **leehjworking** 11 months, 1 week ago

Selected Answer: C

AD: restart = interruption?

B: ASG...Why?

upvoted 3 times

✉ **chikorita** 10 months, 2 weeks ago

why ...oh...why?

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: C

ill go with C

upvoted 1 times

✉ **dev112233xx** 1 year ago

Selected Answer: C

C.. even though question didn't mention the total time of each job. If the job takes more than 15m then Lambda can't be used. Probably the solution with ASG and EC2 is better .. not sure!

upvoted 3 times

✉ **zejou1** 1 year ago

Selected Answer: C

ALB because you are pointing to Lambda function, not a network address

Look at AWS DMS feature <https://aws.amazon.com/dms/features/>

Main requirement - needs the migration to occur w/out interruptions or changes to the company's customers.

C keeps it stupid simple w/ no service interruption

upvoted 1 times

✉ **vherman** 1 year, 1 month ago

Could anybody explain why ALB? I'd go with API Gateway

upvoted 1 times

✉ **zejou1** 1 year ago

Application - you are using Lambda functions that will be sending api commands, you would use network when it is just about routing
upvoted 1 times

✉ **Sarutobi** 1 year, 1 month ago

Selected Answer: C

I would say C.

upvoted 1 times

✉ **hobokabobo** 1 year, 1 month ago

I have a feeling that none of the approaches will work.

a) We have two sources that change the database: migration and new data coming in. In a relational database this results in inconsistent data. Constraints will not be fulfilled.

b) until the database is fully synced the second database has inconsistent data. Some parts of relations and parts of entities are still missing. Constraints will not be fulfilled.

None if the approaches addresses that aggregation tasks fail because of inconsistency of the data base.

upvoted 1 times

✉ **hobokabobo** 1 year, 1 month ago

ACID principle: atomicity, consistency, isolation and durability. All solutions violate this basic principle of relational databases.

<https://en.wikipedia.org/wiki/ACID>

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Issue could be because of same db used for writing and reading heavily. solution to separate this into read replica only for reading. DMS for data migration to aws from onpremises. Writing app to DB and Reading app from DB for reports. Writing

app needs RDSProxy and saves data. Reading app reads from replica.

B is wrong because, Reading job (aggregation) needs to use replica which is mentioned in C. C is correct.

upvoted 2 times

 **Fatoch** 1 year, 1 month ago

is it C or B?

Same person answers two times two different answers

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is corect

upvoted 3 times

 **masetromain** 1 year, 2 months ago

Selected Answer: C

C.

This option would meet the requirements of resolving the data loading issue and migrating without interruption or changes for the company's customers. By using AWS DMS for continuous data replication, the company can ensure that the data being migrated is up to date. By setting up an Aurora Replica and moving the aggregation jobs to run against it, the company can offload some of the read workload from the primary database and reduce the risk of issues with the load jobs. By using AWS Lambda functions behind an ALB and Amazon RDS Proxy to write to the Aurora MySQL database, the company can add an extra layer of security and scalability to the data collection process. Finally, by pointing the collector DNS record to the ALB after the databases are synced and disabling the AWS DMS sync task, the company can ensure a smooth cutover to the new environment.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

A.

This option would not work as it would require to change the primary database and also it may cause interruption for the company's customers during the cutover process.

B.

This option would not work as it would not include Aurora Replica to offload the read workload, this would result in aggregation jobs running on the primary database which can cause the load jobs to fail during heavy loads.

D.

This option would not work as it would require to use kinesis data stream which may cause performance issues and also it may not be the best fit for this use case. Additionally, using Kinesis Data Firehose would add complexity to the data replication process, and may result in increased latency or data loss.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

C is correct. need more read replica for aggregation jobs to read data

upvoted 3 times

Question #51

Topic 1

A health insurance company stores personally identifiable information (PII) in an Amazon S3 bucket. The company uses server-side encryption with S3 managed encryption keys (SSE-S3) to encrypt the objects. According to a new requirement, all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages. The S3 bucket does not have versioning enabled.

Which solution will meet these requirements?

- A. In the S3 bucket properties, change the default encryption to SSE-S3 with a customer managed key. Use the AWS CLI to re-upload all objects in the S3 bucket. Set an S3 bucket policy to deny unencrypted PutObject requests.
- B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.
- C. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests.
- D. In the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted PutObject requests to any entities that access the S3 bucket. Use the AWS CLI to re-upload all objects in the S3 bucket.

Correct Answer: D

Community vote distribution

B (61%)

D (39%)

 **masetromain**  1 year, 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html>

So the correct answer is B. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.

upvoted 37 times

 **Musk** 1 year, 2 months ago

What about the requirement of customer managed keys?

upvoted 9 times

 **hamimelon** 7 months, 1 week ago

Not B. "must be encrypted by keys that the company's security team manages". This implies the company does not wanna use AWS KMS.
upvoted 3 times

 **hogtrough** 1 month, 3 weeks ago

This is why they would use Customer-managed keys in AWS KMS. It is absolutely B

upvoted 1 times

 **jpa8300** 3 months, 1 week ago

Hamimmelon, the Company's security Team can manage the AWS KMS service, so B is the right answer. All the others are not valid.
upvoted 2 times

 **hobokabobo** 1 year, 1 month ago

Completely ignores the task to solve: "all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages."

upvoted 4 times

 **cherep87** 1 year, 1 month ago

Use the AWS CLI to re-upload all objects in the S3 bucket. -

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

Changes to note before enabling default encryption

After you enable default encryption for a bucket, the following encryption behavior applies:

There is no change to the encryption of the objects that existed in the bucket before default encryption was enabled.

When you upload objects after enabling default encryption:

If your PUT request headers don't include encryption information, Amazon S3 uses the bucket's default encryption settings to encrypt the objects.

upvoted 1 times

 **hobokabobo** 1 year ago

Task is to replace any AWS Managed keys to ones "that the company's security team manages"
So they tell us to find a solution that does not use AWS Managed Keys.

upvoted 4 times

 **hogtrough** 1 month, 3 weeks ago

No, the task was to replace SSE-SE keys which have no relation to AWS KMS.

"Amazon S3 automatically enables server-side encryption with Amazon S3 managed keys (SSE-S3) for new object uploads.

Unless you specify otherwise, buckets use SSE-S3 by default to encrypt objects. However, you can choose to configure buckets to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) instead. "

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html>

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Option A is not correct because it uses SSE-S3 with a customer-managed key, but it does not specify how the security team will manage the encryption keys. Additionally, it only denies unencrypted PutObject requests but does not specify how the objects will be encrypted.

Option C is not correct because it does not specify how the security team will manage the encryption keys and it does not specify how the objects will be encrypted.

Option D is not correct because it uses AES-256 with a customer-managed key, but it does not specify how the security team will manage the encryption keys. Additionally, it simply denies unencrypted PutObject requests, but it doesn't specify how the objects will be encrypted.

upvoted 7 times

 **jpa8300** 3 months, 1 week ago

And adding to this in option D they specify uses default AES-256, but KMS also uses the same, so this option just don't make sense.

upvoted 1 times

 **Untamables** Highly Voted  1 year, 2 months ago

Selected Answer: D

I think D is correct.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>

upvoted 19 times

 **djeong95** 1 month, 1 week ago

The issue with D is that it doesn't make it clear where the encryption is happening like all the other options do. Is it server-side (we assume that it is, but it is not what is written)? Or is it client-side?

upvoted 1 times

 **mav3r1ck** Most Recent  2 weeks, 4 days ago

Selected Answer: B

Correct Approach: This option is accurate and meets all the specified requirements. By changing the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS), the company can use customer managed keys (CMKs) for encryption. This allows the security team to manage the keys, addressing the core requirement.

Setting an S3 bucket policy to deny unencrypted PutObject requests ensures future compliance with the encryption policy.

Re-uploading all objects using the AWS CLI ensures that existing objects are encrypted under the new policy, making sure that both current and future objects are encrypted with the keys managed by the company's security team.

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: B

B, option D confuses encryption options. AES-256 is part of the SSE-S3 encryption method and doesn't directly involve customer-managed keys

upvoted 1 times

 **8608f25** 2 months ago

Selected Answer: B

The solution that meets the requirements for encrypting all current and future objects in the Amazon S3 bucket with keys that the company's security team manages, while ensuring server-side encryption, is:

Option B is correct because it directly addresses the new requirement by changing the default encryption method to SSE-KMS, which allows the use of AWS Key Management Service (KMS) keys managed by the company's security team. This option ensures that all future uploads are encrypted with the specified KMS key. It also includes re-uploading existing objects to ensure they are encrypted under the new scheme. Setting an S3 bucket policy to deny unencrypted PutObject requests enforces the encryption requirement for all new uploads.

upvoted 1 times

 **8608f25** 2 months ago

Option D is incorrect because it refers to "AES-256 with a customer managed key" in a way that mixes concepts. AES-256 is the encryption standard used by SSE-S3 and does not directly apply to the use of customer managed keys. For managing keys, the correct approach is through SSE-KMS, which allows specifying a customer managed AWS KMS key.

upvoted 1 times

 **ninomfr64** 3 months, 1 week ago

Selected Answer: B

Not A. SSE-S3 with a customer managed key is not an actual option as SSE-S3 uses S3 managed keys

Not C. S3 bucket policy cannot automatically encrypt objects on GetObject and PutObject requests. With policies you can only allow/deny

actions from specific principals

Not D. AES-256 with a customer managed key is not an actual option as AES-256 is used as value for the header x-amz-server-side-encryption to set SSE-S3 on putObject and SSE-S3 uses S3 managed keys

B is correct as server-side encryption with AWS KMS managed encryption keys (SSE-KMS) is an actual default encryption settings for S3 bucket and you can use S3 bucket policy to deny unencrypted PutObject. These ensure all new objects will be encrypted with customer managed keys. Then using aws cli to re-upload all object will overwrite existing objects (versioning is not enabled)

upvoted 2 times

✉ **ismeagain** 3 months, 3 weeks ago

Selected Answer: D

i think D is correct as B is mentioned KMS managed key..

upvoted 1 times

✉ **Impromtu** 3 months, 3 weeks ago

Selected Answer: B

A - You cannot define your own key

B - Correct. Using SSE-KMS and your own KMS customer managed key, you adhere to the requirements

C - Does not encrypt existing objects, and you cannot "change" the request to "automatically" encrypt

D - You can only choose between SSE-S3 and SSE-KMS (or now DSSE-KMS as well) for default encryption. Underlying the SSE-S3 refers to AES-256 (cfr. "s3:x-amz-server-side-encryption": "AES256") but you cannot specify your customer managed key in that case.

upvoted 1 times

✉ **_Juwon** 4 months ago

Selected Answer: B

If use KMS-CMK , wouldn't it be possible to manage keys directly while using KMS? Does anyone have an opinion on this?

upvoted 1 times

✉ **eurriola10** 4 months, 1 week ago

Selected Answer: B

B is correct

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html#aws-managed-customer-managed-keys>

When you use server-side encryption with AWS KMS (SSE-KMS), you can use the default AWS managed key, or you can specify a customer managed key that you have already created.

upvoted 2 times

✉ **jainparag1** 4 months, 2 weeks ago

Selected Answer: D

Between B and D, it's D which is correct because of cust managed clause.

upvoted 1 times

✉ **heatblur** 4 months, 3 weeks ago

Selected Answer: B

B is the best choice

SSE-KMS allows the use of customer-managed keys. Setting an S3 bucket policy to deny unencrypted PutObject requests ensures that all future uploads are encrypted. Re-uploading all objects in the S3 bucket using the AWS CLI would encrypt existing objects with the new KMS key. This option meets all the requirements.

upvoted 1 times

✉ **jainparag1** 4 months, 2 weeks ago

It's wrong since the key is managed by AWS but they want key to be manged by Security Team. Hence the correct answer is D.

upvoted 2 times

✉ **severlight** 4 months, 4 weeks ago

Selected Answer: B

see dpatra's comment

upvoted 1 times

✉ **KCjoe** 5 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>

SSE-C support AES-256. The question just say "custom managed", it didn't say KMS custom managed, of course it is SSE-C - ustomer-provided keys.

upvoted 2 times

✉ **dpatra** 6 months ago

Selected Answer: B

This aligns with the requirement to use keys managed by the company's security team. With SSE-KMS, you can create and manage encryption keys, fulfilling the requirement. Set an S3 bucket policy to deny unencrypted PutObject requests. Use the AWS CLI to re-upload all objects in the S3 bucket.

upvoted 3 times

 **rif** 6 months ago

D. customer managed key not aws managed key
upvoted 1 times

 **longs** 6 months, 1 week ago

Selected Answer: D

For who is choosing B
KMS AWS managed key can't be managed by customer except AWS
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#key-mgmt>
upvoted 4 times

Question #52

Topic 1

A company is running a web application in the AWS Cloud. The application consists of dynamic content that is created on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group that is configured as a target group for an Application Load Balancer (ALB).

The company is using an Amazon CloudFront distribution to distribute the application globally. The CloudFront distribution uses the ALB as an origin. The company uses Amazon Route 53 for DNS and has created an A record of www.example.com for the CloudFront distribution.

A solutions architect must configure the application so that it is highly available and fault tolerant.

Which solution meets these requirements?

- A. Provision a full, secondary application deployment in a different AWS Region. Update the Route 53 A record to be a failover record. Add both of the CloudFront distributions as values. Create Route 53 health checks.
- B. Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region. Update the CloudFront distribution, and create a second origin for the new ALB. Create an origin group for the two origins. Configure one origin as primary and one origin as secondary.
- C. Provision an Auto Scaling group and EC2 instances in a different AWS Region. Create a second target for the new Auto Scaling group in the ALB. Set up the failover routing algorithm on the ALB.
- D. Provision a full, secondary application deployment in a different AWS Region. Create a second CloudFront distribution, and add the new application setup as an origin. Create an AWS Global Accelerator accelerator. Add both of the CloudFront distributions as endpoints.

Correct Answer: B

Community vote distribution



B (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: B

The correct answer is B. Provisioning an ALB, an Auto Scaling group, and EC2 instances in a different AWS region provides redundancy and failover capability for the application. By creating a second origin for the new ALB in the second region, the CloudFront distribution can automatically route traffic to the healthy origin in case of an issue with the primary origin. This ensures that the application remains highly available and fault-tolerant.

Option A is not correct because it uses Route 53 failover records, which can result in increased latency and DNS resolution time for clients. Option C is not correct because it doesn't provide redundancy for the load balancer, which is a critical component of the application. Option D is not correct because it does not provide redundancy for the application in case of an issue with the primary origin in the first region.

upvoted 22 times

 **God_Is_Love**  1 year, 1 month ago

For HA, always user second region but its there in all options. Here Cloudfront distribution multiple origin groups is the key point Solution Architects should know of. Configuring 2nd origin as ALB --> EC2 instances target group in another regions setup makes highly available. If Cloudfront detects that response is Http error (fault) code like 4XX,5XX etc, it will failover to secondary origin (ALB of another region) which makes this fault tolerant. Answer is B.

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

upvoted 10 times

 **Dgix**  2 weeks, 5 days ago

Selected Answer: B

A is wrong because CloudFront distros can't be added to Route 53.

B is correct

C is wrong because ALBs are single region and don't do failover.

D would work, but is overengineered in this context.

upvoted 1 times

 **8608f25** 2 months ago

Selected Answer: B

Option B is correct because it involves creating a redundant setup in another AWS Region with its own ALB, Auto Scaling group, and EC2 instances. By updating the CloudFront distribution to include a second origin for the new ALB and creating an origin group with primary and secondary origins, CloudFront can automatically route traffic to the secondary origin if the primary is unhealthy. This setup leverages CloudFront's global reach to improve availability and fault tolerance without the need for DNS-level changes.

Option A is not correct because it suggests creating a secondary deployment and updating the Route 53 A record to be a failover record with both CloudFront distributions as values. While Route 53 health checks and failover records can improve availability, CloudFront distributions themselves cannot be directly specified as values in A records for failover purposes. This option might lead to confusion in its implementation details.

upvoted 1 times

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

Selected Answer: B

Who the hell cooked this terrible question design.

Usually, HA means single region, DR means cross region. The question is asking HA while all the answer are using cross region solutions.

When Dynamic content is involved, the dynamic content has to be stored in a persistent storage, while question says the dynamic content is stored on the EC2 instances in an ASG, which means the EC2 instances are ephemeral.

And when Dynamic content is involved, no matter HA or DR, a replication component must be built so that the Dynamic content will be replicated to the other side so that it can be available when the event happens. While, none of the answers mention replication at all.

upvoted 1 times

✉ **ninomfr64** 3 months, 1 week ago

Selected Answer: B

Not A. CloudFront is a global service, having two distributions will not increase fault-tolerance

Not C. Single ALB is a single-point-of-failure and also you cannot have Target Group in a different region

Not D. CloudFront is a global service, having two distributions will not increase fault-tolerance and combining CloudFront with AWS Global Accelerator makes no sense

B is correct as provisioning an ALB, an Auto Scaling group, and EC2 instances in a different AWS region provides redundancy and failover capability for the application. The origin group is the right way to enable failover for CloudFront distributions origin

upvoted 1 times

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

Selected Answer: B

Not Create a second CloudFront Distribution, it's update the distribution with multi origins.

Ref:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html#concept_origin_groups.creating
"Make sure the distribution has more than one origin. If it doesn't, add a second origin."

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

it's a B

upvoted 1 times

✉ **[Removed]** 9 months, 2 weeks ago

Selected Answer: B

Both A and B would work, but A is tangibly worse in terms of performing fail-over (because it relies on DNS) and gains you little, since CloudFront is highly available by its nature, making a second CF distribution doesn't improve your application's robustness.

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: B

Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region.

upvoted 1 times

✉ **dev112233xx** 1 year ago

Selected Answer: B

B is the best solution with very high availability (compared to the R53 failover solution)

upvoted 1 times

✉ **Ajani** 1 year, 1 month ago

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

upvoted 1 times

✉ **Sarutobi** 1 year, 1 month ago

Selected Answer: B

B looks good.

upvoted 1 times

✉ **massa** 1 year, 2 months ago

Selected Answer: B

B is correct.

C is not correct, because ALB is regional service, so ALB have to be added too.

upvoted 2 times

Question #53

Topic 1

A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts. AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enabled on all of its accounts.

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to their applications securely.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be invoked when the JSON file is updated. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges.
- B. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges. Configure the rule to automatically remediate any noncompliant security group that is detected.
- C. In the transit account, create a VPC prefix list with all of the internal IP address ranges. Use AWS Resource Access Manager to share the prefix list with all of the other accounts. Use the shared prefix list to configure security group rules in the other accounts.
- D. In the transit account, create a security group with all of the internal IP address ranges. Configure the security groups in the other accounts to reference the transit account's security group by using a nested security group reference of "/sg-1a2b3c4d".

Correct Answer: C

Community vote distribution

C (100%)

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: C

The correct answer is option C. In this solution, a VPC prefix list is created in the transit account with all of the internal IP address ranges, and then shared to all of the other accounts using AWS Resource Access Manager. This allows for central management of the IP address ranges, and eliminates the need for manual updates to security group rules in each account. This solution also allows for compliance checks to be run using AWS Config and for any non-compliant security groups to be automatically remediated.

Option A is not correct because it would require manual updates to the JSON file and would also require developers to manually update their security group rules, which would lead to operational overhead.

Option B is not correct because it would require the creation of a new AWS Config managed rule and it would also require manual updates to the security group rules in each account.

Option D is not correct because it would require manual updates to the security group in the transit account and it would also lead to operational overhead.

upvoted 22 times

✉️  **jpa8300** 3 months, 1 week ago

I agree that option C is probably the best one, but B is also correct, there is no manual updates to the SG, the remediation is automated in AWS Config. In option C you also need to manually update the prefix list, no? Imagine a new CIDR appears in the offices.

upvoted 1 times

✉️  **chicagobeef** 3 months ago

I doubt all the security groups in the accounts will use the same CIDR ranges. They just need a way to centrally manage the CIDR prefixes. The question did not say that everyone has to comply and any non-compliant resources need to be remediated.

upvoted 2 times

✉️  **ninomfr64**  3 months ago

Selected Answer: C

Not A. This requires to maintain the JSON file, SNS topic in each account, Lambda to update SG. This is a lot of work, also not clear what accounts holds the S3 with the JSON

Not B. I was not able to spot a managed AWS Config rule that could help in this case

<https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html> (but I do not recall managed rule by hart and this doesn't sound like a remote use case, so in the exam this could trick me)

upvoted 1 times

✉️  **ninomfr64** 3 months ago

Not D. You can reference a VPC SG in other account VPCs when you have VPC peering in place, this is not mentioned in the scenario <https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html>. Since there is a Transit Gateway involved it is unlikely to have VPC peering and the resources in a VPC attached to a transit gateway cannot access the security groups of a different VPC that is also attached to the same transit gateway <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-vpc-attachments.html> (this option initially was not bad for me)

C works well as prefix lists are created exactly for this purpose <https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>
upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C for sure

upvoted 1 times

✉️ **Asds** 10 months ago

Selected Answer: C

Definitely prefix

upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: C

prefix list and RAM

upvoted 2 times

✉️ **dev112233xx** 1 year ago

Selected Answer: C

C makes sense

upvoted 2 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/82131-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉️ **AjayD123** 1 year, 2 months ago

Selected Answer: C

[https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:~:text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20\(RAM\).](https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-network-routing-and-security-administration-with-vpc-prefix-lists/#:~:text=A%20Prefix%20List%20is%20a,Resource%20Access%20Manager%20(RAM).)

upvoted 4 times

Question #54

Topic 1

A company runs a new application as a static website in Amazon S3. The company has deployed the application to a production AWS account and uses Amazon CloudFront to deliver the website. The website calls an Amazon API Gateway REST API. An AWS Lambda function backs each API method.

The company wants to create a CSV report every 2 weeks to show each API Lambda function's recommended configured memory, recommended cost, and the price difference between current configurations and the recommendations. The company will store the reports in an S3 bucket.

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

- A. Create a Lambda function that extracts metrics data for each API Lambda function from Amazon CloudWatch Logs for the 2-week period. Collate the data into tabular format. Store the data as a .csv file in an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- B. Opt in to AWS Compute Optimizer. Create a Lambda function that calls the ExportLambdaFunctionRecommendations operation. Export the .csv file to an S3 bucket. Create an Amazon EventBridge rule to schedule the Lambda function to run every 2 weeks.
- C. Opt in to AWS Compute Optimizer. Set up enhanced infrastructure metrics. Within the Compute Optimizer console, schedule a job to export the Lambda recommendations to a .csv file. Store the file in an S3 bucket every 2 weeks.
- D. Purchase the AWS Business Support plan for the production account. Opt in to AWS Compute Optimizer for AWS Trusted Advisor checks. In the Trusted Advisor console, schedule a job to export the cost optimization checks to a .csv file. Store the file in an S3 bucket every 2 weeks.

Correct Answer: B

Community vote distribution



≡ **masetromain** 1 year, 2 months ago

Selected Answer: B

The correct answer is B. Opting in to AWS Compute Optimizer and creating a Lambda function that calls the ExportLambdaFunctionRecommendations operation is the least development time solution. This option allows you to use the built-in AWS Compute Optimizer service to extract metrics data and export it as a CSV file, which can then be stored in an S3 bucket.

Option A is not correct because it requires the development of a Lambda function that extracts metrics data and collates it into tabular format, which adds development time. Option C is not correct because it requires the setup of enhanced infrastructure metrics, which adds development time. Option D is not correct because it requires purchasing the AWS Business Support plan and using the Trusted Advisor console, which adds development time.

upvoted 18 times

≡ **zozza2023** 1 year, 2 months ago

Selected Answer: B

AWS compute optimizer+ lambda

upvoted 8 times

≡ **khchan123** 1 month ago

Selected Answer: C

The correct answer is C.

Option A involves creating a custom Lambda function to extract metrics data from CloudWatch Logs and generate the CSV report, which would require more development time compared to using the Compute Optimizer service.

Option B is partially correct, as it involves using Compute Optimizer and a Lambda function, but it misses the ability to schedule recurring exports directly within the Compute Optimizer console.

Option D suggests using AWS Trusted Advisor, which is a service for monitoring best practices and resources, but it does not provide the specific Lambda function memory and cost recommendations required in this scenario.

upvoted 1 times

≡ **8608f25** 2 months ago

Selected Answer: B

Option B is the most efficient and straightforward solution. By opting into AWS Compute Optimizer, the company can leverage AWS's service for recommendations on optimal AWS resource configurations based on utilization metrics. Using the ExportLambdaFunctionRecommendations operation allows for automating the retrieval of the desired optimization data with minimal code. Scheduling this operation with an Amazon EventBridge rule to run every 2 weeks and exporting the results directly to a CSV file in an S3 bucket meets all the stated requirements with minimal development effort.

upvoted 1 times

✉ ninomfr64 3 months ago

Selected Answer: C

Not A. This requires some serious development, also not 100% sure CW Logs alone provides all the required info.

Not B. This requires some coding to call the ExportLambdaFunctionRecommendations API

Not D. To create CSV reports (organizational view reports) in Trusted Advisor you need to enable Trusted Advisor in your organization, and AWS Organization is not mentioned in the scenario <https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>

C is the right solution as it allows to schedule report with the required info with no development <https://docs.aws.amazon.com/compute-optimizer/latest/ug/exporting-recommendations.html>. This is misleading for me as it mentions to set up enhanced infrastructure metrics that is only available for EC2, but you can do it without development (you can do it from console), this add cost but the ask focus on development effort.

upvoted 2 times

✉ 8608f25 2 months ago

It is not C. Option C describes using AWS Compute Optimizer and setting up a job within the Compute Optimizer console. However, as of the last update, Compute Optimizer does not provide a direct scheduling feature within the console for exporting recommendations to a CSV file. This option suggests functionality that is not directly available in Compute Optimizer.

upvoted 1 times

✉ AWSCertification2024 3 months, 1 week ago

Selected Answer: B

B is correct

Not C because Enhanced infrastructure metrics is a paid feature of Compute Optimizer that applies to Amazon EC2 instances and instances that are part of Auto Scaling groups.

upvoted 2 times

✉ enk 4 months, 2 weeks ago

Selected Answer: D

Lambda = development. Option D has no development. If you are not familiar with dev'ing - publishing a simple Lambda function can require you to wrap all the Node.js or Python or whatever programming language libraries with it in order to execute correctly within AWS Lambda.

Configuring Trusted Advisor (GUI) or scheduling a job is NOT considered Development.

upvoted 2 times

✉ KCjoe 5 months, 3 weeks ago

Selected Answer: D

Basic plan of Trusted Advisor only has 7 core checks. Business plan has all these, so with LEAST development, it must be business plan.

Check categories

Cost optimization

Performance

Security

Fault tolerance

Service limits

upvoted 4 times

✉ rlf 6 months ago

B.

Option C is not correct because "Enhanced infrastructure metrics is a paid feature of Compute Optimizer that applies to Amazon EC2 instances." <https://docs.aws.amazon.com/compute-optimizer/latest/ug/enhanced-infrastructure-metrics.html>

upvoted 1 times

✉ awsent 7 months ago

Selected Answer: B

Compute Optimizer could generate Export for Lambda Functions one-time. In order to schedule every 2 weeks, EventBridge Scheduler/Schedule Rule should be used.

upvoted 3 times

✉ awsent 7 months ago

Answer: B

<https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>

upvoted 1 times

✉ Simon523 7 months ago

Selected Answer: B

AWS Compute Optimizer helps avoid overprovisioning and underprovisioning four types of AWS resources—Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volumes, Amazon Elastic Container Service (ECS) services on AWS Fargate, and AWS Lambda functions—based on your utilization data.

upvoted 3 times

✉ NikkyDicky 9 months, 1 week ago

Selected Answer: B

its a B

upvoted 1 times

✉ EricZhang 10 months, 2 weeks ago

B - https://docs.aws.amazon.com/compute-optimizer/latest/APIReference/API_ExportLambdaFunctionRecommendations.html

upvoted 3 times

✉ **karma4moksha** 11 months ago

Option D i would say as purchasing business support and truster advisor is money but not development time.

upvoted 3 times

✉ **Pete987** 1 year ago

Answer D

A. Not the least effort

B: There is no mention of the need of creating Lambda for exporting recommendations here: <https://docs.aws.amazon.com/compute-optimizer/latest/ug/exporting-recommendations.html>

C: This would have been correct but "Enhanced infrastructure metrics" setting is only for ec2: <https://docs.aws.amazon.com/compute-optimizer/latest/ug/enhanced-infrastructure-metrics.html>

D: Trusted Advisor can be used.<https://docs.aws.amazon.com/awssupport/latest/user/get-started-with-aws-trusted-advisor.html>

upvoted 2 times

✉ **dev112233xx** 1 year ago

Selected Answer: B

B

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/exporting-recommendations.html>

upvoted 3 times

✉ **ninomfr64** 3 months ago

but this proves correctness of answer C, instead B would make use of ExportLambdaFunctionRecommendations API to export thus requesting some little development https://docs.aws.amazon.com/compute-optimizer/latest/APIReference/API_ExportLambdaFunctionRecommendations.html

upvoted 1 times

Question #55

Topic 1

A company's factory and automation applications are running in a single VPC. More than 20 applications run on a combination of Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon RDS.

The company has software engineers spread across three teams. One of the three teams owns each application, and each team is responsible for the cost and performance of all of its applications. Team resources have tags that represent their application and team. The teams use IAM access for daily activities.

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.

Which combination of actions will meet these requirements? (Choose three.)

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

Correct Answer: ACF

Community vote distribution

ACF (52%)

ADF (48%)

 **masetromain**  1 year, 2 months ago

Selected Answer: ACF

A, C and F are the correct answers because they provide the required cost reports and analysis for the company's applications and teams.

A. Activating user-defined cost allocation tags that represent the application and the team allows the company to assign costs to specific applications and teams. This allows the company to see how much each application and team is costing them, which is important for cost forecasting and budgeting.

C. Creating a cost category for each application in Billing and Cost Management allows the company to group costs by application. This makes it easier to understand the costs associated with each application and to compare the costs of different applications over time.

F. Enabling Cost Explorer allows the company to analyze costs and usage over time, and to create custom reports and forecasts. This is important for understanding the costs associated with each application and team, and for forecasting future costs.

upvoted 36 times

 **masetromain** 1 year, 2 months ago

B is not correct because AWS generated cost allocation tags are automatically created for some AWS resources, but it does not provide the required cost reports and analysis for the company's applications and teams.

Option D is not correct because IAM access controls are used to limit access to the billing and cost management features, but it is not necessary to configure it to meet the requirements.

E is not correct because Creating a cost budget allows the company to set a budget for their costs and to receive alerts when costs exceed the budget, but it does not provide the required cost reports and analysis for the company's applications and teams.

upvoted 7 times

 **a_c_** 11 months, 1 week ago

With out granting IAM Access, IAM users cannot access Billing console, so s cannot see the Cost explorer
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/control-access-billing.html>.

Question says teams are responsible for cost

I

upvoted 8 times

 **djeong95** 1 month, 1 week ago

In addition to the IAM access problem answer ACF will face, the problem statement already presents us with the information that resources are already tagged by team/application. Creating cost category seems redundant and even if you did create this redundancy, you are faced with the IAM access problem.

If each team is responsible for the cost and the performance, they would need access to the billing console for their team.

upvoted 1 times

 **e4bc18e** 3 days, 10 hours ago

So you are wrong, tags can be applied to applications so you can easily find them but unless they are actually activated as user defined billing tags then you will not be able to use those tags in cost analysis. Also you have to enable cost explorer it is not enabled by default and cost explorer lets you see the previous 12 months and creates projections for the next 12, so without that option you will not meet the objective.

upvoted 1 times

 **spd**  1 year, 1 month ago

Selected Answer: ADF

Correct ADF - Since resources are tagged, C may not require ?

upvoted 16 times

 **TonytheTiger**  1 week ago

Selected Answer: ACF

Option ACF and NOT ADF - Cost allocation helps you identify who is spending what, within your organization. Cost categories is a cost allocation service to help you map your AWS costs, to your unique internal business structures.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

Selected Answer: ACF

Focusing on enabling the company to attribute AWS costs to each application or team, create cost comparison reports for the last 12 months, and forecast costs for the next 12 months,..Answer: A, C, F.

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

Explanation of Exclusions: B, D, F

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

E. Create a cost budget: Creating a cost budget is valuable for managing expenses and avoiding overspending, but it does not directly facilitate the attribution of costs to applications or teams, nor does it aid in the creation of historical comparison reports or forecasts in the manner required by the company.

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

D. Activate IAM access to Billing and Cost Management: While important for ensuring that team members can access billing information, this action itself doesn't contribute directly to organizing or reporting on costs by application or team, nor does it facilitate forecasting.

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

[correction for typo error above] Explanation of Exclusions: B, D, E

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

here's the detailed recommendation:

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

A. Activate user-defined cost allocation tags: User-defined tags need to be activated for cost allocation purposes. These tags, representing applications and teams, are crucial for attributing costs accurately to the responsible entities within the company. Once activated, these tags will appear in the AWS Billing and Cost Management dashboard, enabling detailed tracking and reporting based on the specified tags.

upvoted 1 times

 **mav3r1ck** 2 weeks, 3 days ago

F. Enable Cost Explorer: Cost Explorer is essential for analyzing past spending and forecasting future costs. It allows for detailed reports that can compare costs from the last 12 months and helps in forecasting for the next 12 months. With the data segmented by user-defined cost allocation tags, Cost Explorer can provide the insights needed to meet the company's reporting and forecasting requirements.

C. Create a cost category for each application in Billing and Cost Management: Cost categories allow for the organization of cost and usage data into logical groups that reflect the company's internal structure, such as by application or team. By leveraging the user-defined tags activated in step A, cost categories can automate the process of cost attribution to these entities, simplifying the creation of targeted reports and forecasts.

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: ACF

Agree with ACF

upvoted 1 times

 **Dgix** 4 weeks, 1 day ago

Selected Answer: ACF

For the full granularity, C is needed rather than D.

upvoted 1 times

 **a54b16f** 1 month, 1 week ago

Selected Answer: ADF

C is not needed. Option A activated the tag, so we could use tags to generate reports. There is no need to create cost category for individual applications, which could be a huge effort and not practical, what if you have hundreds of applications...

upvoted 1 times

 **a54b16f** 1 month, 1 week ago

Selected Answer: ADF

Correct ADF - Since resources are tagged

upvoted 1 times

 **8608f25** 2 months ago

Selected Answer: ACF

Correct answers are:

- A. Activate the user-defined cost allocation tags that represent the application and the team. User-defined cost allocation tags allow you to organize your AWS bill by categorizing costs according to your business's organizational structures (e.g., by application or team).
- C. Create a cost category for each application in Billing and Cost Management. Cost categories enable you to create custom groupings of your AWS costs. By creating a cost category for each application, you can group costs more granularly, which is helpful for detailed reporting and cost attribution to specific teams or applications.
- F. Enable Cost Explorer. Cost Explorer is a tool that allows you to visualize, understand, and manage your AWS costs and usage over time. By enabling Cost Explorer, you can create detailed reports to compare costs from the last 12 months and forecast costs for the next 12 months, meeting the company's requirements for cost management and planning.

upvoted 1 times

 **8608f25** 2 months ago

Option B is not correct. It refers to activating AWS generated cost allocation tags. While AWS-generated tags can provide useful information, they do not typically represent specific applications or teams unless those entities are directly associated with AWS-defined resources or actions. For custom application and team tracking, user-defined tags (Option A) are more appropriate.

upvoted 1 times

 **ninomfr64** 3 months ago

Selected Answer: ADF

Not B. AWS generated tags do not allow you to identify app. You need user-defined tags for this

Not C. Cost Categories allows to define rule to group costs into categories using different dimensions such as: account, tag, service, charge type, and other cost categories. In this scenario User-defined tags are enough to identify applications and teams.

Not E. Budget doesn't help you in creating reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. Use Cost Explorer instead-

upvoted 3 times

 **jpa8300** 3 months, 1 week ago

Selected Answer: ADF

See below severlight explanation. I agree with it.

upvoted 3 times

 **Dips3009** 3 months, 3 weeks ago

can someone help me with this solutions, as I am confused between ACF and ADF

upvoted 1 times

 **ixdb** 3 months, 4 weeks ago

Selected Answer: ACF

ACF is right.

upvoted 2 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: ADF

without IAM access activated only the root account has access to billing info, you need to enable Cost Explorer by simply opening the Cost Explorer console the first time.

upvoted 5 times

 **severlight** 4 months, 4 weeks ago

and you don't need a cost category for each application, as a category is needed for aggregation and you already have all the tags you need to aggregate on the application level.

upvoted 4 times

 **rif** 6 months ago

ADF are correct. user defined cost allocation tag is enough(no need of cost category in this use case because "A company's factory and automation applications are running in **a single VPC**" not multiple accounts so cost categories of C may not be needed.

Cost category is for multiple perspectives under organization structures across multiple accounts with rule based engine. For cost categories : "You can create groupings of costs using cost categories. For example, assume that your business is organized by teams and that each team has multiple accounts within."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>

upvoted 2 times

 **totten** 6 months, 1 week ago

Selected Answer: ADF

A, D, and F. Here's why each of these actions is necessary:

A. Activating user-defined cost allocation tags allows you to tag AWS resources (like EC2 instances, RDS databases, and ECS services) with metadata that represents the application and team. This enables you to allocate costs accurately.

D. Activating IAM access to Billing and Cost Management is necessary to allow the teams to access the cost data and reports. This is crucial for them to analyze costs and generate their own reports.

F. Enabling Cost Explorer is essential for creating custom cost and usage reports. Cost Explorer provides various visualization and reporting capabilities that allow you to filter, group, and analyze costs based on your tags and other criteria. You can create cost allocation reports for each application and team and use these reports to compare costs and forecast future costs.

upvoted 5 times

 **totten** 6 months, 1 week ago

While option B (activating AWS generated cost allocation tags) can be useful, it's not explicitly required to meet the stated requirements. Option C (creating a cost category for each application) is not typically used for tag-based cost allocation and doesn't provide the same level of granularity and flexibility as tags. Option E (creating a cost budget) is a useful practice but is not directly related to the task of allocating costs to applications and teams.

upvoted 2 times

 **awsent** 7 months ago

Selected Answer: ACF

Since the team is already using IAM for the daily access, kind of implies they will know how to enable the right IAM access.

upvoted 1 times

Question #56

Topic 1

An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.

The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.

How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?

- A. Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
- B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC.
- C. Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
- D. Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

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

✉  **masetromain**  1 year, 2 months ago

Selected Answer: B

The correct solution is B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC. This will ensure that the web application can continue to call the third-party API after the migration by using the customer-owned public IP addresses that were assigned to the NAT gateways. This ensures that the third-party API will only see traffic coming from the customer-owned IP addresses that are on the allow list. Option A,C and D doesn't make sense in this context.

upvoted 16 times

✉  **ninomfr64**  3 months ago

Selected Answer: B

In this scenario EC2 instances access the 3P APIs via NAT Gateway. 3P API FW see IP of the NAT Gateway. You can assign Elastic IP to NAT Gateway and you can allocate an IP address from a pool that you have brought to your AWS account to the Elastic IP. Thus B is correct.
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>

upvoted 2 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

its a B

upvoted 1 times

✉  **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

KEYWORD = NAT gateways in the VPC

upvoted 1 times

✉  **AWS_Sam** 10 months, 3 weeks ago

B is the only option that makes sense.

upvoted 1 times

✉  **SkyZeroZx** 10 months, 3 weeks ago

Selected Answer: B

B make sense

upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: B

Register a block of customer owned public IP's

upvoted 2 times

✉  **dev112233xx** 1 year ago

Selected Answer: B

B is the only solution

upvoted 2 times

  **zozza2023** 1 year, 2 months ago**Selected Answer: B**

The correct solution is B

upvoted 4 times

Question #57

Topic 1

A company with several AWS accounts is using AWS Organizations and service control policies (SCPs). An administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllActions",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Sid": "DenyCloudTrail",
      "Effect": "Deny",
      "Action": "cloudtrail:*",
      "Resource": "*"
    }
  ]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the administrator address this problem?

- A. Add s3:CreateBucket with "Allow" effect to the SCP.
- B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
- C. Instruct the developers to add Amazon S3 permissions to their IAM entities.
- D. Remove the SCP from account 1111-1111-1111.

Correct Answer: C

Community vote distribution



✉ **Atila50** 1 year, 2 months ago

Selected Answer: C

SCP doesn't grant permission

upvoted 21 times

✉ **c73bf38** 1 year, 1 month ago

Per the DOCS:

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features. For instructions on enabling SCPs, see Enabling and disabling policy types.

upvoted 6 times

✉ **c73bf38** 1 year, 1 month ago

SCPs alone are not sufficient to granting permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. The administrator must still attach identity-based or resource-based policies to IAM users or roles, or to the resources in your accounts to actually grant permissions. The effective permissions are the logical intersection between what is allowed by the SCP and what is allowed by the IAM and resource-based policies.

upvoted 9 times

✉ **zhangyu20000** 1 year, 2 months ago

C is correct

SCP policy allow everything except clouptrail. SCP is boundary but it does not give allow to IAM users. You have to configure allow for every IAM

upvoted 12 times

✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: C

C, SCP is just a distractor, the users need direct permissions

upvoted 1 times

8608f25 2 months ago

Selected Answer: C

The problem described does not originate from the Service Control Policy (SCP) itself based on the SCP content provided. The SCP allows all actions ("Action": "") except for actions related to AWS CloudTrail ("Action": "CloudTrail:"), which are explicitly denied. Therefore, the inability for developers to create Amazon S3 buckets is not due to this SCP, as the SCP does not restrict S3 actions.
Given the situation, the correct way to address the developers' inability to create Amazon S3 buckets would be:
* C. Instruct the developers to add Amazon S3 permissions to their IAM entities.

Option C is the correct action because the issue likely stems from the IAM permissions (or lack thereof) assigned to the developers' IAM entities (users, groups, or roles). IAM permissions are required to perform actions within AWS accounts, such as creating S3 buckets. If developers lack the necessary IAM permissions, they would not be able to create S3 buckets regardless of the SCP settings.

upvoted 1 times

ninomfr64 3 months ago

Selected Answer: C

The SCP in the scenario is allowing any actions with the exception of clouptrail. Thus, the SCP is not preventing user to create S3 bucket. If the user cannot create a bucket, then the user IAM user/role is missing permissions to create S3 bucket.

upvoted 2 times

shaaam80 4 months, 1 week ago

Selected Answer: C

Answer C.

upvoted 1 times

NikkyDicky 9 months, 1 week ago

Selected Answer: C

it's a C

upvoted 1 times

javitech83 9 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

SkyZeroZx 9 months, 3 weeks ago

Selected Answer: C

I just wanted to add my vote to the mix to hopefully drown out the wrong votes.

Its definitely C. SCP is only a guardrail, it doesn't actually grant access. So the users would need to be given s3 access separately.

And to address the wrong answer, A isn't correct because creating an s3 bucket is not a clouptrail action. Being denied clouptrail wouldn't deny s3 actions.

upvoted 2 times

bhanus 10 months ago

C is the answer. SCP DONT grant permissions. They just set boundaries on what account is capable of giving access to all users. For example, we applied a SCP on an OU that has account A. This SCP has S3fullAWSaccess. This does NOT mean that any IAM user can perform any S3 action. You still need to explicitly define IAM permissions for user to perform action on S3. This is called whitelisting.
Another example, You wrote an SCP that DENIES S3 access and applied it to an OU that has account B. Now Lets say ROOT user of Account B (who got admin privileges) tries to create S3 bucket, they get DENIED error as SCP has already set a bounday saying NOONE in this OU can access S3

upvoted 2 times

Asds 10 months ago

Selected Answer: C

Need to deal with iam policy auth now

upvoted 1 times

Asds 10 months ago

C is right

upvoted 1 times

leehjworking 11 months ago

I am not sure the given situation is possible.

When I tested, member (1111-1111-1111) could create bucket without any policy which can be attached or detached by the oneself.

upvoted 2 times

leehjworking 11 months ago

Are developers allowed to modify their IAM entities in the situation of option C? If so, I am not sure this is the best practice.

upvoted 2 times

mfsec 1 year ago

Selected Answer: C

C is correct

upvoted 2 times

✉️  **dev112233xx** 1 year ago

Selected Answer: C

SCP is not enough. IAM permission is needed

upvoted 2 times

✉️  **Damijo** 1 year ago

Selected Answer: C

C - Users and roles must still be granted permissions with appropriate IAM permission policies. A user without any IAM permission policies has no access at all, even if the applicable SCPs allow all services and all actions.

upvoted 4 times

✉️  **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

SCPs are confusing.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_strategies.html#orgs_policies_allowlist

They brought this idea with easy control for organizations.

C does not sound like good asking devs to add their own permisisons ?

With AWS organizations, FullAWSAccess is there by default allowing all actions.

As Devs could not access S3 create bucket, am guessing the default FullAWSAccess

has been tampered. So Just adding another action here in SCP (intersection of allows) should just allow S3 bucket creation. I'd choose A.

upvoted 3 times

✉️  **Ikyixoayffasdrlaqd** 1 year, 1 month ago

No not correct.

upvoted 2 times

✉️  **God_Is_Love** 1 year, 1 month ago

then you need to explain why not and whats correct

upvoted 1 times

✉️  **testingaws123** 1 year, 1 month ago

look at the first lines of the code, it allows everything. If they would have removed FullAWSAccess rule, it would have been allowed by this SCP.

So probably IAM issue.

upvoted 2 times

✉️  **deegadaze1** 11 months ago

You are wrong ! God_Is_Love was right ...

Check the second code that deny All after CloudTrail

CloudTrail;* -- * Deny all , you will need to add S3 manually!

upvoted 1 times

✉️  **btx** 9 months, 3 weeks ago

No, it does not work like that. The first statement includes all, which includes all S3 actions. Adding any allow of any kind to this policy has not effect act all. Everything is allowed already (except CloudTrail that is explicitly denied)

upvoted 1 times

✉️  **deegadaze1** 11 months ago

Correct !!!

Because of * after the CloudTrail;* at the second DENY RULE of the code.

upvoted 1 times

✉️  **btx** 9 months, 3 weeks ago

The SCP has alreadt an Action * Resource * aallow statement wuthout any conditional. So adding any other allow of any type to the SCP has no effect at all. Everything is allowed by the /* statement (and then only CloudTrail is explicitly denied)

upvoted 2 times

Question #58

Topic 1

A company has a monolithic application that is critical to the company's business. The company hosts the application on an Amazon EC2 instance that runs Amazon Linux 2. The company's application team receives a directive from the legal department to back up the data from the instance's encrypted Amazon Elastic Block Store (Amazon EBS) volume to an Amazon S3 bucket. The application team does not have the administrative SSH key pair for the instance. The application must continue to serve the users.

Which solution will meet these requirements?

- A. Attach a role to the instance with permission to write to Amazon S3. Use the AWS Systems Manager Session Manager option to gain access to the instance and run commands to copy data into Amazon S3.
- B. Create an image of the instance with the reboot option turned on. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.
- C. Take a snapshot of the EBS volume by using Amazon Data Lifecycle Manager (Amazon DLM). Copy the data to Amazon S3.
- D. Create an image of the instance. Launch a new EC2 instance from the image. Attach a role to the new instance with permission to write to Amazon S3. Run a command to copy data into Amazon S3.

Correct Answer: A

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: C

The correct answer is C. Taking a snapshot of the EBS volume using Amazon Data Lifecycle Manager (DLM) will meet the requirements because it allows you to create a backup of the volume without the need to access the instance or its SSH key pair. Additionally, DLM allows you to schedule the backups to occur at specific intervals and also enables you to copy the snapshots to an S3 bucket. This approach will not impact the running application as the backup is performed on the EBS volume level.

Option A is not correct because the instance would need an IAM role with permission to write to S3 and access to the instance via Systems Manager Session Manager.

Option B is not correct because it would require stopping the instance, which would impact the running application.

Option D is not correct because it would require stopping the instance and creating a new EC2 instance, which would impact the running application.

upvoted 31 times

✉️ **mav3r1ck** 2 weeks, 3 days ago

Not true! Feel free to challenge me if you think I am wrong.

Taking a snapshot of the EBS volume using Amazon DLM is a straightforward approach to ensure data durability and availability. However, this option does not directly address the requirement to move data to an S3 bucket. While EBS snapshots are stored on S3, they are not accessible as regular S3 objects for direct file manipulation or viewing, meaning additional steps would be required to access and use the data in the format specified by the requirement.

Verdict: Does Not Fully Meet Requirements. DLM manages snapshots for EBS volumes but doesn't facilitate direct, accessible backups to S3 as described.

upvoted 1 times

✉️ **gustori99** 5 days, 15 hours ago

I'll try to challenge you :-)

You can use EBS direct APIs to access data from an EBS snapshot. This is how you can read the data from the snapshot and copy it to S3.

<https://docs.aws.amazon.com/ebs/latest/userguide/ebs-accessing-snapshot.html>

upvoted 1 times

✉️ **Sab** 5 months ago

Your reasoning is wrong . Option A has mentioned that instance profile role is attached to EC2 instance.

upvoted 2 times

✉️ **Atila50** 1 year, 2 months ago

thank you for correcting some of these answers and for the explanations to them

upvoted 3 times

✉️ **mmendozaf** 1 year, 2 months ago

Assuming that EBS is encrypted, I think that is much easier to run the copy command from AW system manager

upvoted 9 times

bititan **Highly Voted** 1 year, 2 months ago

Selected Answer: A

taking a backup of the data to s3. aws doesn't allow up to view snapshots in s3

upvoted 8 times

tmlong18 2 months, 4 weeks ago

The requirement is only 'back up'

upvoted 1 times

TonytheTiger **Most Recent** 1 week ago

Selected Answer: C

Option C: You can back up the data on your Amazon EBS volumes by making point-in-time copies, known as Amazon EBS snapshot. EBS snapshots are stored in Amazon S3

<https://docs.aws.amazon.com/ebs/latest/userguide/ebs-snapshots.html>

AWS DLM - <https://docs.aws.amazon.com/ebs/latest/userguide/ebs-creating-snapshot.html>

upvoted 1 times

mav3r1ck 2 weeks, 3 days ago

Selected Answer: A

Answer.. A!

This option stands out because it allows secure, keyless access to the EC2 instance without requiring the administrative SSH key pair. By attaching an IAM role with S3 write permissions to the instance, you can use Session Manager to execute data copy commands directly to S3. This method does not disrupt the running application, meeting the requirement for continuous operation.

upvoted 1 times

gofavad926 3 weeks, 2 days ago

Selected Answer: A

A meets the requirements by allowing the application team to back up data without interrupting the service and without needing the SSH key pair.

upvoted 1 times

titi_r 1 month ago

Selected Answer: A

"A" seems ok as an option.

"C" is wrong because the question asks you to copy the DATA=FILES to S3. You cannot copy the files from a snapshot made by an encrypted volume to S3 bucket.

upvoted 1 times

marszalekm 1 month, 1 week ago

Selected Answer: A

<https://repost.aws/knowledge-center/ebs-copy-snapshot-data-s3-create-volume>

upvoted 2 times

adelyn||||||| 2 months, 4 weeks ago

C:

Tested, there is no option to copy the snapshot to S3.

upvoted 1 times

adelyn||||||| 2 months, 4 weeks ago

correction: I mean it should be A, not C.

upvoted 2 times

tmlong18 2 months, 4 weeks ago

the snapshot is stored in S3 but fully managed by AWS

upvoted 2 times

hogtrough 1 month, 3 weeks ago

"EBS snapshots are stored in Amazon S3, in S3 buckets that you can't access directly."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

upvoted 1 times

ninomfr64 3 months ago

Selected Answer: A

Not B and D. because when you create an image of the instance, by default Amazon EC2 shuts down the instance, takes snapshots of any attached volumes, creates AMI, and then reboots the instance. This breaks the requirement to keep the app running
<https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/tkv-create-ami-from-instance.html>

Not C. Because EBS snapshots taken by DLM are stored on S3 that is not accessible from users. also you cannot copy snapshots to S3 (you can copy across regions and across accounts, but still in S3 not accessible from users) <https://repost.aws/knowledge-center/ebs-copy-snapshot-data-s3-create-volume>

A does the job, this is not very clean options as to properly run commands via SSM we need SSM Agents installed (this is in the scenario as Amazon Linux 2 comes with the agent) and IAM Role with SSM permission and this specific point is not stated in the scenario.

upvoted 2 times

 **jpa8300** 3 months, 1 week ago

Selected Answer: C

The best option for creating a backup is using some tool, like DLM, or AWS Backup. Option A mention login to the instance (even with SMSM) and copy the files manually! Not very friendly, neither practical.

upvoted 1 times

 **JWalid** 3 months, 1 week ago

Selected Answer: A

Correct Answer: A

- Systems Manager Session Manager does not need SSH access, bastion hosts, or SSH keys
- Supports Linux, macOS, and Windows
- data can be sent to S3
- Make sure the EC2 instances have a proper IAM role to allow Systems Manager actions

upvoted 2 times

 **JMAN1** 3 months, 1 week ago

Selected Answer: A

DLM does not support to copy data to S3. Answer is A.

upvoted 1 times

 **ayadmawla** 4 months ago

Selected Answer: C

Copy is not the same as DLM Snapshot.

upvoted 1 times

 **kmstan** 4 months ago

Selected Answer: A

Attach a Role to the Instance: This is necessary for the instance to have the required permissions to write to Amazon S3.

Use AWS Systems Manager Session Manager: This option allows you to access the instance without the need for an SSH key pair. It provides a secure way to access and manage instances, especially when administrative access is required, as in this case.

Run Commands to Copy Data to Amazon S3: Once you have access to the instance using Systems Manager Session Manager, you can run commands to copy the data from the encrypted Amazon EBS volume to Amazon S3.

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

Selected Answer: A

Between A and C, I'll go for C. Since AWS recommends using Session Manager over SSH and you don't have any control on snapshot taken by DLM.

upvoted 1 times

 **KyleZheng** 2 months, 4 weeks ago

you selected A and go for C? I think A is correct

upvoted 1 times

 **severlight** 4 months, 4 weeks ago

Selected Answer: A

linux 2 - hence ssm agent is installed, and don't think we can view snapshots produced with data lifecycle manager

upvoted 1 times

 **dumpsowner** 5 months, 2 weeks ago

I think :

C

I found another option might be it is good for you - Amazon-Dumps.com

upvoted 1 times

Question #59

Topic 1

A solutions architect needs to copy data from an Amazon S3 bucket in an AWS account to a new S3 bucket in a new AWS account. The solutions architect must implement a solution that uses the AWS CLI.

Which combination of steps will successfully copy the data? (Choose three.)

- A. Create a bucket policy to allow the source bucket to list its contents and to put objects and set object ACLs in the destination bucket. Attach the bucket policy to the destination bucket.
- B. Create a bucket policy to allow a user in the destination account to list the source bucket's contents and read the source bucket's objects. Attach the bucket policy to the source bucket.
- C. Create an IAM policy in the source account. Configure the policy to allow a user in the source account to list contents and get objects in the source bucket, and to list contents, put objects, and set object ACLs in the destination bucket. Attach the policy to the user.
- D. Create an IAM policy in the destination account. Configure the policy to allow a user in the destination account to list contents and get objects in the source bucket, and to list contents, put objects, and set objectACLs in the destination bucket. Attach the policy to the user.
- E. Run the aws s3 sync command as a user in the source account. Specify the source and destination buckets to copy the data.
- F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data.

Correct Answer: ADF

Community vote distribution

✉ **icassp** Highly Voted 1 year, 2 months ago

Selected Answer: BDF

"The above command should be executed with destination AWS IAM user account credentials only otherwise the copied objects in destination S3 bucket will still have the source account permissions and won't be accessible by destination account users." According to <https://medium.com/tensult/copy-s3-bucket-objects-across-aws-accounts-e46c15c4b9e1>.

upvoted 22 times

✉ **masetromain** 1 year, 2 months ago

You are correct, step E should be executed using the IAM user credentials from the destination account. This is because when objects are copied from one bucket to another, the object's permissions (ACLs) are also copied. Therefore, if the objects are copied using the IAM user credentials from the source account, the objects will have the same permissions as they did in the source bucket, which may not include permissions for the user in the destination account. By using the IAM user credentials from the destination account, the objects will have the appropriate permissions for the user in the destination account once they are copied.

upvoted 4 times

✉ **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: BDF

I switch to BDF;

Step B is necessary so that the user in the destination account has the necessary permissions to access the source bucket and list its contents, read its objects.

Step D is needed so that the user in the destination account has the necessary permissions to access the destination bucket and list contents, put objects, and set object ACLs

Step F is necessary because the aws s3 sync command needs to be run using the IAM user credentials from the destination account, so that the objects will have the appropriate permissions for the user in the destination account once they are copied.

The other choices are not correct because :

- A. and C. are about creating policies in the source account but the user who wants to access the data is in the destination account
- E. is about running the command with the source account, which is not suitable because it will lead to copied objects in destination S3 bucket still have the source account permissions and won't be accessible by destination account users.

upvoted 14 times

✉ **8608f25** Most Recent 2 months ago

Selected Answer: BDF

B. Create a bucket policy to allow a user in the destination account to list the source bucket's contents and read the source bucket's objects. Attach the bucket policy to the source bucket. This step ensures that the destination account has the necessary permissions to access the data in the source bucket.

D. Create an IAM policy in the destination account. Configure the policy to allow a user in the destination account to list contents and get objects in the source bucket, and to list contents, put objects, and set object ACLs in the destination bucket. Attach the policy to the user. This step provides the necessary permissions for a user in the destination account to both access the source bucket's contents and write to the destination bucket.

upvoted 1 times

✉ **8608f25** 2 months ago

F. Run the aws s3 sync command as a user in the destination account. Specify the source and destination buckets to copy the data. Performing the sync operation as a user in the destination account, who has been granted the appropriate permissions, ensures that the data can be copied from the source bucket to the destination bucket successfully.

upvoted 1 times

✉ **ninomfr64** 3 months ago

Selected Answer: BDF

Not A. A bucket policy attached to destination bucket cannot allow the source bucket to execute actions
Not C. Because we are picking option B which relies on a policy allowing a user in the destination account.
Not E. Because we are picking options B and D which rely on a user in the destination account

upvoted 1 times

✉ **jpa8300** 3 months, 1 week ago

Selected Answer: BDF

No need for more explanations, the ones below are enough.

upvoted 1 times

✉ **edder** 4 months, 2 weeks ago

Selected Answer: BDF

BD:
<https://repost.aws/knowledge-center/cross-account-access-s3>

F:
<https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html>

upvoted 1 times

✉ **aviathor** 7 months, 1 week ago

Selected Answer: BDF

A is incorrect since a bucket policy cannot allow another bucket to do anything. B. Is however an option since you can indeed create a bucket policy to allow a user in another account to perform operations on the bucket.

Once you have chosen B, then D and F are the only possible choices.

upvoted 2 times

✉ **H4des** 7 months, 3 weeks ago

Selected Answer: BCE

BCE should also work

Create bucket policy at destination bucket to allow permission on source aws user

Create IAM policy for source aws user to list/get/put on both buckets

Run s3 sync command from source bucket to destination bucket

upvoted 1 times

✉ **CuteRunRun** 8 months, 1 week ago

Selected Answer: BDF

I prefer BDF, I do not know why the correct answer is ADF

upvoted 1 times

✉ **Christina666** 9 months, 1 week ago

Selected Answer: BDF

source bucket: allow destination user + list & get contents permission

destination bucket: allow IAM user to get source bucket contents + destination bucket get/list/put objects + aws sync command

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: BDF

it's BDF for sure

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

Selected Answer: BDF

The entire idea of A is wrong (you achieve nothing by giving rights from one bucket to another) so we start from B and the rest are a common sense

upvoted 2 times

✉ **huanaws088** 12 months ago

Selected Answer: BDF

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/copy-data-from-an-s3-bucket-to-another-account-and-region-by-using-the-aws-cli.html>

upvoted 3 times

✉ **God_Is_Love** 1 year, 1 month ago

Logical answer : Who ever uploads to a bucket becomes its owner. So A should ring a flaw in it. Similar issue in C. So straight away, A, C are wrong. that points to B,D to be correct. Refer <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/copy-data-from-an-s3-bucket-in-one-account-and-region-to-another-account-and-region.html>

Now E or F ? the hint is in D. Destination account user has the necessary privileges to get/put objects permission. So choose destination account or run sync/copy commands. So the answer should be B, D , F

upvoted 6 times

 **hobokabobo** 1 year, 1 month ago

The parts BDF fit together in a way that works.

I think choosing this direction (pulling from the destination account) is slightly more secure than then the other other way round(pushng from source to destination) as only read access is granted to the foreign account but no write access - especially regarding human error: one cannot accidentally tamper with the source, so the worst thing that could happen is that one needs to sync again. The other options don't fit together with other parts.

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: BDF

BDF are the answers

upvoted 4 times

 **zhangyu20000** 1 year, 2 months ago

BCE

Source user must have role that can write to destination bucket

upvoted 3 times

Question #60

Topic 1

A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release.

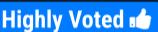
Which solution will meet these requirements?

- A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.
- B. Deploy the application into a new CloudFormation stack. Use an Amazon Route 53 weighted routing policy to distribute the load.
- C. Create a version for every new deployed Lambda function. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load.
- D. Configure AWS CodeDeploy and use CodeDeployDefault.OneAtATime in the Deployment configuration to distribute the load.

Correct Answer: A

Community vote distribution

A (98%)

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: A

A. Create an alias for every new deployed version of the Lambda function. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load is the correct answer as it meets the requirement of supporting a canary release.

Option B is not correct because while it would allow for a canary release, it would involve deploying the new version of the application into a separate CloudFormation stack, which would be a more complex and time-consuming process compared to creating an alias for a new version of the Lambda function.

Option C is not correct because while it would allow for a canary release, it would involve creating a version for every new deployed Lambda function, which would be more complex and time-consuming process compared to creating an alias for a new version of the Lambda function.

upvoted 19 times

✉️  **masetromain** 1 year, 2 months ago

Option D is not correct because AWS CodeDeploy is a deployment service that allows you to automate code deployments to a variety of compute services like EC2 and on-premises servers, but it does not support routing configuration for a canary release on AWS Lambda.

upvoted 6 times

✉️  **karma4moksha** 11 months ago

Thank you masetromain, you have been really helpful for taking the time and providing explanation.

upvoted 1 times

✉️  **Jesuisleon** 11 months ago

He copied from chatgpt, you didn't find it ?

upvoted 7 times

✉️  **ninomfr64** 3 months ago

This is not 100% correct. Actually CodeDeploy support deploy to an AWS Lambda compute platform, the deployment configuration specifies the way traffic is shifted to the new Lambda function versions in your application. You can shift traffic using a canary, linear, or all-at-once deployment configuration. The following lists the predefined configurations available for AWS Lambda canary deployments:

- CodeDeployDefault.LambdaCanary10Percent5Minutes
- CodeDeployDefault.LambdaCanary10Percent10Minutes
- CodeDeployDefault.LambdaCanary10Percent15Minutes
- CodeDeployDefault.LambdaCanary10Percent30Minutes

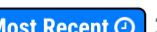
upvoted 1 times

✉️  **Atila50**  1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/28312-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 10 times

✉️  **ninomfr64**  3 months ago

Selected Answer: A

Not B. This introduces R53 in the scenario, but we are not sure if R53 fits in the scenario. To combine R53 and Lambda we should use function URL that is not mentioned and we don't know if the app is public. A lot of uncertainty here

Not C. routing-config is an Alias specific configuration aka Weighted Alias and it is not available for the update-function-configuration command <https://docs.aws.amazon.com/cli/latest/reference/lambda/update-function-configuration.html>

Not D. CodeDeployDefault.OneAtATime is a CodeDeploy option for EC2/on-premise, while in this scenario we need a canary option for Lambda such as CodeDeployDefault.LambdaCanary10Percent5Minutes

A does the job <https://docs.aws.amazon.com/cli/latest/reference/lambda/update-alias.html> and <https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html#configuring-alias-routing>

upvoted 1 times

 **JMAN1** 3 months, 1 week ago

100% A is correct. :) I was confused between D and A. But, this url says Codedeploye.AllatOnce deploy option is not for 'canary release'. https://docs.aws.amazon.com/ko_kr/codedeploy/latest/userguide/deployment-configurations.html

upvoted 1 times

 **totten** 6 months, 1 week ago

Selected Answer: A

Here's why Option A is suitable:

Create an alias: For every new version of your Lambda function, create an alias. Aliases allow you to associate a user-friendly name with a specific version of the function.

Routing configuration: AWS Lambda supports routing configurations that allow you to gradually shift traffic from one alias to another. Using the "routing-config" parameter with the AWS CLI "update-alias" command, you can specify how much traffic each alias should receive.

Gradual release: By configuring the routing, you can control the percentage of traffic directed to the new version (canary). You can gradually increase the traffic percentage as you gain confidence in the new release. If issues arise, you can quickly roll back by adjusting the routing configuration.

upvoted 1 times

 **Christina666** 9 months, 1 week ago

Selected Answer: A

new release-> lambda alias-> update-alias: aws lambda update-alias --function-name my-function --name alias-name --function-version version-number

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

D would be an option if used Lambda-specific config

upvoted 2 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: A

keyword = alias for every new deployed version

is a classic usage for deployment canary for lambdas other option usually is codeDeploy but in this options AllAtOnce then A

upvoted 2 times

 **AMEJack** 11 months, 1 week ago

Sorry OneAtTime

upvoted 1 times

 **AMEJack** 11 months, 1 week ago

Selected Answer: A

CodeDeploy: Although CodeDeploy can help but AllAtOnce is not used for canary traffic shifting.

upvoted 1 times

 God_Is_Love 1 year, 1 month ago

Selected Answer: A

aws update-alias command has routing-config option to route the weighted % traffic

As is correct

<https://aws.amazon.com/blogs/compute/implementing-canary-deployments-of-aws-lambda-functions-with-alias-traffic-shifting/>
Point alias to new version, weighted at 5% (original version at 95% of traffic)

aws lambda update-alias --function-name myfunction --name myalias --routing-config '{"AdditionalVersionWeights" : {"2" : 0.05} }'

upvoted 4 times

 moota 1 year, 1 month ago

Selected Answer: A

According to ChatGPT, The "update-alias" command is a feature of AWS Lambda service. It is used to update the configuration of a Lambda alias, including the routing configuration which can be used for canary releases, blue/green deployments, and other deployment strategies.

upvoted 4 times

 Perkuns 9 months, 4 weeks ago

or you know, you could start thinking yourself rather than use glorified rubbish google

upvoted 1 times

 aliasdoe110 9 months, 3 weeks ago

Dont get mad, get Glad.

upvoted 1 times

✉ **zhangyu20000** 1 year, 2 months ago

A is correct.

D does not have routing to distribute load

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: D

AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and on-premises instances. CodeDeploy allows to perform a canary release, which is a technique that releases new versions of software to a small subset of users or systems before releasing it to the entire infrastructure. This makes it possible to test the new version of the software before releasing it to the entire population.

Option A creates an alias for every new deployed version of the Lambda function, but it doesn't include the ability to perform a canary release. Option B Deploy the application into a new CloudFormation stack, and use an Amazon Route 53 weighted routing policy to distribute the load, this option can be used for canary release, but it is not the best solution for it.

Option C creates a version for every new deployed Lambda function, but it does not include the ability to perform a canary release.

upvoted 1 times

✉ **jaysparky** 1 year, 1 month ago

You have 2 different answers.....I think it is better you delete this.

upvoted 5 times

✉ **chikorita** 10 months, 1 week ago

he can't.....nobody can delete once posted

upvoted 2 times

Question #61

Topic 1

A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS sftp.example.com through the use of Amazon Route 53.

What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

- A. Move the EC2 instance into an Auto Scaling group. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record sftp.example.com in Route 53 to point to the ALB.
- B. Migrate the SFTP server to AWS Transfer for SFTP. Update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname.
- C. Migrate the SFTP server to a file gateway in AWS Storage Gateway. Update the DNS record sftp.example.com in Route 53 to point to the file gateway endpoint.
- D. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record sftp.example.com in Route 53 to point to the NLB.

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

 **tinyflame**  1 year, 2 months ago

Selected Answer: B

A=ALB cannot be used with SFTP
B = Correct
C=Storage Gateway is not an SFTP Server
D=NLB can be used with SFTP, but EC2 is single
upvoted 26 times

 **masetromain**  1 year, 2 months ago

Selected Answer: B

Option B is the correct answer. Migrating the SFTP server to AWS Transfer for SFTP will improve the reliability and scalability of the SFTP solution. AWS Transfer for SFTP is a fully managed SFTP service that enables the company to transfer files directly into and out of Amazon S3 using the SFTP protocol. By using this service, the company can offload the management of the SFTP server to AWS, which will provide high availability, scalability, and security. The company can then update the DNS record sftp.example.com in Route 53 to point to the server endpoint hostname, which will ensure that the SFTP server is reachable on the DNS.

upvoted 10 times

 **masetromain** 1 year, 2 months ago

Option A, C and D do not provide the same level of scalability and reliability as AWS Transfer for SFTP. While placing the EC2 instance behind a load balancer can help improve availability, it will not necessarily improve scalability, and it would still require the company to manage the SFTP server. Option C , migrating the SFTP server to a file gateway in AWS Storage Gateway, would not necessarily improve the scalability and reliability of the SFTP solution, as it would still require the company to manage the SFTP server.

upvoted 4 times

 **rioisverycute** 3 months, 2 weeks ago

How about the cron job?

upvoted 1 times

 **NikkyDicky**  9 months, 1 week ago

Selected Answer: B

B of course
upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword = AWS Transfer for SFTP
then B
upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: B

B is the way to go..
upvoted 3 times

Question #62

Topic 1

A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.

What should the solutions architect do to meet these requirements?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
- B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- C. Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- D. Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI.

Correct Answer: D

Community vote distribution

B (100%)

✉  **masetromain**  1 year, 2 months ago

Selected Answer: B

The correct answer is B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command. This approach allows the solutions architect to export the application as an image in OVF format, which preserves the software and configuration settings, and then import it into Amazon EC2 using the EC2 import command.

upvoted 13 times

✉  **sammyhaj** 3 months ago

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

upvoted 2 times

✉  **masetromain** 1 year, 2 months ago

Option A is incorrect because it uses AWS DataSync and FSx for Windows File Server to replicate the data store, but it doesn't preserve the software and configuration settings of the application.

Option C is incorrect because it uses AWS Storage Gateway to export a CIFS share, but it doesn't preserve the software and configuration settings of the application.

Option D is incorrect because it uses AWS Systems Manager and AWS Backup to create a snapshot of the VM, but it doesn't preserve the software and configuration settings of the application.

upvoted 8 times

✉  **ninomfr64**  3 months ago

Selected Answer: B

A = SMB share cannot host VMware datastore. Also, installing agent modify configuration settings

B = correct

C = not clear how the backup copy is created and what format is used to allow then creating an AMI from it

D = hybrid activation allows SSM to manage on-premise / other cloud VM but doesn't enable AWS Backup. This instead requires a backup gateway to backup VMware environment <https://aws.amazon.com/blogs/storage/backup-and-restore-on-premises-vmware-virtual-machines-using-aws-backup/>

upvoted 2 times

✉  **SorenBendixen** 7 months, 3 weeks ago

Selected Answer: B

The only thing that is missing from the B answer is that the OVF file has to be transformed to a OVA file : <https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>.

upvoted 2 times

✉  **Brightalw** 8 months ago

what the B is wrong is that the VM format, should be OVA or VMDK or VHD, not OVF

upvoted 2 times

✉️ **CuteRunRun** 8 months ago

Selected Answer: B

I prefer B I do not know why the correct is D.

upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

it's a B

upvoted 1 times

✉️ **rbm2023** 11 months, 1 week ago

Selected Answer: B

<https://www.learnitguide.net/2023/01/how-to-migrate-vmware-vm-to-aws-ec2.html>

upvoted 3 times

✉️ **Brightalw** 8 months ago

It said the VM fomat is OVA or VMDK, not OFV

upvoted 1 times

✉️ **asifjanjua88** 1 year ago

I vote to B. Why the admin has selected D as Answer.

upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: B

B is the answer - OFV.

upvoted 2 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

Use VM Import/Export. B is correct . <https://aws.amazon.com/ec2/vm-import/>

upvoted 4 times

✉️ **God_Is_Love** 1 year, 1 month ago

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

Prerequisites

Create an Amazon S3 bucket for storing the exported images or choose an existing bucket. The bucket must be in the Region where you want to import your VMs. For more information about S3 buckets, see the Amazon Simple Storage Service User Guide.

Create an IAM role named vmimport. For more information, see Required service role.

If you have not already installed the AWS CLI on the computer you'll use to run the import commands, see the AWS Command Line Interface User Guide.

upvoted 2 times

✉️ **Signup_Nickname** 1 year, 2 months ago

Selected Answer: B

I vote B

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

upvoted 1 times

Question #63

Topic 1

A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.

The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).
- B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- C. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function. Increase the provisioned concurrency of the Lambda function.
- D. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- E. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instance. Adjust the Lambda function to mount the EFS file share.

Correct Answer: DE

Community vote distribution



✉️ **zhangyu20000** 1 year, 2 months ago

A: create Docker image and save it to ECR
B: run this image on Fargate

No answer should have Lambda the will be time out
upvoted 23 times

✉️ **masetromain** 1 year, 2 months ago

You are correct, both options A and B involve creating a Docker image of the application code and running it on Amazon Elastic Container Service (ECS) using either Fargate or EC2 as the launch type. These options would allow for more control over the resources allocated to the application and potentially prevent timeout errors. Option A is necessary to create the image and store it in a registry, and option B is necessary to run the image on Fargate which is a managed container orchestration service that eliminates the need for provisioning and scaling of the underlying infrastructure.

upvoted 7 times

✉️ **masetromain** 1 year, 2 months ago

Selected Answer: AB

The correct answer is A and B.

A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).

- This step is necessary to package the application code in a container and make it available for running on ECS.

B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.

- This step is necessary to run the containerized application on Fargate, which is a fully managed container orchestration service that eliminates the need to provision and scale the underlying infrastructure.

upvoted 14 times

✉️ **masetromain** 1 year, 2 months ago

Option C and E are not correct because they don't address the problem of timeout errors. AWS Step Functions and Amazon Elastic File System (EFS) are services that can be used to coordinate and manage workflows and file storage respectively, but they don't help with the specific problem of the Lambda function timing out.

Option D is not correct because AWS Fargate is a serverless compute engine for containers that eliminates the need for provisioning and scaling the underlying infrastructure.

It means that the company does not have to manage the underlying infrastructure, which is what the company wants.

upvoted 5 times

 **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: AB

AB, ECR + ECS Margate

upvoted 1 times

 **Ak47g** 3 months, 1 week ago

Selected Answer: AB

A: create Docker image and save it to ECR

B: run this image on Fargate

upvoted 1 times

 **Nicoben** 3 months, 3 weeks ago

Selected Answer: AB

A: create docker image and store in on ECR

B: run it on a AWS-managed infrastructure (as required)

upvoted 1 times

 **blackgamer** 5 months, 2 weeks ago

The correct answer is A and B. But Lambda function should be replaced with EventBridge.

upvoted 1 times

 **ggrodsckiy** 5 months, 3 weeks ago

Selected Answer: BC

B - 100%

C OR E ??

upvoted 1 times

 **CuteRunRun** 8 months ago

Selected Answer: AB

I think is AB

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: AB

it's AB

upvoted 1 times

 **Jonalb** 9 months, 2 weeks ago

Selected Answer: AB

AB

its correct!

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: AB

A + B

A , basic dockerized the application and use Elastic Container Register

B , deploy how serverless with fargate without overhead management infrastructure

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

A + B.

upvoted 2 times

 **dev112233xx** 1 year ago

Selected Answer: AB

A+B makes sense to me

upvoted 2 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: AB

Based on Serverless solutions used, need to go with Fargate in combination with either ECS/EC2. As company does not want to manage infra, we go for because Fargate-ECS combo as Fargate-EC2 needs more maintenance . That means D is out. E is obviously out EFS does not

contribute to lambda invocation timeouts.

C is wrong because, increased concurrency (more lambda versions) won't solve timeouts.

That leaves A and B as right answers.

upvoted 4 times

 **klog** 1 year, 1 month ago

Selected Answer: AB

C is not right, question clearly said no involve infrastructure, EC2 is a infrastructure, Lamda time out 15 mins.

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: AB

lamda will time out

A: create Docker image and save it to ECR

B: run this image on Fargate

upvoted 2 times

 **Musk** 1 year, 2 months ago

Selected Answer: AB

AB makes most sense

upvoted 2 times

Question #64

Topic 1

A company has an organization in AWS Organizations. The company is using AWS Control Tower to deploy a landing zone for the organization. The company wants to implement governance and policy enforcement. The company must implement a policy that will detect Amazon RDS DB instances that are not encrypted at rest in the company's production OU.

Which solution will meet this requirement?

- A. Turn on mandatory guardrails in AWS Control Tower. Apply the mandatory guardrails to the production OU.
- B. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower. Apply the guardrail to the production OU.
- C. Use AWS Config to create a new mandatory guardrail. Apply the rule to all accounts in the production OU.
- D. Create a custom SCP in AWS Control Tower. Apply the SCP to the production OU.

Correct Answer: B

Community vote distribution

B (95%) 5%

 **masetromain**  1 year, 2 months ago

Selected Answer: B

The correct answer is B. AWS Control Tower provides a set of "strongly recommended guardrails" that can be enabled to implement governance and policy enforcement. One of these guardrails is "Encrypt Amazon RDS instances" which will detect RDS DB instances that are not encrypted at rest. By enabling this guardrail and applying it to the production OU, the company will be able to enforce encryption for RDS instances in the production environment.

Option A is incorrect because mandatory guardrails are pre-defined by AWS and cannot be customized.

Option C is incorrect because AWS Config does not provide mandatory guardrails for RDS instances.

Option D is incorrect because AWS Control Tower does not provide a feature called custom SCP (Service Control Policy), it uses guardrails instead.

upvoted 17 times

 **pitakk**  1 year, 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>
upvoted 5 times

 **Musk** 1 year, 2 months ago

The only thing is that this option talks about guardrails, while the article talks about controls, not mandatory.

upvoted 1 times

 **8608f25**  1 month, 4 weeks ago

Selected Answer: B

Option B is correct because AWS Control Tower's strongly recommended guardrails include checks for best practices and additional security measures that are not enforced by default but are highly recommended. Among these, there is likely a guardrail that can detect unencrypted RDS DB instances, aligning with the company's requirement. Applying this guardrail to the production OU will ensure that all RDS DB instances in that OU are checked for encryption at rest.

upvoted 1 times

 **ninomfr64** 3 months ago

Selected Answer: B

A = Mandatory controls are owned by AWS Control Tower, and they apply by default to every OU on your landing zone and they can't be deactivated

B = correct <https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

C = You cannot create new mandatory controls as they are owned by AWS Control Tower

D = You can create custom SCP in AWS Control Tower as part of the Customizations for AWS Control Tower

<https://docs.aws.amazon.com/controlltower/latest/userguide/cfcn-set-up-custom-scps.html> However this requires a lot of work

upvoted 2 times

 **ninomfr64** 3 months ago

Note on D, the question is asking to detect and not to mandate, thus D would not meet requirement

upvoted 2 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: B

check masetromain's comment

upvoted 1 times

 **dkx** 8 months, 4 weeks ago

- A. No, because mandatory controls are owned by AWS Control Tower, and they apply to every OU on your landing zone. These controls are applied by default when you set up your landing zone, and they can't be deactivated. Moreover, none of them address RDS encrypted at rest.
- B. Yes, because Strongly recommended controls are owned by AWS Control Tower. They are based on best practices for well-architected multi-account environments. These controls are not enabled by default, and they can be deactivated through the AWS Control Tower console or the control APIs. Moreover, three of them are RDS detective controls
- C. No, because AWS Config does not create mandatory guardrails; AWS Config has managed and custom rules
- D. No, because SCPs are created in AWS Orgs and are not designed to detect Amazon RDS DB instances that are not encrypted at rest.

upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

It's. B

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

A seems but previous exist rule
then B is more appropriate in this case

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#disallow-rds-storage-unencrypted>

upvoted 1 times

 **EricZhang** 10 months, 2 weeks ago

C - using AWS Config for detective action

upvoted 2 times

 **OCHT** 1 year ago

Selected Answer: C

Option B suggests enabling an appropriate guardrail from the list of strongly recommended guardrails in AWS Control Tower and applying it to the production OU. While AWS Control Tower provides a set of pre-packaged guardrails that enforce best practices for security, operations, and compliance, there is no guarantee that there is a pre-packaged guardrail specifically for detecting Amazon RDS DB instances that are not encrypted at rest.

In contrast, option C creates a custom rule in AWS Config that specifically checks for Amazon RDS DB instances that are not encrypted at rest. This provides more flexibility and control in ensuring that the company's specific requirement is met.

upvoted 2 times

 **passthatexam1** 12 months ago

It's incorrect ideally you only apply to the OU and not to an individual account, therefore this needs to be discounted.

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

Enable the appropriate guardrail

upvoted 2 times

 **Ajani** 1 year, 1 month ago

Selected Answer: B

Mandatory controls are owned by AWS Control Tower, and they apply to every OU on your landing zone. These controls are applied by default when you set up your landing zone, and they can't be deactivated.

The solution requirement falls under a proactive(Recommended Control).

<https://docs.aws.amazon.com/controltower/latest/userguide/rds-rules.html#ct-rds-pr-16-description>

Optional controls are OU specific.

upvoted 4 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

Tip - As this detective guardrail is available, answer is B. But if the guardrail is not available in that predefined list, the answer would be --C

<https://aws.amazon.com/blogs/mt/aws-control-tower-detective-guardrails-as-an-aws-config-conformance-pack/>

upvoted 3 times

 **klog** 1 year, 1 month ago

Selected Answer: B

question is asking for detection, not mandate

upvoted 2 times

Question #65

Topic 1

A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting.

The company's existing architecture includes the following:

- A VPC with private and public subnets, and a NAT gateway.
- Site-to-Site VPN for connectivity with the on-premises environment.
- EC2 security groups with direct SSH access from the on-premises environment.

The company needs to increase security controls around SSH access and provide auditing of commands run by the engineers.

Which strategy should a solutions architect use?

- A. Install and configure EC2 Instance Connect on the fleet of EC2 instances. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- B. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's devices. Enable AWS Config for EC2 security group resource changes. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- D. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attached. Attach the IAM role to all the EC2 instances. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

Correct Answer: D

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: D

The correct answer is D. This strategy uses IAM roles and AWS Systems Manager to provide secure and auditable SSH access to the instances. The IAM role is attached to all the EC2 instances and has the AmazonSSMManagedInstanceCore managed policy attached, which allows the instances to be managed by Systems Manager. The engineers then install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager. This approach provides secure and auditable access to the instances without the need for IP-based security group rules or additional infrastructure.

upvoted 18 times

masetromain 1 year, 2 months ago

Option A uses EC2 Instance Connect to provide secure and auditable SSH access to the instances, but it requires additional infrastructure and configuration.

Option B provides auditing of commands run by the engineers, but it relies on IP-based security group rules, which can be difficult to manage and may not be as secure as using IAM roles.

Option C uses AWS Config and Firewall Manager to automatically remediate changes to security group rules, but it still relies on IP-based security group rules and does not provide an auditable method of access to the instances.

upvoted 3 times

masetromain 1 year, 2 months ago

For option A to work, the following additional infrastructure and configuration would be required:

The EC2 Instance Connect service needs to be enabled in the AWS account and the appropriate IAM permissions would need to be granted to the engineers.

The EC2 instances would need to have the EC2 Instance Connect agent installed and configured.

The engineers would need to install the EC2 Instance Connect CLI on their devices and have the necessary credentials to authenticate with AWS.

In addition, the company would need to update their processes and procedures to ensure that engineers are only using EC2 Instance Connect to access the instances and that all access is being logged and audited.

upvoted 4 times

 **adrian202** 3 months, 2 weeks ago

The key factor is that Option A explains to remove the port 22 inbound SSH access security group, they would need to keep that present: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html>

upvoted 2 times

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: D

A is wrong because Instance connect does not provide auditing

B is wrong because it mentions OS audit logs. we need to audit SSH traffic

C is wrong because we want to audit not remediate as asked in question. config service is to record using predefined rules and remediate as well

D is correct because,

By attaching the AmazonSSMManagedInstanceCore policy to an IAM role, EC2 instances can be controlled and monitored through the Systems Manager service, enabling capabilities such as remote instance management, patching, and compliance reporting. (ChatGPT response its answers are brief and helpful sometimes)

upvoted 10 times

 **gofavad926**  3 weeks, 2 days ago

Selected Answer: D

D, use SSM

upvoted 1 times

 **8608f25** 1 month, 4 weeks ago

Selected Answer: D

Option D is the best strategy because it leverages AWS Systems Manager Session Manager, which allows for secure instance management without the need for SSH access. By attaching an IAM role with the AmazonSSMManagedInstanceCore policy to EC2 instances, engineers can use Session Manager for shell access to instances without needing to open port 22, significantly enhancing security. Session Manager also automatically logs session activity to S3 or CloudWatch Logs, providing the required command auditing capability. This eliminates the need for direct SSH access and offers a centralized, secure, and audited method for engineers to access and run commands on instances.

upvoted 1 times

 **rioisverycute** 3 months, 2 weeks ago

Selected Answer: B

It required to increase security around ssh access, why so many people voted on D?

upvoted 1 times

 **djeong95** 1 month, 1 week ago

Cloudwatch agent does not provide auditable logs for SSH sessions; it only provides metrics about CPU/Memory/Network Packets/etc; nothing about what user started session at what time and ran certain trackable API calls while in that session.

upvoted 1 times

 **Chung234** 5 months, 3 weeks ago

The answer is D. Option A is wrong because EC2 Instance Connect requires the host security group to permit SSH traffic inbound.

<https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec2-instance-connect-and-session-manager-ssh-connections>

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

It's D

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: D

keyword = AWS Systems Manager Session Manager

then D

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: D

D for sure.

upvoted 2 times

 **Ajani** 1 year, 1 month ago

Why its NOT A

To connect using the Amazon EC2 console, the instance must have a public IPv4 address.

If the instance does not have a public IP address, you can connect to the instance over a private network using an SSH client or the EC2 Instance Connect CLI. For example, you can connect from within the same VPC or through a VPN connection, transit gateway, or AWS Direct Connect.

EC2 Instance Connect does not support connecting using an IPv6 address.

going with D:

upvoted 2 times

 **lygf** 1 year, 1 month ago

Selected Answer: D

Need to be able to audit the commands ran on the machine.

upvoted 2 times

 **DWsk** 1 year, 1 month ago

I don't understand why it can't be A for this one. Why is AWS Systems Manager Session better than EC2 Instance Connect? They both require installing something on the instances.

upvoted 1 times

 **lygf** 1 year, 1 month ago

Could option A audit the commands ran on the server, as required by the question? I knew D certainly can.

upvoted 1 times

 **anita_student** 1 year, 1 month ago

For EC2 instance connect there are a few requirements:

- instance has public IP (the instances in question are private)
- you have port 22 open (A says remove port 22 inbound)

upvoted 4 times

 **moota** 1 year, 1 month ago

Selected Answer: D

According to ChatGPT,

Yes, AWS Systems Manager Session Manager can track the commands that are executed during a session. The session is recorded in the form of a log, which can be accessed and reviewed later. The log contains information such as the start time, end time, and the user who initiated the session, as well as a record of all the commands executed during the session, including their output and exit codes. This information can be useful for auditing purposes, troubleshooting, and compliance reporting.

upvoted 2 times

 **tinyflame** 1 year, 2 months ago

Selected Answer: B

provide auditing of commands run by the engineers = B Only

upvoted 3 times

 **joefromnc** 7 months, 2 weeks ago

Read docs you can audit command using SSM <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html>

upvoted 1 times

 **rif** 6 months ago

"In addition to providing information about current and completed sessions in the Systems Manager console, Session Manager provides you with the ability to audit session activity in your AWS account using AWS CloudTrail"

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-auditing.html>

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-auditing.html>

upvoted 1 times

Question #66

Topic 1

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create an SCP to set a fixed monthly account usage limit. Apply the SCP to the developer accounts.
- B. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- C. Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts.
- D. Create an IAM policy to deny access to costly services and components. Apply the IAM policy to the developer accounts.
- E. Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- F. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services.

Correct Answer: BDF*Community vote distribution*

kiran15789 1 year, 1 month ago

Selected Answer: BCF

I prefer D over C as IAM cant be applied to Account
upvoted 14 times

spd 1 year, 1 month ago

Selected Answer: BCF

Clear - BCF - SCP is preferable over IAM
upvoted 13 times

gofavad926 3 weeks, 2 days ago

Selected Answer: BCF

BCF - SCP, budget and custom lambda to terminate services
upvoted 1 times

wooin992 3 weeks, 3 days ago

Selected Answer: BDF

BDF
cannot apply scp in account, need to apply it in OU
upvoted 1 times

8608f25 1 month, 4 weeks ago

Selected Answer: BCF

B. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process. AWS Budgets allows you to set custom cost and usage budgets that alert you when you exceed your thresholds.
C. Create an SCP to deny access to costly services and components. Apply the SCP to the developer accounts. By creating an SCP that specifically denies access to costly AWS services, the company can prevent developers from launching such services, thereby helping to keep costs within the fixed monthly budget.
F. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached. Invoke an AWS Lambda function to terminate all services. While AWS Budgets cannot directly terminate services when a budget is exceeded, you can configure an alert to trigger a notification. This notification can then invoke a Lambda function designed to assess and terminate services as necessary, based on the company's policies.

upvoted 1 times

duriselvan 2 months, 2 weeks ago

Setting a monthly cost budget with a variable target amount, with each subsequent month growing the budget target by 5 percent. Then, you can configure your notifications for 80 percent of your budgeted amount and apply an action. For example, you could automatically apply a custom IAM policy that denies you the ability to provision additional resources within an account.

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>
ans :bdf

upvoted 1 times

✉  ninomfr64 3 months ago

Selected Answer: BCF

- A = SCP is used to limit permission that administrator can grant IAM users/roles, SCP cannot set a fixed monthly account usage limit
B = correct
C = correct
D = it could work, but it would require more work wrt SCP
E = Budget actions cannot terminate all kind of services, actually supports 3 types of actions 1/ apply IAM policy to IAM identities, 2/ apply SCP to an OU and 3/ terminate EC2 and RDS instances
F = correct

upvoted 1 times

✉  jpa8300 3 months, 1 week ago

Selected Answer: BDF

Although, C is correct, some people here say that SCP cannot be attached to an account, but it is not true, you can, the most common option when we want to deny permissions to an account is to use an IAM policy.

upvoted 1 times

✉  rlf 6 months ago

BCF.
In Option D, we can not apply IAM policy to an AWS Account.

upvoted 1 times

✉  SK_Tyagi 7 months, 3 weeks ago

Selected Answer: BDF

I'd go with BDF, since there's no mention of OU. As a rule of thumb, IAM policies to restrict are applied on Accounts, Users, Groups and SCP's on OU's.

upvoted 4 times

✉  vn_thanhitung 7 months, 3 weeks ago

IAM policies for user ? <https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies-overview.html>

upvoted 1 times

✉  vn_thanhitung 7 months, 3 weeks ago

Sorry I mistake, IAM policies can be applied on User.

upvoted 1 times

✉  CuteRunRun 8 months ago

Selected Answer: BCF

BCF is right.
I think SCP is more convenient than IAM.
You need to config the IAM to all accounts manually

upvoted 1 times

✉  [Removed] 8 months, 3 weeks ago

Selected Answer: BCF

prefer SCP over IAM in org accounts

upvoted 1 times

✉  NikkyDicky 9 months, 1 week ago

Selected Answer: BCF

It's a BCF

upvoted 1 times

✉  PhuocT 9 months, 3 weeks ago

Selected Answer: BCF

C - SCP would be preferred to control the services used in Organization's AWS accounts.

upvoted 1 times

✉  SkyZeroZx 9 months, 3 weeks ago

Selected Answer: BCF

Clear - BCF - SCP is preferable over IAM

upvoted 1 times

✉  Roontha 10 months, 1 week ago

Answer : B,C,F

Use case reference from AWS with architecture diagram.

<https://aws.amazon.com/blogs/mt/control-developer-account-costs-with-aws-cloudformation-and-aws-budgets/>

upvoted 6 times

✉  rbm2023 11 months, 1 week ago

Selected Answer: BCF

I agree with B C and F. C instead of D because with option D states that the IAM policy should be applied to the developer accounts, this seems like we would require to apply this for each user individually, since the company already makes use of Organizations why not create a SCP as guardrail for avoiding the use of all costly services. Something like the SCP below:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "DenyCostlyServices",  
      "Effect": "Deny",  
      "Action": [  
        "aws-portal:*",  
        "cloudfront.*",  
        "directconnect.*",  
        "globalaccelerator.*",  
        "shield.*",  
        "waf.*",  
        "waf-regional.*"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

upvoted 3 times

Question #67

Topic 1

A company has applications in an AWS account that is named Source. The account is in an organization in AWS Organizations. One of the applications uses AWS Lambda functions and stores inventory data in an Amazon Aurora database. The application deploys the Lambda functions by using a deployment package. The company has configured automated backups for Aurora.

The company wants to migrate the Lambda functions and the Aurora database to a new AWS account that is named Target. The application processes critical data, so the company must minimize downtime.

Which solution will meet these requirements?

- A. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the automated Aurora DB cluster snapshot with the Target account.
- B. Download the Lambda function deployment package from the Source account. Use the deployment package and create new Lambda functions in the Target account. Share the Aurora DB cluster with the Target account by using AWS Resource Access Manager (AWS RAM). Grant the Target account permission to clone the Aurora DB cluster.
- C. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions and the Aurora DB cluster with the Target account. Grant the Target account permission to clone the Aurora DB cluster.
- D. Use AWS Resource Access Manager (AWS RAM) to share the Lambda functions with the Target account. Share the automated Aurora DB cluster snapshot with the Target account.

Correct Answer: C

Community vote distribution



✉️ **masetromain** 1 year, 2 months ago

Selected Answer: B

The correct answer is option B. This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime.

In this solution, the Lambda function deployment package is downloaded from the Source account and used to create new Lambda functions in the Target account. The Aurora DB cluster is shared with the Target account using AWS RAM and the Target account is granted permission to clone the Aurora DB cluster, allowing for a new copy of the Aurora database to be created in the Target account. This approach allows for the data to be migrated to the Target account while minimizing downtime, as the Target account can use the cloned Aurora database while the original Aurora database continues to be used in the Source account.

upvoted 17 times

✉️ **masetromain** 1 year, 2 months ago

Option A is not the best solution because it doesn't share the Aurora DB cluster with the Target account and this would cause data inconsistencies as the Source and Target accounts would not share the same data.

Option C is not the best solution because, it does not specify how the data will be migrated and it would cause downtime as the Source and Target accounts are not sharing the same data.

Option D is not the best solution because it does not specify how the Lambda function will be migrated and it would cause data inconsistencies as the Source and Target accounts are not sharing the same data.

upvoted 2 times

✉️ **lxrdm** 9 months, 1 week ago

For option A, its also not possible because automated snapshots cannot be shared..

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-share-snapshot.html>

upvoted 2 times

✉️ **Simon523** 7 months, 3 weeks ago

Selected Answer: B

AWS Resource Access Manager (RAM) can only share the follow services:

- Amazon Aurora – DB clusters
 - Amazon EC2 – capacity reservations and dedicated hosts
 - AWS License Manager – License configurations
 - AWS Outposts – Local gateway route tables, outposts, and sites
 - Amazon Route 53 – Forwarding rules
 - Amazon VPC – Customer-owned IPv4 addresses, prefix lists, subnets, traffic mirror targets, transit gateways, transit gateway multicast domains
- <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 11 times

 **Dgix** Most Recent 1 month, 1 week ago

Selected Answer: B

A is viable, but as AWS RAM can share Aurora clusters, B is faster. However, AWS RAM can't share lambdas, so C and D are out.

upvoted 1 times

 **Dgix** 1 month, 1 week ago

B, C, and D are all out since AWS RAM cannot share either Lambdas or Aurora DB clusters. A is the only viable one - you must use a manual snapshot for the DB, share it, and redeploy any deployment package in the destination account. (The question tries to trip you up by its wording: lambda deployments can't be downloaded, but the same deployment packages used to deploy the lambdas can, for instance from S3 or from source)

upvoted 1 times

 **8608f25** 1 month, 4 weeks ago

Selected Answer: B

Option B is the most accurate and efficient solution based on this AWS article content (https://aws.amazon.com/about-aws/whats-new/2019/07/amazon_aurora_supportscloningacrossawsaccounts-/). It correctly outlines the steps for Lambda migration and utilizes the Aurora DB cluster cloning feature across accounts via AWS RAM, which aligns with the article's description. This approach ensures minimal downtime and efficient migration by allowing direct cloning of the Aurora database.

Option C incorrectly suggests using AWS RAM to share Lambda functions, which is not supported yet based on latest sharable AWS resources: <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 1 times

 **master9** 2 months, 2 weeks ago

Selected Answer: C

AWS Resource Access Manager (RAM) to share AWS Lambda functions and Aurora DB clusters with another AWS account. AWS RAM allows you to share resources that are created and managed by other AWS services with individual AWS accounts or with the accounts in an organization or organizational units (OUs) in AWS Organizations.

To share a Lambda function with another AWS account, you can delegate access to an IAM user (or all users) in the other AWS account so that they can assume a role in your account and invoke the Lambda function in your account.

To share an Aurora DB cluster with another AWS account, you can create a resource share in AWS RAM and specify the Amazon Resource Name (ARN) of the Aurora DB cluster as the resource to share. You can then specify the AWS account IDs of the accounts with which you want to share the resource.

upvoted 1 times

 **ninomfr64** 3 months ago

Selected Answer: B

A = you can share snapshot to restore DB, but this will introduce some downtime

B = correct (cloning a DB allows for very limited downtime)

C = if you only share Lambda you are not migrating it, also it appears the Lambda is not a RAM sharable resource

<https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html>

D = it appears the Lambda is not a RAM sharable resource and you cannot directly share an automated snapshot, you need first to create a manual snapshot by copying the automated snapshot, and then share that copy

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-share-snapshot.html>

upvoted 1 times

 **ninomfr64** 3 months ago

A is not correct as you cannot directly share an automated snapshot, you need first to create a manual snapshot by copying the automated snapshot, and then share that copy <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-share-snapshot.html>

upvoted 1 times

 **learnwithaniket** 3 months, 1 week ago

Selected Answer: B

There is limit on the number of resources you can share with AWS RAM.

AWS RAM does not support direct sharing of Lambda functions between accounts.

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

it's B.

In A - automated snapshots are not shareable

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: B

Option B minimizes downtime, compared to A, where we only share a snapshot of the cluster. For C we do not migrate the lambdas, we just share them, which is not the idea of the exercise.

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

The correct answer is option B. This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime.

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

in case the letter A use only snapshot not sync the complete data and is possible lost data in the process

upvoted 2 times

 **Perkuns** 9 months, 4 weeks ago

Selected Answer: C

They just want to migrate the Lambda and Aurora DB, they dont care about the app itself

upvoted 1 times

 **rbm2023** 11 months, 1 week ago

Selected Answer: B

The question is about migration and not sharing, so the answer is how to use a RAM feature to help you on the migration. In option D they are not migrating anything, both Lambda and Aurora are being shared with the Target account and not migrated. In option C is a similar situation, the Lambda is not being migrated. Option A seems a good option but might cause a larger downtime. Hence option D is more appropriate because you can use the cluster share with the Target account and clone the database cluster into it. In my view this answer should contemplate in which moment the cutoff from Source to Target would occur.

upvoted 3 times

 **takecoffee** 1 year ago

Selected Answer: B

You can share the following Amazon Aurora resources by using AWS RAM.

upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: B

B is the way forward

upvoted 2 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

AWS RAM can share ec2 instances, lambdas, DB clusters, RDS, event Redshift clusters.

Refer AWS SA video here - <https://www.youtube.com/watch?v=KL9SICG52zY>

If company would not have had critical data, answer C is good. as existing app should not be down, we have to download lambda and then share. so answer is B. other wise you can stop app and share with RAM (Resource shares)

upvoted 4 times

 **Cassa** 12 months ago

However, if on migration the AWS RMS already will stop the Aurora I don't see a problem use this window to migrate Lambda also?

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: B

B is correct. Move Lambda and Aurora both to target account

upvoted 4 times

Question #68

Topic 1

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure Amazon S3 to send event notifications to the SQS queue. Create an EC2 Auto Scaling group with a minimum size of one instance. Update the data processing script to poll the SQS queue. Process the S3 objects that the SQS message identifies.
- C. Migrate the data processing script to a container image. Run the data processing container on an EC2 instance. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- D. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file. Use an S3 event notification to invoke the Lambda function.

Correct Answer: D

Community vote distribution

A (71%)

D (29%)

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: A

The correct answer is A, migrating the data processing script to an AWS Lambda function and using an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects. This solution meets the company's requirements of high availability and scalability, as well as reducing long-term management overhead, and is likely to be the most cost-effective option.

Option B involves creating an SQS queue and configuring S3 to send event notifications to it. The data processing script would then poll the SQS queue and process the S3 objects that the SQS message identifies. While this option also provides high availability and scalability, it is less cost-effective than using Lambda, as it requires additional resources such as an SQS queue and an EC2 Auto Scaling group.

upvoted 20 times

✉️  **hamimelon** 7 months, 1 week ago

Agree. Also, it says the company does not wanna manage long-term overhead, which points to serverless.

upvoted 2 times

✉️  **dpatra** 6 months ago

SQS is out of the question because the script already has a built in logic that will prevent it to reprocess a message that's already been processed

upvoted 1 times

✉️  **masetromain** 1 year, 2 months ago

Option C, migrating the data processing script to a container image and running it on an EC2 instance, would still require the company to manage the underlying EC2 instances and may not be as cost-effective as using Lambda.

Option D, migrating the data processing script to a container image that runs on Amazon ECS on AWS Fargate, would still require the company to manage the underlying infrastructure and may not be as cost-effective as using Lambda. Additionally, it introduces additional complexity by adding a Lambda function that calls the Fargate RunTask API operation.

upvoted 4 times

✉️  **red_panda** 1 week, 6 days ago

ECS in Fargate mode you don't need to manage anything underling infra!

You're totally forgot about cost, for sure running an ECS Fargate has lower cost than running a Lambda for 5 minutes every 10 minutes! Also the function to trigger the ECS workload (in option D), running for milliseconds (as need only to notify the doc upload in S3), so it's more correct the D answer.

Ask to any Gen AI model, you will have mine answer with more details :)

upvoted 1 times

 **zhangyu20000** Highly Voted  1 year, 2 months ago

A is correct, it provide HA, scale, less management. Task only need 5 minutes

B: enen more complex

C: container still run on one EC2, not scale

d: need container, Farget and Lambda. Complex than A

upvoted 7 times

 **red_panda** Most Recent  1 week, 6 days ago

Selected Answer: D

Ok i was thinking between A and D.

I'm pretty sure which is D our answer, see the details.

The requirements are:

- COST as much as possible low

- OPERATIONS as much as possible managed.

So at the first reading, the A option seems to be the correct option (because it's totally AWS managed), but here we're totally forgot the cost. Running a Lambda function, for 5 minutes every 10 minutes, it's very very more expensive than a simple ECS task running continuously.

Finally, ECS in fargate mode is totally AWS managed, so we will have lower cost, and a serverless and HA environment, which auto-scale if we need more processing at time.

For me, option D is the correct answer.

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: A

A, use lambda function is much cost-effective than use ECS Margate

upvoted 1 times

 **8608f25** 1 month, 4 weeks ago

Selected Answer: A

Option A is the most cost-effective and efficient solution. AWS Lambda allows for running code in response to triggers such as S3 event notifications without the need to manage servers, thereby directly addressing the requirement to reduce long-term management overhead. Since the script is only needed when new files are uploaded and takes about 5 minutes to process each file, Lambda's ability to scale automatically and its billing model based on actual compute time used make it an ideal solution. Lambda can process files immediately upon upload, maximizing efficiency and minimizing idle time.

Option D proposes using Amazon ECS on AWS Fargate with Lambda to trigger tasks. This solution introduces container orchestration, which can improve scalability and reduce some management overhead. However, it is not as cost-effective as directly invoking a Lambda function to process files, considering the lightweight nature of the task and the added complexity of managing container orchestration and Lambda functions together.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

Selected Answer: D

100% the answer is D.

5 minutes to process EACH FILE? And the EC2 instance is processing files 60% of the time?

Lambda would be crazy expensive in this scenario. ECS/Fargate = cheaper for sure. See link in @covabix879 comment for proof of this.

Greyeye said something rather ridiculous: "If you get 1000 images, you will see 1000 tasks. That is not economical or cheap."

How can 1x EC2 instance running a script every 10 minutes process 1000 images with each one taking 5 minutes? Even if the script processed images in parallel, e.g. one image per vCPU at a time, that instance would need 500 vCPUs! For the EC2 instance to be idle 40% of the time, it would need 833 vCPUs. That's ridiculous.

But even if 1000 images suddenly appeared, the Lambda solution would still result in 1000 Lambdas all firing and running for 5 minutes each. Which is going to be more expensive than ECS/Fargate.

upvoted 2 times

 **ninomfr64** 2 months, 4 weeks ago

Selected Answer: A

A = correct

B = does not reduce long-term management overhead

C = does not reduce long-term management overhead

D = does not reduce long-term management overhead

Note: D is a cheap options as mentioned by other here below could be cheaper than A. However, in addition to maintaining the script code it requires to maintain the container image and the lambda

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: A

in the real world it might be D, but with provided details and keeping in mind lambda retries in case of A, I would vote for A.

upvoted 1 times

 **Sandeep_B** 5 months, 2 weeks ago

Selected Answer: A

D is more complex and overload for administration. Hence Vote for A
upvoted 1 times

 **covabix879** 6 months, 1 week ago

Selected Answer: D

<https://blogs.perficient.com/2021/06/17/aws-cost-analysis-comparing-lambda-ec2-fargate/> Even Fargate running continuously is cheaper than Lambda running half of the time. So long running work load not cost effective with Lambda (Every 10 minutes run for 5 minutes. So half of the time lambda is running) Therefore Fargate is the most cost-effective solution.

upvoted 4 times

 **kjcncjek** 7 months ago

running lambda for 5 minutes is not cost effective, so answer is D
upvoted 2 times

 **Greyeve** 7 months, 3 weeks ago

Selected Answer: A

I vote A

D will invoke a new Fargate task per every PUT command.
If you get 1000 images, you will see 1000 tasks. That is not economical or cheap.

if D was invoking a new task by other means like EventBridge, this would have been a lot cheaper.

upvoted 1 times

 **CuteRunRun** 8 months ago

Selected Answer: A

I prefer A

upvoted 1 times

 **chico2023** 8 months, 1 week ago

Selected Answer: A

I would go with A as well. According to Olabiba:
"Yes, option A would generally be more cost-effective than option D."

In option A, you would migrate the data processing script to an AWS Lambda function, which has a pay-per-use pricing model. You would only pay for the actual number of requests and the duration of the function execution. This can be more cost-effective for short-duration tasks like processing files.

On the other hand, in option D, you would migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Fargate has a different pricing model, where you pay for the vCPU and memory resources allocated to your containers. This can be more expensive compared to the pay-per-use model of AWS Lambda."

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

it's A

upvoted 1 times

 **rbm2023** 11 months, 1 week ago

Selected Answer: A

The question is about the most cost effective, the lambda choice (A) is appropriate because the task will run for around 5 minutes and lambdas have a time limit of 15 minutes. If the task took more than 15 minutes then the option D would be appropriate for the scalability, availability and cost effectiveness.

upvoted 2 times

 **sergza** 11 months, 1 week ago

Selected Answer: D

I Actually Like Fargate Answer. AWS Lambda is expensive if you're using it for regularly occurring, long-running processes that do not take advantage of the very short scaling time the service provides. Since it is going to run for 5 min for every 10 min it roughly going to be active 50 % of the time. Anyway it could be cheaper Look into these analysis <https://blogs.perficient.com/2021/06/17/aws-cost-analysis-comparing-lambda-ec2-fargate/> <https://sixfeetup.com/blog/cost-to-run-aws-lambda-function-all-the-time>

upvoted 4 times

Question #69

Topic 1

A financial services company in North America plans to release a new online web application to its customers on AWS. The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover.

Which solution will meet these requirements?

- A. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB.
- B. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB enable health checks to ensure high availability between Regions.
- C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC. Place the Auto Scaling group behind the ALB. Set up the same configuration in the us-west-1 VPC. Create an Amazon Route 53 hosted zone. Create separate records for each ALB. Enable health checks and configure a failover routing policy for each record.
- D. Create a VPC in us-east-1 and a VPC in us-west-1. Configure VPC peering. In the us-east-1 VPC, create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs. Place the Auto Scaling group behind the ALB. Create an Amazon Route 53 hosted zone. Create a record for the ALB.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: C

The correct answer is C. Choice C meets the requirements for the application to be highly available and to dynamically scale to meet user traffic, as well as implementing a disaster recovery environment in the us-west-1 Region through active-passive failover.

In choice C, the company creates a VPC in us-east-1 and a VPC in us-west-1, and sets up an Application Load Balancer (ALB) and Auto Scaling group in both VPCs. The ALB extends across multiple Availability Zones in each VPC, and the Auto Scaling group deploys the EC2 instances across these Availability Zones. The Auto Scaling group is placed behind the ALB, which allows for automatic scaling of the instances to meet user traffic.

An Amazon Route 53 hosted zone is also created, with separate records for each ALB. Health checks are enabled for each record, and a failover routing policy is configured. This allows for active-passive failover between the two regions, ensuring high availability for the application.

upvoted 16 times

 **masetromain** 1 year, 2 months ago

Choice A, B, and D do not fully meet the requirements of the disaster recovery environment in the us-west-1 Region and the failover routing policy because they do not include the necessary configurations for active-passive failover.

In choice A, the VPCs in us-east-1 and us-west-1 are peered and the Auto Scaling group and Application Load Balancer (ALB) are extended across multiple availability zones in both regions. However, there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

Choice B, the VPCs in us-east-1 and us-west-1 are separate, and the configuration is replicated in both regions but there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

upvoted 3 times

 **masetromain** 1 year, 2 months ago

Choice D is similar to choice A, the VPCs in us-east-1 and us-west-1 are peered and the Auto Scaling group and Application Load Balancer (ALB) are extended across multiple availability zones in both regions. However, there is no explicit failover routing policy configured, so it is not clear how the application would failover to the us-west-1 region in the event of an outage.

Choice C is the correct answer as it includes all the necessary components for a disaster recovery environment in the us-west-1 region. It creates separate VPCs, Application Load Balancer, and Auto Scaling Group in both regions, and it enables health checks and configures a failover routing policy for each record. This ensures that in the event of an outage, the application can automatically failover to the us-west-1 region with minimal downtime.

upvoted 4 times

✉  **NikkyDicky** Most Recent 9 months, 1 week ago

Selected Answer: C

It's C

upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: C

C for DR

upvoted 2 times

✉  **God_Is_Love** 1 year, 1 month ago

Selected Answer: C

Active-Passive failover with primary and secondary records in Route53

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

https://d1tcczg8b21j1t.cloudfront.net/strapi-assets/32_Route_53_health_checks_4_64165fc533.png

upvoted 3 times

✉  **God_Is_Love** 1 year, 1 month ago

VPC Peering is good for fully accessing all resources in a shared env but that's not asked here, so A and D gets eliminated. B does not mention the weighted routing config enable ment although setup is good. So answer is C

upvoted 2 times

✉  **zozza2023** 1 year, 2 months ago

Selected Answer: C

active-passive failover==>a failover routing policy within route 53

upvoted 4 times

✉  **zhangyu20000** 1 year, 2 months ago

C is correct

upvoted 3 times

Question #70

Topic 1

A company has an environment that has a single AWS account. A solutions architect is reviewing the environment to recommend what the company could improve specifically in terms of access to the AWS Management Console. The company's IT support workers currently access the console for administrative tasks, authenticating with named IAM users that have been mapped to their job role.

The IT support workers no longer want to maintain both their Active Directory and IAM user accounts. They want to be able to access the console by using their existing Active Directory credentials. The solutions architect is using AWS IAM Identity Center (AWS Single Sign-On) to implement this functionality.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and set the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- B. Create an organization in AWS Organizations. Turn on the IAM Identity Center feature in Organizations. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.
- C. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure IAM Identity Center and select the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- D. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure IAM Identity Center and set the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.

Correct Answer: D

Community vote distribution

D (82%)

Other

 **masetromain**  1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/69172-exam-aws-certified-solutions-architect-professional-topic-1/>

You are correct, I apologize for the oversight. To meet the requirements of the IT support workers, option D would be the correct solution:

This option will first enable all features in AWS Organizations, then create and configure an AD Connector to connect to the company's on-premises Active Directory. Then, it will configure IAM Identity Center (AWS SSO) and set the AD Connector as the identity source, allowing the IT support workers to access the console using their existing Active Directory credentials. Finally, it will create permission sets and map them to the existing groups within the company's Active Directory. This solution will also be cost-effective as it does not involve creating a new directory in AWS Directory Service.

upvoted 21 times

 **dev112233xx**  1 year ago

Selected Answer: D

D is the correct answer.. B is wrong answer

From aws documentation:

Q: Which AWS accounts can I connect to IAM Identity Center?

You can add any AWS account managed using AWS Organizations to IAM Identity Center. You need to enable all features in your organizations to manage your accounts single sign-on.

upvoted 14 times

 **carpa_jo** 3 months, 2 weeks ago

Source: <https://aws.amazon.com/iam/identity-center/faqs/#product-faqs#iam-identity-center-faqs#identity-sources-and-applications-support>
upvoted 1 times

 **gofavad926**  3 weeks, 2 days ago

Selected Answer: B

B, Turn on the IAM Identity Center feature in Organizations... similar to D, but without enabling directly the SSO, you can't configure it...

upvoted 1 times

✉ **8608f25** 1 month, 4 weeks ago

Selected Answer: D

Option D is the best because AWS FAQs asked the following question and answered: "Which AWS accounts can I connect to IAM Identity Center?

You can add any AWS account managed using AWS Organizations to IAM Identity Center. You need to enable all features in your organizations to manage your accounts single sign-on." Link: <https://aws.amazon.com/iam/identity-center/faqs/#product-faqs#iam-identity-center-faqs#identity-sources-and-applications-support>

With the clarification that enabling all features in AWS Organizations is necessary for integrating with IAM Identity Center, Option D becomes the most accurate and compliant solution. It correctly combines the need to enable all features in AWS Organizations with the use of an AD Connector for a direct connection to the company's on-premises Active Directory, which remains the most cost-effective way to leverage existing Active Directory credentials for AWS console access.

upvoted 1 times

✉ **LazyAutonomy** 2 months, 1 week ago

Selected Answer: D

Most cost effective is D.

But C is also technically a valid solution that meets all the other requirements. A two way trust means AD users in the on-premise AD can be added to AD groups in the AWS-managed AD.

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: D

A = you do not turn on AWS IdC feature only in AWS Orgs. It is either Consolidation billing or All features

B = same as above

C = requirements is to login users based on-premise AD, for this there is no need to AWS Managed AD with a local domain/directory and 2-way trust. AD Connector is enough and cheaper

D = correct

upvoted 1 times

✉ **marszalekm** 3 months ago

I love such questions, while both B and D seems reasonable, I thinking more about B because of this
<https://docs.aws.amazon.com/singlesignon/latest/userguide/get-set-up-for-idc.html>

upvoted 1 times

✉ **Russs99** 3 months, 3 weeks ago

Selected Answer: B

you can absolutely use an AD Connector as the identity source for AWS IAM Identity Center without turning on all features in your AWS organization. In fact, it's the most cost-effective and recommended approach if you only need single sign-on functionality with your existing on-premises Active Directory

upvoted 2 times

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

Selected Answer: D

<https://docs.aws.amazon.com/singlesignon/latest/userguide/prereq-orgs.html>

``If you've already set up AWS Organizations and are going to add IAM Identity Center to your organization, make sure that all AWS Organizations features are enabled. When you create an organization, enabling all features is the default.''

upvoted 2 times

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

Selected Answer: D

see dev112233xx's answer

upvoted 1 times

✉ **Tofu13** 6 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-prereqs-considerations.html#:~:text=if%20you've%20already%20set%20up%20aws%20organizations%2C%20make%20sure%20that%20all%20features%20are%20enabled.>

upvoted 2 times

✉ **[Removed]** 8 months, 3 weeks ago

Selected Answer: B

i think it's b because having all the features enabled is not a requirement, otherwise it could incur in more charges. the features are not enabled by default , you have to go one by one or select all to enable them

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Actually not. AWS Org has 2 feature modes: All features enabled (default) and Consolidated billing. AWS Orgs is free of charge regardless feature mode select see Billing section in the <https://aws.amazon.com/organizations/faqs/>

upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

It's D.
B would work if was supported
upvoted 1 times

✉  **karma4moksha** 11 months ago

Selected Answer: D

After reading all comments i concur with D. Reason being , requirement is no duplication fs users so it all stay at one place, thats what they want. So rule out all the 2-way trust options. Why not B? because there is no way in AWS organisations, you can only enable IAM identity center. The available feature sets are only two : All features, or only consolidated billing. Check here
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#feature-set-cb-only

upvoted 3 times

✉  **rbm2023** 11 months, 1 week ago

Selected Answer: D

The options where they turn on only the AWS SSO feature in Organizations must be excluded (A and B). Because it is a requirement to have all features enabled in the organizations.
Reference from https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html
Prerequisites for using AWS IAM Identity Center or former AWS SSO:
"Your AWS account must be managed by AWS Organizations. If you have not set up an organization, you don't have to. When you enable IAM IC, you will choose whether to have AWS create an organization for you.
If you already set up AWS Organizations, make sure that all features are enabled."
Between C and D, you do not need to create and configure a new AWS Managed Microsoft AD since you already have an AD present in the on premises, so there is no reason to expend more on this solution. Hence the response is D.

upvoted 4 times

✉  **Cccb35** 11 months, 1 week ago

Selected Answer: B

I think, the correct is "B". Because, when you create an organization, enabling all features is the default, according this link:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html

"When you create an organization, enabling all features is the default. With all features enabled, you can use the advanced account management features available in AWS Organizations such as integration with supported AWS services and organization management policies."

This would rule out the option "D"

upvoted 3 times

✉  **Amac1979** 1 year ago

Selected Answer: D

D as Vherman said below

upvoted 2 times

Question #71

Topic 1

A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 10 GB.

Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads.

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

- A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
- B. Configure an S3 bucket in each Region to receive the uploads. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
- C. Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
- D. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
- E. Modify the app to add random prefixes to the files before uploading.

Correct Answer: AD

Community vote distribution

AD (97%)

zozza2023 Highly Voted 1 year, 2 months ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB
upvoted 10 times

OCHT Highly Voted 1 year ago

Selected Answer: AD

Explanation for this .

B: Configuring an S3 bucket in each Region to receive the uploads and using S3 Cross-Region Replication to copy the files to the distribution S3 bucket may improve data durability and availability, but it does not address the issue of slow uploads from Australia.

C: Amazon Route 53 with latency-based routing can route the uploads to the nearest S3 bucket Region based on network latency, but it cannot guarantee faster upload speeds or better reliability.

E: Adding random prefixes to the files before uploading will not improve upload performance or reliability.

Thence, I select A and D.

upvoted 6 times

ninomfr64 Most Recent 2 months, 3 weeks ago

Selected Answer: AD

A = correct (improve upload performance)
B = this could work along with C to improve performance, but this will not fix upload failure for files >5GB as you need multi-part upload
C = see answer B
D = correct (required to fix upload failures for >5GB files)
E = this could help with throttling which is not clearly stated as an issue
upvoted 1 times

chico2023 7 months, 2 weeks ago

Selected Answer: DE

Answer: A, D? Maybe. But I prefer D and E. Let me explain why:

Requirement is: "A solutions architect must improve the app's performance for these uploads."

Should we change S3 or the app? (or both?)

Depending on how you interpret this question, you might think on the app, then it should be D and E, seriously. And it DOES make sense. Bear with me here. If you break the files into chunks, you will still have to upload them, let's say 10GB. And here comes the option E, which helps improving uploads with PARALLELISM, and you didn't touch S3 to fix that, just the app :)

B and C would also work and would address the issue with users in Australia but it would change their design. I am not sure this is required, but in the real world, it's good to have options ;)

All in all, I personally would go with D, E, but AD and BC would also work.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: AD

its AD

upvoted 2 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: AD

A and D satisfy the requirement

upvoted 1 times

 **SkyZeroZx** 10 months, 3 weeks ago

Selected Answer: AD

Transfer Accelerator + Multi-part uploads for files more 500MB

Question similar to AWS Certified Solutions Architect Associate

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: AD

AD all day

upvoted 2 times

 **aqiao** 1 year ago

Selected Answer: AD

B is not suitable here, since it wants to improve upload experience, not download

upvoted 2 times

 **Musk** 1 year, 2 months ago

I like AD but I am unsure. If the users in US don't complain about issues, it must be because multi-part upload is already enabled, otherwise it would fail 50% of the times. If only Australia users complain, it must be something else... Maybe A+B is a better option, although B is not the most cost efficient certainly.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

AD is correct

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: AD

<https://www.examtopics.com/discussions/amazon/view/74177-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answers would be A and D.

A. Enabling S3 Transfer Acceleration on the S3 bucket and configuring the app to use the Transfer Acceleration endpoint for uploads will improve the app's performance for users in Australia by providing a fast and secure way to transfer large files over the Internet.

D. Configuring the app to break the video files into chunks and using a multipart upload to transfer files to Amazon S3, will improve the app's performance for users in Australia by allowing them to upload large files in parallel, which can increase upload speed and reduce the risk of upload failures.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

B. Configuring an S3 bucket in each Region to receive the uploads and using S3 Cross-Region Replication to copy the files to the distribution S3 bucket is not the most cost-effective solution for this specific use case.

C. Setting up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region is not a solution that would improve the performance of the uploads specifically for users in Australia.

E. Modifying the app to add random prefixes to the files before uploading will not improve the app's performance for users in Australia.

upvoted 1 times

 **hobokabobo** 1 year, 1 month ago

yes, it will. Other options are more important, but sure random (rsp. any hash that distributes well) prefixes improve performance a lot.

upvoted 2 times

Question #72

Topic 1

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance. Update the connection settings in the application to point to the Aurora reader endpoint.
- B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- C. Create a two-node Amazon Aurora MySQL DB cluster. Migrate the RDS DB instance to the Aurora DB cluster. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.
- D. Create an Amazon S3 bucket. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store. Install the latest Open Database Connectivity (ODBC) driver for the application. Update the connection settings in the application to point to the Athena endpoint

Correct Answer: B

Community vote distribution

B (100%)

✉️  **God_Is_Love**  1 year, 1 month ago

Selected Answer: B

Amazon RDS Proxy is a fully managed database proxy service for Amazon Relational Database Service (RDS) that makes applications more scalable, resilient, and secure. It allows applications to pool and share connections to an RDS database, which can help reduce database connection overhead, improve scalability, and provide automatic failover and high availability.

upvoted 9 times

✉️  **zhangyu20000**  1 year, 2 months ago

B is correct.

C: Aurora is useless, Proxy is pointing to existing RDS

upvoted 6 times

✉️  **pangchn**  6 days, 18 hours ago

Selected Answer: B

C is wrong since RDS proxy for Aurora cluster only support reader endpoint, where in question it doesn't mention the read-only as requirement

upvoted 1 times

✉️  **ninomfr64** 2 months, 3 weeks ago

Selected Answer: B

A = using Aurora MySQL Serverless will not fix the issue, also serverless V1 is not great with HA. If you are running a single instance (no read replicas) it will attempt to create a new DB Instance in the same AZ

B = correct (RDS Proxy in addition to pooling connections, makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections and detects failover and routes requests to standby instance up to 66% faster failover time)

C = Creating and migrating to Aurora cluster is not needed, RDS Proxy is enough

D = this requires a lot of work

upvoted 4 times

✉️  **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

it's a B

upvoted 1 times

✉️  **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword = RDS proxy

upvoted 1 times

✉️  **mfsec** 1 year ago

Selected Answer: B

Create an RDS proxy.

upvoted 1 times

  **klog** 1 year, 1 month ago**Selected Answer: B**

proxy will be a buffer

upvoted 1 times

  **masetromain** 1 year, 2 months ago**Selected Answer: B**

The correct solution is B. Create an RDS proxy. Configure the existing RDS endpoint as a target. Update the connection settings in the application to point to the RDS proxy endpoint.

An RDS proxy is a service that allows you to pool and share connections to an RDS database. By using an RDS proxy, your application can automatically reconnect to the database after a failover event, without the need to restart the application.

Solution A, migrating to Aurora Serverless, may not solve the problem because Aurora Serverless does not support Multi-AZ.

Solution C and D are not the correct solutions because it does not solve the problem of reconnecting to the database after a failover event.

upvoted 4 times

  **God_Is_Love** 1 year, 1 month ago

What?? Aurora does not support Multi AZ ? its a blunder !

upvoted 5 times

  **chikorita** 10 months, 1 week ago

was about to point this

upvoted 1 times

  **BabaP** 10 months, 1 week ago

they are copying the answers from chatgpt

upvoted 5 times

  **k8s_Seoul** 7 months ago

masetromain ~> X

GPTromain ~> O lol

upvoted 1 times

  **SeemaDataReader** 3 months, 1 week ago

Even if the person is copying from chatgpt, they are saving your time and giving some pointers.

upvoted 1 times

Question #73

Topic 1

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate.

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

- A. Set up AWS IoT Core. For each device, create a corresponding Amazon MQ queue and provision a certificate. Connect each device to Amazon MQ.
- B. Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group. Set the Auto Scaling group as the target for the NLConnect each device to the NLB.
- C. Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.
- D. Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB. Configure a mutual TLS certificate authorizer on the HTTP API. Run an MQTT broker on an Amazon EC2 instance that the NLB targets. Connect each device to the NLB.

Correct Answer: D

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: C

The correct solution is C. Set up AWS IoT Core. For each device, create a corresponding AWS IoT thing and provision a certificate. Connect each device to AWS IoT Core.

AWS IoT Core is a fully managed service that enables secure, bi-directional communication between internet-connected devices and the AWS Cloud. It supports the MQTT protocol and includes built-in device authentication and access control. By using AWS IoT Core, the company can easily provision and manage the X.509 certificates for each device, and connect the devices to the service with minimal operational overhead.

upvoted 16 times

masetromain 1 year, 2 months ago

Option A, setting up Amazon MQ queues and connecting each device to a queue, would require significant operational overhead to manage the queues and ensure that each device is properly authenticated and connected.

Option B and D, using a Network Load Balancer (NLB) with a Lambda authorizer or an Amazon API Gateway HTTP API with a mutual TLS certificate authorizer and running an MQTT broker on EC2 instances, would also introduce more operational complexity and overhead compared to using AWS IoT Core.

upvoted 4 times

gofavad926 Most Recent 3 weeks, 2 days ago

Selected Answer: C

C, use IoT Core

upvoted 1 times

8608f25 1 month, 4 weeks ago

Selected Answer: C

Option C is the most suitable solution as AWS IoT Core is specifically designed for IoT scenarios, including device management and secure communication. AWS IoT Core natively supports MQTT, a lightweight communication protocol ideal for IoT devices. It allows devices to connect securely with an individual X.509 certificate for authentication, significantly reducing operational overhead compared to managing a custom MQTT broker or other intermediate services. AWS IoT Core also simplifies device management and scaling, making it the best choice for the described use case.

upvoted 1 times

bjexamprep 2 months, 2 weeks ago

Selected Answer: C

I don't like C, but C might be the preferred answer.

There are thousands of devices. If C is the real answer, there should be a way to automatically create IOT thing and provision certificate. The answer seems implying to create IOT thing and provision certificates manually. If IoT core doesn't have this automation feature, this definitely is not the right answer in real life.

If there is this automation way and the question designer is expecting the exam taker to know this detail, that might be too specific for the exam takers.

D is ugly, and usually is not a correct answer in most question designs. But it provides a feasible way in the real life comparing with C.

upvoted 3 times

waoo 8 months, 1 week ago

答案是C

<https://aws.amazon.com/cn/iot-core/faqs/?nc=sn&loc=5&dn=2>

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

it's C

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: C

I choose C

upvoted 1 times

✉ **zejou1** 1 year ago

Selected Answer: C

<https://docs.aws.amazon.com/iot/latest/developerguide/attach-to-cert.html>

It is C, - you have to do this through IOT core, for the devices you need an AWS IOT "thing" and then provision a certificate for the thing. from there connect the device.

upvoted 2 times

✉ **forceli** 1 year, 1 month ago

Selected Answer: A

-The AWS IoT Device SDKs support device communications using the MQTT

-Device connections to AWS IoT use X.509 client certificates

<https://docs.aws.amazon.com/iot/latest/developerguide/iot-connect-devices.html>

upvoted 1 times

✉ **forceli** 1 year, 1 month ago

Sorry I meant "C"

upvoted 2 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is correct (less op overhead than A)

upvoted 2 times

✉ **zhangyu20000** 1 year, 2 months ago

C is correct

upvoted 3 times

Question #74

Topic 1

A company is running several workloads in a single AWS account. A new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the IAM role that the engineers use for access.

What should the solutions architect do to create the solution?

- A. Upload AWS CloudFormation templates that contain approved resources to an Amazon S3 bucket. Update the IAM policy for the engineers' IAM role to only allow access to Amazon S3 and AWS CloudFormation. Use AWS CloudFormation templates to provision resources.
- B. Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources.
- C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS CloudFormation during stack creation.
- D. Provision resources in AWS CloudFormation stacks. Update the IAM policy for the engineers' IAM role to only allow access to their own AWS CloudFormation stack.

Correct Answer: B

Community vote distribution

C (98%)

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: C

Tricky one. Question has a hint -"to enforce the new restriction on the IAM role" (note its not IAM policy as mentioned in option B) Creating a policy with approved resources first and assuming/applying that role to engineers will enforce. So C is correct. (B lacks enforcement, B is incorrect)

upvoted 15 times

 **rbm2023**  11 months, 1 week ago

Selected Answer: C

C is correct not B , AWS CloudFormation makes calls to create, modify, and delete those resources on their behalf. To separate permissions between a user and the AWS CloudFormation service, use a service role. AWS CloudFormation uses the service role's policy to make calls instead of the user's policy. For more information, see AWS CloudFormation service role . check this out .

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html>

Option B would allow engineers to provision resources using other methods outside of CloudFormation, which would not comply with the new company policy. This would make it difficult to enforce the new restriction on the IAM role that the engineers use for access.

upvoted 8 times

 **gofavad926**  3 weeks, 2 days ago

Selected Answer: C

C, use the IAM service role to execute the stack

upvoted 1 times

 **8608f25** 1 month, 3 weeks ago

Selected Answer: C

Option C is the most effective solution. It involves updating the engineers' IAM role to only allow actions related to AWS CloudFormation, effectively preventing direct provisioning or modification of AWS resources outside of CloudFormation. By creating a service role (with permissions to provision approved resources) that CloudFormation assumes when executing templates, you enforce the provisioning of only approved resources through CloudFormation. This setup provides a clear separation of permissions: engineers can manage CloudFormation stacks but cannot directly create resources unless defined in a CloudFormation template and permitted by the service role.

Option B suggests updating the IAM policy to allow only the provisioning of approved resources and CloudFormation actions. This approach could theoretically work by explicitly listing allowed actions for specific AWS services in the IAM policy. However, it might be challenging to maintain and could inadvertently permit actions outside of CloudFormation, depending on the policy's specificity.

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

Selected Answer: C

A = doesn't prevent to have a CloudFormation template with non-approved resources deployed

B = this doesn't prevent engineers to provision resources from console or cli

C = correct

D = doesn't prevent to provision non-approved resources or to provision only via CloudFormation

upvoted 2 times

 **subupro** 4 months ago

B would be created generally in organization. C is fine , but more restriction , the user can only use the cloud formation stack sets only which is not good for organization level.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: C

with B engineer will be able to directly provision resources without using of CF

upvoted 1 times

 **venvig** 7 months, 2 weeks ago

Selected Answer: C

The two contenders are Option B and C.

Option B would allow the users to provision the approved resources without using CloudFormation (as the Users' IAM role would permission that). So, this violates the requirement.

Option C would ensure that Only Cloudformation can provision the resources. So, that's the correct answer.

upvoted 1 times

 **CuteRunRun** 8 months ago

Selected Answer: C

I prefer C, because you need to give permission to cloud formation

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C no doubt

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: C

C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions.

upvoted 2 times

 **c73bf38** 1 year, 1 month ago

Selected Answer: C

C IAM policy is allowing to provision of approved resources.

upvoted 3 times

 **Musk** 1 year, 2 months ago

Selected Answer: C

B does not enforce CF, otherwise it would work.

upvoted 3 times

 **Untamables** 1 year, 2 months ago

Selected Answer: C

C

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/security-best-practices.html#use-iam-to-control-access>
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html>

upvoted 3 times

 **Nicocacik** 1 year, 2 months ago

Selected Answer: C

You have to use a service role

upvoted 4 times

 **masetromain** 1 year, 2 months ago

C. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS CloudFormation during stack creation.

This option is also correct, it is a way to restrict the access of engineers to only be able to perform AWS CloudFormation actions and provision only approved resources. By giving only permissions to the IAM role used by engineers for CloudFormation and creating a separate IAM role with permissions to provision approved resources and then assigning that role to CloudFormation during stack creation, we ensure that engineers can only provision the approved resources using CloudFormation.

upvoted 2 times

 **masetromain** 1 year, 2 months ago

Both options B and C are correct.

Option B: Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation. Use AWS CloudFormation templates to create stacks with approved resources.

Option C: Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation actions. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role. Assign the IAM service role to AWS

CloudFormation during stack creation.

Both options will enforce the new restriction on the IAM role that the engineers use for access, by limiting their access only to approved resources and only allowing them to provision resources using AWS CloudFormation. The specific option is:

upvoted 1 times

 **Japanese1** 4 months, 2 weeks ago

B works but is inappropriate.

You fail to consider that you NEED to use CFN for resource provisioning.

Option B does not meet the requirement to limit this.

upvoted 1 times

 **zhangyu20000** 1 year, 2 months ago

C is correct

A: only allow CF, no approved resources

B: role allow approved resources and CF. User can bypass CF

D: CF only

upvoted 3 times

 **masetromain** 1 year, 2 months ago

B: Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation is correct but by itself it does not guarantee that the engineers will use only approved resources or will use AWS CloudFormation to provision them. The solutions architect should also implement additional controls such as using AWS Organizations to centrally manage access policies, using AWS Config to monitor and enforce compliance with the company's policies, or creating a custom resource in the CloudFormation templates to validate the provisioned resources against a predefined list of approved resources.

upvoted 1 times

Question #75

Topic 1

A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.

The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.

Which storage strategy is the MOST cost-effective and meets the design requirements?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
- B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that runs a query to delete any records older than 120 days.
- D. Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

Correct Answer: B

Community vote distribution



✉️ **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: B

The most cost-effective and efficient solution that meets the design requirements would be option B, Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.

DynamoDB is a NoSQL key-value store designed for high scale and performance. It is fully managed by AWS and can easily handle millions of small records per minute. Additionally, with the TTL feature, you can set an expiration time for each record, so that the data can be automatically deleted after the specified time period.

upvoted 20 times

✉️ **masetromain** 1 year, 2 months ago

Option A, storing each incoming record as a single .csv file in an Amazon S3 bucket, would not be a good option because it would be difficult to retrieve individual records from the .csv files, and will likely increase the cost of data retrieval.

Option C, storing each incoming record in a single table in an Amazon RDS MySQL database, would be a more expensive option as RDS is typically more expensive than DynamoDB. Additionally, running a cron job to delete old data could lead to additional operational overhead.

Option D, storing incoming records in batches in an S3 bucket, would be a less efficient option as it would require additional processing and parsing of the data to retrieve individual records.

upvoted 3 times

✉️ **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: B

B, dynamodb is the best option

upvoted 1 times

✉️ **8608f25** 1 month, 3 weeks ago

Selected Answer: B

For small records less than 4 KB, DynamoDB can efficiently handle the ingestion of millions of records per minute from devices around the world, meeting the application's design requirements for low-latency data access. Additionally, DynamoDB's Time to Live (TTL) feature allows for automatic deletion of items after a specific period, aligning with the requirement to store data for only 120 days.

upvoted 1 times

✉️ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: B

A = S3 is not great with small files and searching for data based on index (a common pattern is to store object metadata in a database like DDB, OpenSearch or RDS/Aurora). Many small files can lead to high costs for retrieval

B = correct

C = single-table design, high volume write/retrieval of small objects and no need for complex query are better served and cost less with DDB rather than RDS

D = more efficient than A, but still S3 metadata search feature is limited

upvoted 1 times

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

Selected Answer: B

see uC6rW1aB's answer

upvoted 1 times

✉ **vjp_training** 6 months, 3 weeks ago

Selected Answer: B

B is the best for cost-effective.

D is more cost for S3 request

upvoted 1 times

✉ **uC6rW1aB** 7 months, 1 week ago

Selected Answer: B

Ref: <https://aws.amazon.com/dynamodb/pricing/on-demand/>

DynamoDB read requests can be either strongly consistent, eventually consistent, or transactional. A strongly consistent read request of up to 4 KB requires one read request unit. For items larger than 4 KB, additional read request units are required.

upvoted 3 times

✉ **uC6rW1aB** 7 months, 1 week ago

for a US East write object price:

S3 Standard put object per thousand cost \$0.005 -> 1 million put cost \$5 (per minutes in this situation)

Dynamo DB 1 million write cost \$1.25 is a lot of cheaper

upvoted 4 times

✉ **Gmail78** 7 months, 2 weeks ago

Selected Answer: D

Dynamo DB is at least 5X more expensive than S3 for this use case. There are millions of writes and each is 4K, total disk space is 10-15TB.

upvoted 1 times

✉ **vn_thanh tung** 7 months, 1 week ago

D - S3 metadata search feature does not exist

upvoted 1 times

✉ **Soweetadad** 7 months, 2 weeks ago

Selected Answer: D

Although both B and D are correct, Option D is more cost effective.

upvoted 1 times

✉ **dkx** 8 months, 4 weeks ago

A. No, because millions of writes to a single .csv file would cause read and write latency

B. Yes, because DynamoDB can support peaks of more than 20 million requests per second.

C. No, because creating nightly cron is unnecessary, and a relational database isn't designed to ingest millions of small records per minute

D. No, because S3 supports 210,000 PUT requests per minute (3,500 requests per second * 60 seconds per min) which is far less than 1,000,000+ writes per minute

upvoted 4 times

✉ **YodaMaster** 9 months, 1 week ago

Selected Answer: D

Going with D as it's more cost effective. Question didn't ask for more efficient.

upvoted 1 times

✉ **blackgamer** 5 months, 2 weeks ago

B satisfies the requirement but D is not. The keyword here is Low latency - "a durable location where it can be retrieved with low latency"

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

D is more cost effective, even if more complex

upvoted 2 times

✉ **[Removed]** 9 months, 2 weeks ago

Selected Answer: D

While B is viable, it seems like it's a massively expensive option - millions of writes per minute is a lot of WCU. Similarly, C would require a beefy database to support that many writes, may or may not be cheaper than the DDB option. But in a question asking for most cost effective, scalable writes from many sources screams an S3-based solution to me, which leaves A and D. Too many small files (A) and S3's performance will degrade, and millions of objects per minute seems like it would tax S3's ability to index buckets. Nothing in D is impossible to implement; though it's not the simplest solution, it's by far the cheapest.

upvoted 2 times

 geo1551 10 months ago

I think it is A.

I'm not English native speaker, but I read it the way that each incoming record will be stored in separate file, thus the retrieval of a single record would be fast based on its key. S3 is by far the cheapest option of all.

upvoted 1 times

 youngmanaws 11 months, 3 weeks ago

Most cost-effective will be D. and the following makes the size under 5TB , under the limits.

The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.

upvoted 4 times

 youngmanaws 11 months, 2 weeks ago

sorry, metadata is incorrect because the following: "millions of small records per minute from devices all around the world. Each record is less than 4 KB in size "

upvoted 3 times

 Amac1979 1 year ago

Selected Answer: B

B DynamoDB

upvoted 1 times

 mfsec 1 year ago

Selected Answer: B

B. Design the application to store each incoming record in an Amazon DynamoDB table

upvoted 1 times

Question #76

Topic 1

A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDS for MySQL DB instance.

Which solution will provide the HIGHEST availability for the database?

- A. Configure automated backups on Amazon RDS. In the case of disruption, promote an automated backup to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.
- B. Configure global tables and read replicas on Amazon RDS. Activate the cross-Region scope. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- C. Configure global tables and automated backups on Amazon RDS. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source.

Correct Answer: D

Community vote distribution

D (93%) 7%

✉ **zejou1** 1 year ago

Selected Answer: D

This really should be multi-az but you could move to it w/ D.

Here is the key to this one though; Highest Availability - the read replica is an asynchronous copy, while backup is a "time". Easier to do the read replica, and flip the switches than to reload from backup. Global Tables relate to DynamoDB <https://disaster-recovery.workshop.aws/en/services/databases/dynamodb/dynamo-global-table.html>

Little handy "DR" guide

upvoted 14 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: D

A = you cannot promote an automated backup to a standalone DB (you restore a backup into a new DB instance instead). Creating a read replica could help in this scenario in case it is cross-region. This is not specified

B = RDS does not support global table, copying a read replicas from a region to another make no sense to me

C = see B

D = correct

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

D for sure

upvoted 1 times

✉ **rbm2023** 11 months, 1 week ago

Selected Answer: D

There is Aurora Global Database, DynamoDB Global Tables and the question is about RDS for MySQL DB Instance.

<https://jayendrapatil.com/aws-aurora-global-database-vs-dynamodb-global-tables/>

So, options B and C are not acceptable.

Option D refers to using a cross-region replication for disaster recovery which can be found here <https://disaster-recovery.workshop.aws/en/services/databases/rds/rds-cross-region.html>

Following article demonstrates a similar scenario using RDS for SQL Server

<https://aws.amazon.com/blogs/database/use-cross-region-read-replicas-with-amazon-relational-database-service-for-sql-server/>

The design seems to be what we are looking in terms of option D.

<https://d2908q01vomqb2.cloudfront.net/887309d048beef83ad3eabf2a79a64a389ab1c9f/2022/11/15/dbblog-2614-image001.png>

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: D

D makes the most sense

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: D

No global tables concept in RDS, B,C are eliminated. A is wrong in terms of backing up Db copy to a standalone instance ? D provides read replicas for reading and also switches as a failover in times of disruption and becomes primary. this is how HA can be maintained. D is correct.

upvoted 3 times

✉ **spd** 1 year, 1 month ago

Selected Answer: D

MySQL - Read Replica. In this case, this is not aurora so not the global table option and hence can not be B and C

upvoted 1 times

✉ **sambb** 1 year, 1 month ago

I haven't found any information about a "global table" for RDS.

Global tables are for DynamoDB. For Aurora, it's called "global databases".

RDS for MySQL supports cross-region read replicas <https://aws.amazon.com/fr/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/>, so D has a better availability than A.

upvoted 2 times

✉ **icassp** 1 year, 2 months ago

Selected Answer: D

for B,C, Amazon RDS does not support global tables yet. Only Aurora supports.

upvoted 4 times

✉ **AlanKrish** 1 year, 1 month ago

Is Aurora not part of RDS? You can choose Aurora's compatibility with MySQL and PostgreSQL).

upvoted 1 times

✉ **zhangyu20000** 1 year, 2 months ago

D is correct

upvoted 3 times

✉ **masetromain** 1 year, 2 months ago

<https://www.examtopics.com/discussions/amazon/view/69438-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

It is possible that some people may think that option D. Configure read replicas on Amazon RDS. In the case of disruption, promote a cross-Region and read replica to be a standalone DB instance. Direct database traffic to the promoted DB instance. Create a replacement read replica that has the promoted DB instance as its source. is the best solution, as it also utilizes read replicas and cross-Region promotion to minimize downtime. However, it is important to consider that while this solution provides high availability, it doesn't provide the same level of automatic replication that global tables do. In case of a disruption, there is a risk of data loss during the manual switchover.

and also with option D, you are still working with a single point of failure, the primary database, while in option B you have multiple copies of your data distributed across different regions, so in case of a failure you can switch over to one of the replicas without loss of data.

upvoted 2 times

✉ **Shahul75** 1 year, 2 months ago

B is not right. Only Aurora has global tables. RDS don't

upvoted 1 times

✉ **[Removed]** 1 year, 1 month ago

Cant be B due to global tables, ReadReplicas are supported with RDS and other options of restoring from backup do not create high availability

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: B

The correct answer is option B. Configuring global tables and read replicas on Amazon RDS with the cross-Region scope enabled provides the highest availability for the database. In case of disruption, the company can use AWS Lambda to copy the read replicas from one Region to another Region, ensuring that the website remains operational at all times. This solution provides automatic failover across multiple regions and allows for fast recovery in case of a disruption.

Option A involves promoting an automated backup to be a standalone DB instance and creating a replacement read replica that has the promoted DB instance as its source. This solution is less efficient since it requires manual intervention and additional steps to promote the backup and create a replacement read replica.

upvoted 2 times

✉ **Sarutobi** 1 year, 1 month ago

If the disruption is an outage that takes the Region offline completely, how could we use Lambda to copy the read replica from the Region that is no longer available to the backup to another Region?

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Option C involves configuring global tables and automated backups on Amazon RDS. This solution is less efficient since it does not provide automatic failover across multiple regions and requires additional steps to copy the read replicas from one Region to another Region using AWS Lambda.

Option D involves configuring read replicas on Amazon RDS. In the case of disruption, promoting a cross-Region and read replica to be a standalone DB instance. This solution is less efficient than Option B since it does not provide automatic failover across multiple regions and requires manual intervention to promote the read replica to a standalone instance.

upvoted 1 times

 **bcx** 9 months, 3 weeks ago

In fact global tables is a Dynamo DB thing. And RDS has Aurora Global Database. In this case Aurora is out of the question, it says RDS MySql, not Aurora (RDS) MySQL.

upvoted 1 times

Question #77

Topic 1

Example Corp. has an on-premises data center and a VPC named VPC A in the Example Corp. AWS account. The on-premises network connects to VPC A through an AWS Site-To-Site VPN. The on-premises servers can properly access VPC A. Example Corp. just acquired AnyCompany, which has a VPC named VPC B. There is no IP address overlap among these networks. Example Corp. has peered VPC A and VPC B.

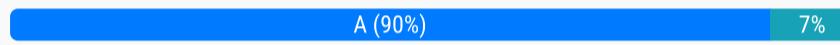
Example Corp. wants to connect from its on-premise servers to VPC B. Example Corp. has properly set up the network ACL and security groups.

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

- A. Create a transit gateway. Attach the Site-to-Site VPN, VPC A, and VPC B to the transit gateway. Update the transit gateway route tables for all networks to add IP range routes for all other networks.
- B. Create a transit gateway. Create a Site-to-Site VPN connection between the on-premises network and VPC B, and connect the VPN connection to the transit gateway. Add a route to direct traffic to the peered VPCs, and add an authorization rule to give clients access to the VPCs A and B.
- C. Update the route tables for the Site-to-Site VPN and both VPCs for all three networks. Configure BGP propagation for all three networks. Wait for up to 5 minutes for BGP propagation to finish.
- D. Modify the Site-to-Site VPN's virtual private gateway definition to include VPC A and VPC B. Split the two routers of the virtual private gateway between the two VPCs.

Correct Answer: D

Community vote distribution



✉ **rbm2023** 11 months, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/pt_br/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html
Transit gateway is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks. AWS Transit Gateway + VPN, using the Transit Gateway VPN Attachment, provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet, as shown in the following picture.
<https://docs.aws.amazon.com/images/whitepapers/latest/aws-vpc-connectivity-options/images/image4.png>
Option A is the correct answer since the transit gateway will allow both VPCs to connect to the on-premises network.
Option B suggests the same feature but is using the Transit Gateway in an incorrect way. The sole purpose of the gateway is to have a point for interconnectivity.

upvoted 7 times

✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: A

A, Transit Gateway
upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: A

Option A is the most straightforward and effective solution. A transit gateway acts as a cloud router that simplifies network topology and connectivity between on-premises networks, VPCs, and other AWS services. By attaching both VPCs (A and B) and the Site-to-Site VPN to a single transit gateway and updating the route tables accordingly, Example Corp. can enable seamless communication between its on-premises network and both VPCs. This approach minimizes operational effort by centralizing network management and eliminating the need for complex routing configurations or multiple VPN connections.

Option D proposes modifying the Site-to-Site VPN's virtual private gateway to include both VPC A and VPC B. However, a virtual private gateway cannot be directly shared or split between VPCs in the manner described. This option misunderstands the architecture of AWS networking components and their capabilities.

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: A

A = correct
B = if you setup a second VPN you do not need a TGW
C = peering does not allow edge-to-edge routing (aka VPC B cannot access on-premises via VPC A and vice versa)
D = Virtual Private Gateway is specific to a single VPC
upvoted 1 times

✉ **Russ99** 7 months, 2 weeks ago

Selected Answer: A

reluctantly selecting option A. these answers do not take into consideration that the On-promises already has a peered connection to VPC A through the existing site to site

upvoted 2 times

 **CuteRunRun** 8 months ago

Selected Answer: A

I think A is right, I do not know why other guys select D

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

surely A

upvoted 1 times

 **Tunstim** 11 months, 1 week ago

For those that have written SAP-C02, how relevant are these questions to the real exam questions? After adequate preparation, I wanted to truly test my knowledge before dabbling into the exam and would really appreciate anyone's candid opinion.

Thanks.

upvoted 4 times

 **chikorita** 6 months, 4 weeks ago

please reply to him

upvoted 2 times

 **Parsons** 11 months, 2 weeks ago

Selected Answer: A

A is the best option.

Creating a transit gateway and attaching Site-to-Site VPN, VPC A, and VPC B to the transit gateway would enable the on-premise servers to access VPC B with minimal operational effort. The transit gateway route tables would need to be updated with IP range routes for all the other networks to enable communication between the VPCs and the on-premises servers.

upvoted 2 times

 **Arnaud92** 1 year ago

Selected Answer: A

Solution A is the only one possible solution

upvoted 1 times

 **Arnaud92** 1 year ago

B is impossible : When you create a S2S VPN connection, it's between 2 entities (here, the onprem and VPC B). It says that they connect the onprem to VPCB with S2VPN AND THEN to a TGW, it's not possible to connect a S2S VPN from onprem to VPC to a TGW (it's a 3 entities).

You can however connect a S2S VPN to a TGW (onprem to TGW) (which is solution A).

C : Does not work, there is no transitivity on AWS. S2S VPN cannot reach VPC B through VPC A

D is impossible : There is no magic, you cannot "split" router (that does not exist). VGW is attach to a single VPC. A S2S VPN cannot multiplex VPC

upvoted 4 times

 **Arnaud92** 1 year ago

A : the best (and the only one possible) answer : When you have 2 VPC, you have multiple solution to connect to onprem :

- Create 2 S2S VPN (1 for each VPC)

- or Create a TGW, attach both VPC to it and attach S2S VPN to it too

- or Create a third VPC (VPC routing), and peer VPC A with VPC routing, VPC B to VPC routing, attach a S2S VPN to VPC routing and use a NVA on VPC routing to route traffic. NVA can do transitivity.

Here, solution A is one of the possible answer

upvoted 4 times

 **mfsec** 1 year ago

Selected Answer: A

A. Create a transit gateway. Attach the Site-to-Site VPN

upvoted 1 times

 **dev112233xx** 1 year ago

Selected Answer: A

A makes sense to me

upvoted 1 times

 **taer** 1 year ago

Selected Answer: A

A for me

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

A has this weird wording - attaching S-S VPN ? transit gateway attaches to VPCs only not S-S vpn. A is wrong. Since VPC A and VPC B are already peered, the easiest solution to connect from the on-premises servers to VPC B would be to create another Site-to-Site VPN connection

between the on-premises data center and VPC B. This would require minimal operational effort, as the existing VPN connection with VPC A can remain unchanged.

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

oops this is wrong..VPN can be attached...

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Moderator, please delete this comment..

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/how_it_works.html

When you create a virtual private gateway, you can specify the private Autonomous System Number (ASN) for the Amazon side of the gateway. If you don't specify an ASN, the virtual private gateway is created with the default ASN (64512). You cannot change the ASN after you've created the virtual private gateway. Due to this reason, So A is not possible (with least effort). Answer should be B.

upvoted 1 times

 **Arnaud92** 1 year ago

THe VGW for VPCA is no more needed on A because you attach the VPCA to the TGW.

The ASN will be on the TGW attachment with the S2S VPN.

This is the best solution.

In the meantime, B is impossible. When you create a S2S VPN connection, it's between 2 entites (here, the onprem and VPC B). It says that they connect the onprem to VPCB with S2SVPN AND THEN to a TGW, it's not possible to connect a S2S VPN from onprem to VPC to a TGW. You can however connect a S2S VPN to a TGW (onprem to TGW).

upvoted 1 times

 **spd** 1 year, 1 month ago

Selected Answer: A

TGW is the solutions

upvoted 1 times

 **CloudFloater** 1 year, 1 month ago

Selected Answer: D

D.

A - setting up new transit gateway - more operational cost

B - new site-to-site - vpn - more operational cost

C - updating route tables for site to site vpn and 3 VPCs, bgp config update for 3 networks .. more operational cost

D - because it requires the least amount of operational effort. By modifying the Site-to-Site VPN's virtual private gateway definition to include both VPC A and VPC B and splitting the two routers of the virtual private gateway between the two VPCs, the on-premises servers can connect to both VPCs with minimal additional effort. This solution leverages the existing Site-to-Site VPN and does not add any additional layers of complexity to the network.

upvoted 1 times

 **Sarutobi** 1 year, 1 month ago

It looks like you understood D. How can you split two routers of the VGW between two VPCs? The VGW is an object that can be attached to a single VPC at a time. What are the two routers they talk about here? Are there on-prem routers?

upvoted 1 times

 **Arnaud92** 1 year ago

D is not possible. There is no magic, you cannot "split" router (that does not exist). VGW is attach to a single VPC. A S2S VPN cannot multiplex VPC ;)

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: A

solution is A

upvoted 1 times

Question #78

Topic 1

A company recently completed the migration from an on-premises data center to the AWS Cloud by using a replatforming strategy. One of the migrated servers is running a legacy Simple Mail Transfer Protocol (SMTP) service that a critical application relies upon. The application sends outbound email messages to the company's customers. The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only.

The company decides to use Amazon Simple Email Service (Amazon SES) and to decommission the legacy SMTP server. The company has created and validated the SES domain. The company has lifted the SES limits.

What should the company do to modify the application to send email messages from Amazon SES?

- A. Configure the application to connect to Amazon SES by using TLS Wrapper. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Attach the IAM role to an Amazon EC2 instance.
- B. Configure the application to connect to Amazon SES by using STARTTLS. Obtain Amazon SES SMTP credentials. Use the credentials to authenticate with Amazon SES.
- C. Configure the application to use the SES API to send email messages. Create an IAM role that has ses:SendEmail and ses:SendRawEmail permissions. Use the IAM role as a service role for Amazon SES.
- D. Configure the application to use AWS SDKs to send email messages. Create an IAM user for Amazon SES. Generate API access keys. Use the access keys to authenticate with Amazon SES.

Correct Answer: A*Community vote distribution*

scuzzy2010 Highly Voted 1 year, 1 month ago

Selected Answer: B

B is correct.

<https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

STARTTLS supports ports 25, 587, and 2587

TLSWRAPPER supports ports 465 and 2465

upvoted 13 times

God_Is_Love 1 year, 1 month ago

FYI Amazon SES supports STARTTLS encryption over port 587, which is the recommended port for email transmission. But existing port 25 can be configured too as in this case as the migration came from SMTP port 25

upvoted 5 times

Untamables Highly Voted 1 year, 2 months ago

Selected Answer: B

In this scenario, you should use Amazon SES SMTP interface to send emails because the application can use SMTP only.

<https://docs.aws.amazon.com/ses/latest/dg/send-email-smtp.html>

<https://docs.aws.amazon.com/ses/latest/dg/smtp-credentials.html>

<https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

upvoted 8 times

8608f25 Most Recent 1 month, 3 weeks ago

Selected Answer: B

Here's why option B is the correct choice:

STARTTLS Support: Amazon SES supports STARTTLS, a protocol command used to upgrade an existing insecure connection to a secure connection using TLS (Transport Layer Security). This is crucial since the legacy SMTP server does not support TLS, and STARTTLS can be used to initiate a secure connection.

SMTP Credentials: Amazon SES requires authentication to send emails through its SMTP interface. This is achieved by using SMTP credentials, which are different from AWS access keys. SMTP credentials can be obtained from the Amazon SES console and are used to authenticate with the Amazon SES SMTP endpoint.

Operational Simplicity: This approach allows the application to continue using SMTP for sending emails, which aligns with the application's existing capabilities. By using STARTTLS, the application can upgrade its connection to Amazon SES to a secure one, ensuring compliance with security best practices without significant changes to the application's email sending functionality.

upvoted 1 times

LazyAutonomy 2 months, 1 week ago

Selected Answer: A

Terrible Q. All answers are wrong.

A is wrong because you cannot send emails through SES SMTP using SMTP credentials derived from temporary STS tokens (ie IAM roles). Must

use an IAM user access keys to derive creds.

B is wrong because the question imposes a constraint that prevents us from selecting an answer that requires upgrading or modifying the application itself. Could you just offload SMTP STARTTLS/AUTH to the local sendmail/postfix daemon? Maybe, if it were Linux, but what if it's Windows? Cygwin? WSL?

C & D - wrong, for a similar rationale as B.

But the question designer OBVIOUSLY doesn't know that IAM roles can't be used for SES SMTP auth, because these questions are written by inexperienced, unqualified people who are not themselves architects or engineers.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

To be fair, the question says this:

"The legacy SMTP server does not support TLS encryption and uses TCP port 25. The application can use SMTP only."

The question doesn't say the application cannot handle STARTTLS or SMTP AUTH. In theory, if an application claims to support SMTP, then it should support all features of SMTP, which includes STARTTLS and AUTH. It only says the legacy SMTP server cannot handle TLS. So I suppose perhaps B is correct after all :-)

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

Selected Answer: B

A = this sends email via SES API while application can use SMTP only

B = correct

C = this sends email via SES API while application can use SMTP only

D = this sends email via SES SDK (API) while application can use SMTP only

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

Need to correct my comment on A. This is a TLS Wrapper (A) vs STARTTLS (B), where STARTTLS allows initiating an encrypted connection by first establishing an unencrypted connection. While TLS Wrapper is a means of initiating an encrypted connection without first establishing an unencrypted connection (it's the client's responsibility to connect to the endpoint using TLS, and to continue using TLS for the entire conversation). As our app can only work with SMTP we should go for B

upvoted 1 times

 **edder** 4 months, 2 weeks ago

Selected Answer: B

The correct answer is B.

A: We are unable to obtain authentication information.

C,D: Does not meet SMTP requirements.

B: This is the correct procedure.

<https://repost.aws/knowledge-center/ses-set-up-connect-smtp>

<https://docs.aws.amazon.com/ses/latest/dg/security-protocols.html>

upvoted 1 times

 **totten** 6 months, 1 week ago

Selected Answer: B

Here's why option B is the correct choice:

SMTP Protocol: The legacy SMTP server uses the SMTP protocol, and Amazon SES provides an SMTP interface for sending email, which is suitable for your application.

STARTTLS: Using STARTTLS ensures that your communication with Amazon SES is encrypted, which is a best practice for secure email transmission.

SMTP Credentials: Amazon SES SMTP credentials are required to authenticate your application with Amazon SES when sending emails. These credentials include an SMTP username and password.

upvoted 2 times

 **totten** 6 months, 1 week ago

Option A mentions TLS Wrapper, which isn't a standard approach when using Amazon SES for sending email. Amazon SES supports STARTTLS for secure communication.

Option C suggests using the SES API, which is a valid approach but requires code modifications to use the SES API instead of SMTP. Since your application can only use SMTP, this option might involve significant code changes.

Option D mentions using AWS SDKs and IAM users, which is more suitable for programmatic access to SES but not for legacy SMTP applications that can only send via SMTP.

Therefore, Option B is the most appropriate choice for configuring your application to send email messages from Amazon SES while preserving the SMTP protocol and ensuring secure communication.

upvoted 3 times

 **CuteRunRun** 8 months ago

Selected Answer: A

I selecte A

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

It's B - to preserve SMTP protocol

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

B because is "legacy" app then use properties to set SMTP keyword === Obtain Amazon SES SMTP credentials

upvoted 1 times

✉ **F_Eldin** 11 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/big-data/query-and-visualize-aws-cost-and-usage-data-using-amazon-athena-and-amazon-quicksight/>

upvoted 1 times

✉ **rbm2023** 11 months, 1 week ago

Selected Answer: B

Option A states that the company would require to do more changes in the application than a replatform migration strategy where we are supposed to migrate the application with minimal changes. In Option A using the TLS wrapper would require an additional layer of software (stunnel) to be installed and configured on the EC2 instance, which may introduce additional complexity and management overhead.

In option B, we need to configure the application to connect to SES using STARTTLS using SMTP credentials, since the legacy SMTP server does not support TLS encryption. This would require minimal change to the application.

upvoted 3 times

✉ **Cassa** 12 months ago

Selected Answer: B

To set up a STARTTLS connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 25, 587, or 2587, issues an EHLO command, and waits for the server to announce that it supports the STARTTLS SMTP extension. The client then issues the STARTTLS command, initiating TLS negotiation. When negotiation is complete, the client issues an EHLO command over the new encrypted connection, and the SMTP session proceeds normally

To set up a TLS Wrapper connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 465 or 2465. The server presents its certificate, the client issues an EHLO command, and the SMTP session proceeds normally.

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: B

B. Configure the application to connect to Amazon SES by using STARTTLS.

upvoted 1 times

✉ **Dimidrol** 1 year ago

Selected Answer: B

B , <https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

upvoted 3 times

✉ **dev112233xx** 1 year ago

Selected Answer: A

B is wrong because STARTTLS uses port 25 and EC2 instances can't send outbound traffic through port 25 (you must ask AWS to allow port 25)

upvoted 2 times

✉ **F_Eldin** 10 months, 1 week ago

<https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>

says:

"Amazon Elastic Compute Cloud (Amazon EC2) throttles email traffic over port 25 by default. To avoid timeouts when sending email through the SMTP endpoint from EC2, submit a Request to Remove Email Sending Limitations"

And the question explicitly says:

"The company has lifted the SES limits."

upvoted 2 times

✉ **hobokabobo** 1 year, 1 month ago

Selected Answer: B

The key to this question imo is the sentence "The application can use SMTP only".

So we cannot go for encryption.

Imo there is no TLS wrapper for Mail that supports authentication which is needed for SES, one needs a proxying mailserver for that(need support for auth and encryption, rewriting mail).

With StartTLS SMTP protocol is supported by AWS and the legacy application can send the mail to AWS just as it did to the legacy mailserver. (Of course: a unix machine has not just one application but a lot of little apps like cron, at ... and low traffic mailserver consumes like no resources, so in real world every unix machine should have a small local smtp, eg a postfix configured to forward all traffic from every tool app, system ... to ses but that real world option is not provided as possible answer: so B.)

upvoted 2 times

✉ **hobokabobo** 1 year, 1 month ago

you may look at <https://www.stunnel.org/>, if find a way to make auth work with ses: well then go for A. Afaik it is not possible - but happy to learn if there is a way.

upvoted 1 times

✉ **hobokabobo** 1 year, 1 month ago

also have a look at

<https://hector.dev/2015/01/17/sending-e-mail-via-amazon-ses-over-smtp-with-iam-roles/>

Using iam roles does not realy work with smpt auth.(I didn't get it to work and it seems no one else either)

upvoted 1 times

Question #79

Topic 1

A company recently acquired several other companies. Each company has a separate AWS account with a different billing and reporting method. The acquiring company has consolidated all the accounts into one organization in AWS Organizations. However, the acquiring company has found it difficult to generate a cost report that contains meaningful groups for all the teams.

The acquiring company's finance team needs a solution to report on costs for all the companies through a self-managed application.

Which solution will meet these requirements?

- A. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a table in Amazon Athena. Create an Amazon QuickSight dataset based on the Athena table. Share the dataset with the finance team.
- B. Create an AWS Cost and Usage Report for the organization. Define tags and cost categories in the report. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.
- C. Create an Amazon QuickSight dataset that receives spending information from the AWS Price List Query API. Share the dataset with the finance team.
- D. Use the AWS Price List Query API to collect account spending information. Create a specialized template in AWS Cost Explorer that the finance department will use to build reports.

Correct Answer: D

Community vote distribution

A (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: A

The correct solution is A.

Creating an AWS Cost and Usage Report for the organization and defining tags and cost categories in the report will allow for detailed cost reporting for the different companies that have been consolidated into one organization. By creating a table in Amazon Athena and an Amazon QuickSight dataset based on the Athena table, the finance team will be able to easily query and generate reports on the costs for all the companies. The dataset can then be shared with the finance team for them to use for their reporting needs.

Option B is not correct because it does not provide a way to query and generate reports on the costs for all the companies.

Option C is not correct because it only provides spending information from the AWS Price List Query API and does not provide detailed cost reporting for the different companies.

Option D is not correct because it only uses the AWS Price List Query API and does not provide a way to query and generate reports on the costs for all the companies.

upvoted 13 times

 **moota**  1 year, 1 month ago

Selected Answer: A

I can customize reporting in Cost Explorer but cannot find how to do templates.

upvoted 5 times

 **ninomfr64**  2 months, 3 weeks ago

Selected Answer: A

A = correct

B = there isn't specialized templates in AWS Cost Explorer. It provides default reports, but also enables you to change the filters and constraints used to create the reports. You can save the reports that you made as a bookmark, download the CSV file, or save them as a report

C & D = AWS Price List provides a catalog of the products and prices for AWS services that you can purchase on AWS, not cost of your resources

upvoted 1 times

 **CuteRunRun** 8 months ago

Selected Answer: A

I prefer A

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

its n A

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

Selected Answer: A

I vote A mostly because there is no template option in Cost Explorer and A is the only other option which covers the scenario
upvoted 1 times

✉️ **F_Eldin** 11 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/big-data/query-and-visualize-aws-cost-and-usage-data-using-amazon-athena-and-amazon-quicksight/>
upvoted 3 times

✉️ **mfsec** 1 year ago

Selected Answer: A

A. Create an AWS Cost and Usage Report for the organization.
upvoted 1 times

✉️ **zhangyu20000** 1 year, 2 months ago

A is correct
B: no such template for cost explorer
CD: Price List Query API is for list price, not for usage
upvoted 2 times

Question #80

Topic 1

A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.

The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.

Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS.
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load.
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance.

Correct Answer: CE*Community vote distribution*

CE (67%)

BC (18%)

Other

✉  **masetromain**  1 year, 2 months ago

Selected Answer: CE

C and E are the correct answers.

Option C: Leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data would help to resolve the issues with the API servers being consistently overloaded. By using Kinesis, the data can be ingested and processed in real-time, allowing the API servers to handle the increased load. Using Lambda to process the data can also help to improve the overall performance and scalability of the platform.

Option E: Re-architecting the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance would help to resolve the issues with high write latency. DynamoDB is a NoSQL database that is designed for high performance and scalability, making it a good fit for this use case. Additionally, DynamoDB supports auto-scaling, which can help to ensure that the database can handle the expected growth in the number of sensors.

upvoted 19 times

✉  **OCHT** 1 year ago

While options C and E may also provide some benefits, they may not address the underlying issues with the overloaded API servers and high write latency in the database. Therefore, options B and D are the best combination for resolving the issues and enabling growth as new sensors are provisioned.

upvoted 1 times

✉  **SuperP43** 1 year, 1 month ago

I disagree with option E. Re-architecting the database tier from RDS to DynamoDB is not possible. RDS is a SQL database, and DynamoDB is a NoSQL database.

The correct one should be C and B

upvoted 4 times

✉  **ajeeshb** 4 weeks, 1 day ago

That is why it says to "Re-architect the DB tier".

upvoted 1 times

✉  **tromyunpak** 10 months, 1 week ago

if it was read operations yes but the issue is write latency. also rds proxy is used to handle the write operations

upvoted 2 times

✉  **tromyunpak** 10 months, 1 week ago

also rds proxy is not used (sorry typo) to handle write operations properly

upvoted 1 times

✉  **kamaro** 1 year, 1 month ago

I agree with you.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html

Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. The underlying storage grows automatically as needed. An Aurora cluster volume can grow to a maximum size of 128 tebibytes (TiB).

upvoted 2 times

 **zejou1** 1 year ago

Naw, you can migrate: <https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/>

Plus, with DynamoDB it scales, don't need to add read replica complexity and it also supports IoT out of the box - <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.WhyDynamoDB.html>

This is for IoT sensors that send data and I don't need to store forever so, DynamoDB for this use case is better and cheaper allowing scale

upvoted 1 times

 **Sarutobi** 11 months ago

I think this is the big point in this question and that DynamoDB is being position by AWS for IoT very hard. Although is technically possible to migrate with DMS from SQL to DynamoDB, is hard, but harder yet is the change of model inside the application or service.

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Option A, Resizing the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS will not solve the problem, as the problem is not just related to storage size but also high write latency.

Option B, Re-architecting the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and adding read replicas would help to improve the read performance, but it won't help in reducing write latency.

Option D, Using AWS X-Ray to analyze and debug application issues and adding more API servers to match the load, would help in identifying the problem and resolving it, but it will not help in reducing the load on the servers.

upvoted 3 times

 **TonytheTiger** Most Recent 6 days, 11 hours ago

Selected Answer: CE

Option CE and BC. The only reason I choose E over B because said SO. Per AWS, DynamoDB is suitable for IoT (Sensor data and log ingestion)

<https://docs.aws.amazon.com/whitepapers/latest/best-practices-for-migrating-from-rdbms-to-dynamodb/suitable-workloads.html>

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: CE

CE, kinesis + lambda & Dynamodb

upvoted 1 times

 **a54b16f** 1 month, 1 week ago

Selected Answer: BC

Switching from RDS mysql to aurora will improve performance, by up to 10 times, which could solve the write issue. Switching from relationship database to nosql is not practical, need re-engineering whole application. plus, the performance improvement of nosql are around data read, not data write (creating/updating indexes is a huge effort)

upvoted 1 times

 **8608f25** 1 month, 3 weeks ago

Selected Answer: BC

* B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Aurora provides several benefits over standard RDS MySQL, including better performance, scalability, and availability. It automatically grows storage as needed, up to 128 TB, potentially providing better write performance. Aurora also supports up to 15 read replicas with very low replication latency, improving read performance significantly and reducing the load on the primary database instance.

upvoted 1 times

 **8608f25** 1 month, 3 weeks ago

* C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data.

By using Amazon Kinesis Data Streams, the company can collect, process, and analyze real-time, streaming data so that it can react to new information quickly. This service allows for the ingestion of a large amount of data generated by IoT sensors. AWS Lambda can then be used to process this data in real-time, which can help to offload the work from the API servers, reducing their load. This setup can scale automatically with the number of incoming data records, providing a more efficient and cost-effective solution to handle growth.

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

Selected Answer: CE

A = does not fix permanently (who knows that 6TB is enough?)

B = going from RDS to Aurora will not fix the issue

C = correct

D = this could work, but it is not cost efficient (more EC2 instance along the line)

E = correct

upvoted 2 times

 **Pupu86** 5 months ago

Selected Answer: CE

The requirement is to resolve high write latency while Aurora is a good fit for structured datasets but option B has indicated read replica as a direction for resolution against a question seeking resolution in write latency. So Option B is definitely out.

upvoted 1 times

 **duriselvan** 7 months, 3 weeks ago

Amazon RDS FeaturesAmazon RDS supports multiple database engines, including Amazon Aurora, MySQL, MariaDB, Oracle, Microsoft SQL Server, and PostgreSQL. Amazon RDS allows you to scale your database instances' storage size and performance. Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. Amazon RDS provides a cost-effective way to manage relational databases in the cloud. DynamoDB FeaturesPrimarily, DynamoDB features flexibility, scalability, and performance. It offers high availability out of the box with no need for setup or configuration. DynamoDB automatically replicates your data across multiple Availability Zones within a Region to give you fault tolerance and high availability.

upvoted 1 times

 **duriselvan** 7 months, 3 weeks ago

c and E ans 100 %

upvoted 1 times

 **rizzu2023** 8 months ago

CE

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

upvoted 1 times

 **easytoo** 8 months, 2 weeks ago

b-c-b-c-b-c-b-c

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: CE

CE for sure. classic IoT use case

upvoted 1 times

 **Asds** 9 months, 3 weeks ago

Selected Answer: BD

Rds MySQL to Aurora to scale automatically and stay relational

upvoted 1 times

 **HussamShokr** 9 months, 3 weeks ago

Selected Answer: BC

Options A, D, and E are not the most suitable choices for resolving the issues and enabling growth while keeping the platform cost-efficient in this scenario:

A. Resizing the MySQL General Purpose SSD storage to 6 TB might increase the volume's IOPS, but it won't address the underlying scalability and performance issues caused by the growing number of sensors and high write latency.

D. While using AWS X-Ray for analyzing and debugging application issues can help optimize performance, it alone won't be sufficient to handle the increased workload caused by the growing number of sensors.

E. Re-architecting the database tier to use Amazon DynamoDB instead of RDS MySQL would require significant changes to the application and might not be cost-efficient, considering the already established use of RDS MySQL. DynamoDB is a NoSQL database and requires a different data modeling approach compared to a relational database like MySQL.

upvoted 1 times

 **bcx** 9 months, 3 weeks ago

Selected Answer: CE

C: Kinesis Data Stream, scalable large volume ingestion. Process with Lambda, also scalable.

E: Use DynamoDB, Aurora, replicas, etc are not meant for this class of applications. You would have to increase more and more capacity and will be too expensive. At one time it may not be enough.

upvoted 1 times

 **Jesuisleon** 10 months, 1 week ago

Selected Answer: CE

A is wrong. for gp2, 3 iops per gb and when you increase your ebs from 4tb to 6tb, you increase your iops from 1,2000 to 1,6000(not 1,8000 because the max iops for gp2 is 1,6000, see <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>), the key word in the question is "resolve the issues permanently" this method can't resolve the problem permanently.

B is wrong because the scenario is mainly focus on writing to db, so read replica really can't help too much.

D is wrong since the bottleneck is at DB "RDS metrics show high write latency"

upvoted 2 times

 **dev112233xx** 10 months, 3 weeks ago

Selected Answer: CE

C&E for me...

If you choose B&E (Kinesis+Lambda to Ingest Aurora database) you will need also to add to the solution RDS Proxy, since Lambda will keep opening DB connections and this will impact the DB performance and probably the cost

upvoted 1 times

Question #81

Topic 1

A company is building an electronic document management system in which users upload their documents. The application stack is entirely serverless and runs on AWS in the eu-central-1 Region. The system includes a web application that uses an Amazon CloudFront distribution for delivery with Amazon S3 as the origin. The web application communicates with Amazon API Gateway Regional endpoints. The API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket.

The company is growing steadily and has completed a proof of concept with its largest customer. The company must improve latency outside of Europe.

Which combination of actions will meet these requirements? (Choose two.)

- A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs.
- B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints.
- D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.
- E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database.

Correct Answer: AC

Community vote distribution



✉ **masetromain** 1 year, 2 months ago

Selected Answer: AC

A and C are correct answers.

- A. Enable S3 Transfer Acceleration on the S3 bucket and ensure that the web application uses the Transfer Acceleration signed URLs will accelerate the uploads of documents to S3 bucket, this will help to reduce the latency for users outside of Europe.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints will help the company to improve the latency by caching the responses of the API Gateway closer to the users.

upvoted 17 times

✉ **bcx** 9 months, 3 weeks ago

A is wrong because the users of S3 are the lambda functions, not the end user. "The API Gateway APIs call AWS Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket."

upvoted 2 times

✉ **Sab** 7 months ago

Users of S3 are not lambda, lambda is used only for writing to serverless database. Also, Aurora serverless global database only writes in one cluster and the other region cluster are used only for reads. So no matter from which location you upload, the metadata will be written to cluster in Central Europe . If it was Global DynamoDB table then it could have helped to reduce latency.

upvoted 2 times

✉ **ninomfr64** 2 months, 3 weeks ago

"web app uses CloudFront distribution for delivery with Amazon S3 as the origin" and "Lambda functions that store metadata in an Amazon Aurora Serverless database and put the documents into an S3 bucket" these 2 sentences let me think that users are not uploading via CloudFront into the S3 bucket at its origin, rather docs are uploaded from the Lambda

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

- B. Creating an accelerator in AWS Global Accelerator and attaching it to the CloudFront distribution will not help in this scenario as it only helps to route the traffic to the optimal endpoint based on the location of the user.
- D. Provisioning the entire stack in two other locations that are spread across the world and using global databases on the Aurora Serverless cluster will help to reduce the latency but it would be more complex to implement and manage.
- E. Adding an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database will not help in this scenario because it is only used to improve connection management and load balancing for Amazon RDS databases, but not for Aurora Serverless databases.

upvoted 4 times

✉ **masetromain** 1 year, 2 months ago

<https://www.examtopics.com/discussions/amazon/view/69470-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉ **Japanese1** 4 months, 2 weeks ago

Complexity is not evidence against option D.

Furthermore, option D is correct because the question statement also suggests that costs can be incurred.

On the other hand, A is not a method to eliminate geographical factors.

upvoted 1 times

✉️  **red_panda** Most Recent 4 days, 14 hours ago

Selected Answer: AC

A and C for me are the correct answers.

D is not so useful as we are recreating the entire stack and increase a lot the costs. As first approach, A and C are the most appropriate

upvoted 1 times

✉️  **faiexamonly** 2 weeks, 1 day ago

Selected Answer: AC

Aurora Serverless does not support global database. search DB instance class requirements in

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database-getting-started.html>

upvoted 1 times

✉️  **Dgix** 2 weeks, 5 days ago

Selected Answer: AC

By elimination: B is pointless, as CF already does geo proximity. D is impossible as global DBs aren't supported by Aurora Serverless. E doesn't really help.

Remaining: A and C, which are sensible and will do the trick.

upvoted 1 times

✉️  **gofavad926** 3 weeks, 2 days ago

Selected Answer: AC

AC, s3 transfer acceleration + edge-optimised api gateway

upvoted 1 times

✉️  **ninomfr64** 2 months, 3 weeks ago

Selected Answer: CD

This is tricky. Here is my take having in mind that the question is "The company must improve latency outside of Europe".

A = Transfer Acceleration improves upload/downlad time, but we have already CloudFront that can also be used to speedup upload. This will not further improve. Also I don't know how to combine TA with CF

B = This will not help and also I don't know how to combine GA with CF

C = correct

D = correct

E = RDS Proxy do not improve latency

upvoted 1 times

✉️  **djeong95** 1 month, 1 week ago

Looks like D is wrong because you don't use global databases on the Aurora Serverless cluster. That is just not a feature given by Aurora Serverless (even v2). However, it does support using Aurora Serverless in global databases. "The secondary clusters" in the link below is a reference to Aurora Global Database.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless.ha>:~:text=You%20can%20use%20Aurora%20Serverless%20v2%20capacity%20in%20the%20secondary%20clusters%20so%20they%27re%20ready%20to%20take%20over%20during%20disaster%20recovery.

upvoted 1 times

✉️  **djeong95** 1 month ago

In addition, we are more likely to get latency from Lambda functions loading documents into S3 from API Gateway calls than we are from Lambda functions loading metadata into Aurora Serverless DB.

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

✉️  **JMAN1** 3 months, 1 week ago

Selected Answer: CD

Tricky Tricky.

A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs. -> Wrong. No such thing like TA signed URLs.

B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution. -> Wrong GA does not support CF.

C. Change the API Gateway Regional endpoints to edge-optimized endpoints.

D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.

E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database. -> Wrong. It is not related with latency.

upvoted 2 times

✉️  **jpa8300** 3 months, 1 week ago

Yes there is, <https://stackoverflow.com/questions/37437782/aws-transfer-acceleration-with-pre-signed-urls-using-javascript-sdk>

upvoted 1 times

✉️  **JMAN1** 2 months, 3 weeks ago

Sorry. I was wrong. Answer is A C.

serverless does not support global database and RDS proxy.

upvoted 1 times

✉  **JMAN1** 2 months, 3 weeks ago

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html#aurora-serverless.limitations>
upvoted 1 times

✉  **kmstan** 3 months, 4 weeks ago

Selected Answer: AC

A and C makes sense.

A is clear as what masetromain has explained.

C, An edge-optimized API endpoint typically routes requests to the nearest CloudFront Point of Presence (POP). It certainly improve the latency of traffic originating from Europe as the traffic will now be directed to the nearest POP instead of the origin API Gateway.

upvoted 1 times

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

Selected Answer: AC

see Sab answer

upvoted 1 times

✉  **wookchan** 6 months ago

"The company must improve latency outside of Europe."

Then in where are you going to provision an additional stack? It only says "outside of Europe."

USA? Asia? Where?

You have to consider an overall latency.

I'll go for AC

upvoted 1 times

✉  **AMohanty** 7 months ago

AD

Issue is minimize latency for "users uploading documents"

Its NOT an issue with the latency of website being delivered to the users.

Global Accelerator - Is used to decrease latency in having the user request delivered using AWS backbone network to the point of Origin
But it doesn't accelerate delivery of uploaded files into S3 so A is a better option.

RDS Proxy is used to decrease the time in establishing the DB connectivity ... It keeps few DB connections on warm-by condition. Option D doesn't help in reducing cross-Region latency

API Gateway edge point will reduce the latency in serving the website closer to ur location. But here question is about uploading document.

Aurora Serverless Global - can be used for uploading meta-data reducing latency time.

upvoted 1 times

✉  **uC6rW1aB** 7 months, 1 week ago

Selected Answer: AC

On a global scale, and particularly for users outside of Europe, the API Gateway and S3 access operations are the most likely components to introduce significant latency.

For the API Gateway, changing from regional endpoints to edge-optimized endpoints would bring API calls closer to global users.

For S3, enabling Transfer Acceleration would speed up the uploading and downloading of files.

Therefore, based on the provided system overview, these two components are the most likely areas needing optimization to reduce latency.

upvoted 1 times

✉  **Gabehcoud** 7 months, 2 weeks ago

Selected Answer: CD

even though option D is complex, it would decrease the latency outside eu region.

upvoted 2 times

✉  **nharaz** 7 months, 4 weeks ago

S3 Transfer Acceleration primarily improves upload speeds to an S3 bucket and doesn't significantly affect the latency of the web application itself.

upvoted 1 times

✉  **CuteRunRun** 8 months ago

Selected Answer: CD

I prefer CD.

A is not right. You already get a cloudfront, what is the acceleration used for.

upvoted 1 times

✉  **longns** 6 months, 1 week ago

in S3 hosted web application you upload directly to s3 using s3 url

upvoted 1 times

✉  **ninomfr64** 2 months, 3 weeks ago

You can (and should) avoid enabling S3 web site hosting working with CloudFront. You can simply configure the S3 as the distribution origin

upvoted 1 times

 **chico2023** 8 months, 1 week ago

Selected Answer: AC

Answer: A and C (over C and D which I also am inclined to).

For me, the lack of a really clear direction like "What solution will provide the best latency improvement in a cost effective way", for example, opens the debate into two possible ways.

I personally like the idea presented in C and D, but if I want to improve latency for users outside Europe, initially I would try to perform A and C. Simply because I am not sure which regions I am going to use. I know that it says "Provision the entire stack in two other locations that are spread across the world." But where, exactly? One in Sao Paulo and the other in Cape Town? How much will it improve for users in Auckland, if that's the case?

There this great blog explaining S3 Transfer Acceleration with signed URLs and how they can improve latency. Have a look:
<https://www.blendedsoftware.com/articles/how-to-accelerate-file-uploads-with-aws-s-3/>

upvoted 3 times

 **easystoo** 8 months, 2 weeks ago

c-d-c-d-c-d-c-d

Enabling S3 transfer acceleration and using Global Accelerator may help but are more targeted to optimizing S3 and CloudFront performance specifically. RDS proxies can help but do not address the broader issue of latency outside the eu-central-1 region. Spreading the stack across regions and using Aurora global databases will provide the most comprehensive latency improvements.

upvoted 2 times

Question #82

Topic 1

An adventure company has launched a new feature on its mobile app. Users can use the feature to upload their hiking and rafting photos and videos anytime. The photos and videos are stored in Amazon S3 Standard storage in an S3 bucket and are served through Amazon CloudFront.

The company needs to optimize the cost of the storage. A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days. The solutions architect needs to implement a solution that maintains millisecond retrieval availability of the photos and videos at the lowest possible cost.

Which solution will meet these requirements?

- A. Configure S3 Intelligent-Tiering on the S3 bucket.
- B. Configure an S3 Lifecycle policy to transition image objects and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days.
- C. Replace Amazon S3 with an Amazon Elastic File System (Amazon EFS) file system that is mounted on Amazon EC2 instances.
- D. Add a Cache-Control: max-age header to the S3 image objects and S3 video objects. Set the header to 30 days.

Correct Answer: B

Community vote distribution

A (97%)

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: A

The correct answer is A. Configure S3 Intelligent-Tiering on the S3 bucket.

Amazon S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers based on changing access patterns. Objects that are accessed frequently are stored in the frequent access tier and objects that are accessed infrequently are stored in the infrequent access tier. This allows for cost optimization without requiring manual intervention. This makes it an ideal solution for the scenario described, as it can automatically move objects that are infrequently accessed after 30 days to a lower-cost storage tier while still maintaining millisecond retrieval availability.

upvoted 14 times

 **masetromain** 1 year, 2 months ago

Option B is not correct as it only moves data to S3 Glacier Deep Archive after 30 days, which would still require additional steps to retrieve the data.

Option C is not correct because Amazon Elastic File System (Amazon EFS) is a file storage service for use with Amazon EC2 instances, it does not provide a cost-effective solution for storing and retrieving large amounts of data.

Option D is not correct because adding a Cache-Control: max-age header only controls the caching behavior of the objects and does not address the cost optimization requirements.

upvoted 2 times

 **jhonivy** 1 year, 2 months ago

Option D works for the reduction cost on retrieval request

upvoted 1 times

 **youngprinceton** 1 year, 2 months ago

take the test then tell us if your answers are valid, if they are share them with us ;)

upvoted 1 times

 **Vsos_in29** Most Recent 1 month, 2 weeks ago

A is right

B S3 Glacier Deep Archive after 30 days is not correct, retrieval takes time so incorrect.

upvoted 1 times

 **Sandeep_B** 5 months, 2 weeks ago

Selected Answer: A

millisecond retrieval availability

upvoted 1 times

 **wookchan** 6 months ago

A, no brainer

upvoted 2 times

 **uC6rW1aB** 7 months, 1 week ago

Selected Answer: A

A. Configure S3 Intelligent-Tiering on the S3 bucket: This option would automatically move objects to different storage tiers based on their access patterns. For objects that are infrequently accessed, this would help to reduce storage costs. For those that continue to be accessed frequently, they would remain in a higher-cost but faster-access tier. This should be the option that meets the requirements.

B. Configure an S3 Lifecycle policy to transition image and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days: This option would significantly lower storage costs, but the retrieval time for Glacier Deep Archive could take several hours, which does not meet the millisecond retrieval requirement.

upvoted 1 times

✉ **CuteRunRun** 8 months ago

Selected Answer: A

A is right

upvoted 1 times

✉ **aviathor** 8 months, 2 weeks ago

Selected Answer: A

B is wrong due to the Glacier Deep Archive part which is not warranted by the question.

C is wrong due to the cost of EFS and because it would require some kind of EC2 instance.

D would help caching the objects on proxies and clients, but other than that...

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A of course

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

Selected Answer: A

I was hesitating between A and D and D looks like a really good option but it's missing one part - we do not do anything with the storage class in this option - we only update the cache TTL which would possibly reduce some costs, however, we keep paying the same price for storage. Hence I switched to A

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

A - easy question

upvoted 1 times

✉ **dev112233xx** 1 year ago

Selected Answer: A

A - S3 Intelligent-Tiering can fit the requirement

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

First half of question drags you to answer B but SA found that some media is being used even after downloads. so data is being accessed in unknown patterns. Way to go is Intelligent tier.

upvoted 4 times

✉ **God_Is_Love** 1 year, 1 month ago

*I meant even after 30 days (not downloads in above comment)

upvoted 1 times

✉ **JungMun** 1 year, 1 month ago

Selected Answer: D

This is my open. The question ask us maintains millisecond retrieval ability. It means we can't use cold storage (So, A, B is not answer). EFS is expensive and not durable. If we use client cache (Ignore client's volume), we can reduce network costs(actually s3's storage costs is really cheap). It means that we can reduce costs too.

upvoted 1 times

✉ **JungMun** 1 year, 1 month ago

There are lots of wrong types. Please forgive me. English is not familiar with me yet.

upvoted 2 times

✉ **c73bf38** 1 year, 1 month ago

The keyword is millisecond retrieval time, which rules everything out except A.

upvoted 2 times

✉ **klog** 1 year, 1 month ago

Selected Answer: A

bc A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days.

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: A

typico A S3 Intelligent-Tiering

upvoted 2 times

 **jhonivy** 1 year, 2 months ago

D it will reduce the cost on retrieval requests

upvoted 1 times

Question #83

Topic 1

A company uses Amazon S3 to store files and images in a variety of storage classes. The company's S3 costs have increased substantially during the past year.

A solutions architect needs to review data trends for the past 12 months and identify the appropriate storage class for the objects.

Which solution will meet these requirements?

- A. Download AWS Cost and Usage Reports for the last 12 months of S3 usage. Review AWS Trusted Advisor recommendations for cost savings.
- B. Use S3 storage class analysis. Import data trends into an Amazon QuickSight dashboard to analyze storage trends.
- C. Use Amazon S3 Storage Lens. Upgrade the default dashboard to include advanced metrics for storage trends.
- D. Use Access Analyzer for S3. Download the Access Analyzer for S3 report for the last 12 months. Import the .csv file to an Amazon QuickSight dashboard.

Correct Answer: B

Community vote distribution



✉ **zejou1** 1 year ago

Selected Answer: C

Storage class: After you configure a filter, you'll start seeing data analysis based on the filter in the Amazon S3 console in 24 to 48 hours. However, storage class analysis observes the access patterns of a filtered data set for 30 days or longer to gather information for analysis before giving a result

Storage Lens: All S3 Storage Lens metrics are retained for a period of 15 months. However, metrics are only available for queries for a specific duration, which depends on your metrics selection. This duration can't be modified. Free metrics are available for queries for a 14-day period, and advanced metrics are available for queries for a 15-month period.

You have to upgrade regardless to query up to 12 months

upvoted 13 times

✉ **Untamables** 1 year, 2 months ago

Selected Answer: C

Both B and C are good.
I guess AWS wants clients to use S3 Storage Lens... Hence I vote C.

upvoted 7 times

✉ **zozza2023** 1 year, 2 months ago

agree with u gess aws want us to know about Lens

upvoted 3 times

✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: C

C, S3 Storage Lens offers comprehensive visibility into storage usage and activity trends across the AWS Organization, facilitating informed decisions on cost optimization and storage efficiency

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: C

Option C refers to using Amazon S3 Storage Lens, which provides organization-wide visibility into object storage usage and activity trends. By upgrading to include advanced metrics and recommendations, users can access detailed insights that help optimize storage costs across their S3 resources. S3 Storage Lens offers dashboard views and metrics that can directly inform on the appropriate storage class based on actual usage patterns, making it a comprehensive solution for the stated requirements.

upvoted 1 times

✉ **AWSPro1234** 2 months, 2 weeks ago

Amazon S3 Storage Class Analysis:

Amazon S3 provides a Storage Class Analysis tool that helps you analyze access patterns to your S3 objects over time. You can enable it on your S3 bucket to collect data on object access patterns.

upvoted 1 times

✉ **AWSPro1234** 2 months, 2 weeks ago

Answer is B.

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: C

To me here the key sentence is "review data trends for the past 12 months"

A = CUR provides detailed usage data but it is not the best tool for this job

B = S3 storage class analysis provides recommendation for Standard and Standard IA storage classes, but does not provide data trends

C = correct

D = Access Analyzer provides visibility for buckets that are configured to allow access to anyone on the internet or other AWS accounts

upvoted 1 times

✉ **Nicoben** 3 months, 3 weeks ago

Selected Answer: B

B is the right answer, because it suffices a bucket analysis --> <https://docs.aws.amazon.com/AmazonS3/latest/userguide/analyticss-storage-class.html>

C instead is a solution for a more organization-wide analysis of bucket -->
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens.html

upvoted 1 times

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

Selected Answer: C

see AMohanty answer

upvoted 1 times

✉ **Simon523** 6 months, 3 weeks ago

Selected Answer: B

S3 Storage Class Analysis enables you to monitor access patterns across objects to help you decide when to transition data to the right storage class to optimize costs.

upvoted 2 times

✉ **jpa8300** 3 months, 1 week ago

Storage Class is only used for recommendation for Standard to Standard IA

upvoted 1 times

✉ **AMohanty** 7 months ago

C

Storage Class is only used for recommendation for Standard to Standard IA

upvoted 3 times

✉ **uC6rW1aB** 7 months, 1 week ago

Selected Answer: C

Option B: Amazon S3's Storage Class Analysis function is mainly used to analyze the access patterns of objects in S3 buckets so that you can transfer these objects to the most cost-effective storage class. However, this feature does not provide detailed historical data for the past 12 months; it is more about observing current usage patterns and making the best storage class decisions based on those patterns.

If you need detailed storage trends and object status over the past 12 months, option C (using Amazon S3 Storage Lens) may be a better choice. Amazon S3 Storage Lens provides comprehensive storage analysis, including historical trends and advanced metrics, which may be more suitable for analyzing long-term data and storage conditions.

upvoted 2 times

✉ **YodaMaster** 9 months, 1 week ago

I choose C.

B. Storage class analysis only provides recommendations for Standard to Standard IA classes. The company uses a variety of storage classes.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

a hard one ... I guess C, but could be B :/

upvoted 1 times

✉ **Limlimwdwd** 10 months, 1 week ago

Selected Answer: B

By using Amazon S3 analytics Storage Class Analysis you can analyze storage access patterns to help you decide when to transition the right data to the right storage class. This new Amazon S3 analytics feature observes data access patterns to help you determine when to transition less frequently accessed STANDARD storage to the STANDARD_IA (IA, for infrequent access) storage class.

So it meet the qn objective of identify the appropriate storage class for the objects

upvoted 1 times

✉ **leehjworking** 11 months ago

Selected Answer: C

SCAs recommendations are based on the previous 30-90 days. <https://aws.amazon.com/s3/faqs>

upvoted 1 times

 **Maria2023** 11 months, 2 weeks ago

The question asks for analysis 12 months back. Reading the documentation storage class analysis works from the action onwards. Same with advanced metrics for lens. Or this is not a real question or the only option remains A...

upvoted 4 times

Question #84

Topic 1

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: C

The correct answer is C. Use AWS Organizations and AWS CloudFormation StackSets.

AWS Organizations allows the management of multiple AWS accounts as a single entity and AWS CloudFormation StackSets allows creating, updating, and deleting stacks across multiple accounts and regions in an organization. This solution allows creating a single CloudFormation template that can be deployed across multiple accounts and regions, and also allows for the management of access and permissions for the different accounts through the use of IAM roles and policies in the management account.

upvoted 14 times

 **masetromain** 1 year, 2 months ago

Option A and D both use AWS CloudFormation, but do not take into account the management of multiple accounts and regions. Option B uses AWS Organizations but doesn't include the use of CloudFormation StackSets, which is necessary for managing deployments across multiple accounts and regions.

upvoted 4 times

 **jpa8300** 3 months, 1 week ago

I agree with what you say here, C is a good choice, but in B they mention Control Tower which is also used to manage multiple accounts, couldn't it be a correct answer also?

upvoted 1 times

 **ninomfr64**  2 months, 3 weeks ago

Selected Answer: C

A = cloud work but it is hard

B = Control Tower cannot manage stack deployments across accounts

C = correct

D = nested stack allows to provision resources by using different CloudFormation templates

upvoted 2 times

 **totten** 6 months, 1 week ago

Selected Answer: C

Option C is the most suitable. Here's why:

AWS Organizations: AWS Organizations helps you centrally manage multiple AWS accounts, which is especially useful when dealing with multiple Regions and accounts. You can organize your accounts into an organizational structure, apply policies across accounts, and manage billing.

AWS CloudFormation StackSets: StackSets is a CloudFormation feature that enables you to deploy CloudFormation stacks across multiple accounts and Regions with a single CloudFormation template. This simplifies the process of deploying and managing infrastructure consistently across your organization.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C no doubt

upvoted 2 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: C

keywords = AWS Organizations && AWS CloudFormation StackSets.

upvoted 1 times

 **rbm2023** 11 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-organization/>
Cloud Formation Stack Sets allow you to roll out Cloud Formation stacks over multiple AWS accounts and in multiple Regions with just a couple of clicks. When we launched Stack Sets, grouping accounts was primarily for billing purposes. Since the launch of AWS Organizations, you can centrally manage multiple AWS accounts across diverse business needs including billing, access control, compliance, security, and resource sharing.

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: C

Use AWS Organizations and AWS CloudFormation StackSets

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: C

The correct answer is C

upvoted 4 times

Question #85

Topic 1

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts, Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a Cloud Formation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

Correct Answer: C

Community vote distribution

C (100%)

-  **masetromain** Highly Voted 1 year, 2 months ago
same question of "Questions #84"
upvoted 15 times
-  **yorkicurke** Most Recent 5 months, 1 week ago
These Site Moderators getting lazy boy!
upvoted 2 times
-  **NikkyDicky** 9 months, 1 week ago
Selected Answer: C
C. a dup question
upvoted 2 times
-  **rbm2023** 11 months, 1 week ago
Selected Answer: C
This question is duplicated in the Exam Topics site. Question 85 is the same as Question 84
upvoted 1 times
-  **bordy20** 11 months, 1 week ago
C:
<https://sanderknape.com/2017/07/cloudformation-stacksets-automated-cross-account-region-deployments/#:~:text=A%20StackSet%20is%20a%20set,deploying%20to%20multiple%20accounts%2Fregions.>
upvoted 1 times
-  **Nguyen25183** 1 year ago
Thought that my internet was interrupted. then i was wrong =)))
upvoted 3 times
-  **Musk** 1 year, 2 months ago
This is repeated :-(
upvoted 2 times
-  **tatdatpham** 1 year, 2 months ago
Selected Answer: C
Duplicate question with #84
upvoted 3 times
-  **zhangyu20000** 1 year, 2 months ago
C is correct answer
upvoted 3 times

Question #86

Topic 1

A company plans to refactor a monolithic application into a modern application design deployed on AWS. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements:

- It should allow changes to be released several times every hour.
- It should be able to roll back the changes as quickly as possible.

Which design will meet these requirements?

- Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.
- Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application. To deploy, swap the staging and production environment URLs.
- Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment.
- Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

Correct Answer: B

Community vote distribution

B (100%)

 **masetromain** Highly Voted  1 year, 2 months ago

Selected Answer: B

The correct answer is B. Specifying AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application and swapping the staging and production environment URLs. This approach allows the company to deploy updates several times an hour and quickly roll back changes as needed.

Option A, Deploying a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances, while it may provide a way to roll back changes by replacing instances with previous versions, it may not allow for rapid deployment of updates multiple times per hour.

upvoted 14 times

 **masetromain** 1 year, 2 months ago

Option C, Using AWS Systems Manager to re-provision the infrastructure for each deployment. Updating the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and using Amazon Route 53 weighted routing to point to the new environment, would require more time-consuming steps and may not be able to roll back changes as quickly.

Option D, Rolling out the application updates as part of an Auto Scaling event using prebuilt AMIs. Using new versions of the AMIs to add instances and phasing out all instances that use the previous AMI version with the configured termination policy during a deployment event, while it may be a way to roll back changes, it doesn't allow for rapid deployment of updates multiple times per hour.

upvoted 4 times

 **jpa8300** 3 months, 1 week ago

Good explanation, but concerning option C it is not quite right, you say that 'may not be able to roll back changes as quickly.', but since it is using Route 53 weighted configuration, in case of failure of the new instances, you just need to change again the weighted configuration to point 100% to the old instances while you replace again the new instances by old instances.

upvoted 1 times

 **ninomfr64** Most Recent  2 months, 3 weeks ago

Selected Answer: B

A = replacing existing EC2 instances does not allow for roll back the changes as quickly as possible

B = correct (tough Beanstalk is not the best service for releasing several times every hour)

C = could work, but here you are combining SSM and user data to achieve what beanstalk does natively

D = this would not work as you need to build AMIs (AMI Builder not mentioned) and also rapid rollback is better achieved avoiding termination of old AMI version

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

probably B

upvoted 1 times

 **rbm2023** 11 months, 1 week ago

Selected Answer: B

Imagine the cost for replacing AMIs and EC2 or re-provision infrastructure several times per day. Although cost effectiveness is not part the requirement in the question. the only option that seems correct is B.

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

B. Specify AWS Elastic Beanstalk

upvoted 1 times

 **Untamables** 1 year, 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 3 times

Question #87

Topic 1

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB Cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB Cluster.

Which combination of steps will meet these requirements? (Choose two.)

- A. Add an inbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the source over the default Aurora port.
- B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port.
- C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port.
- D. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the default Aurora port.
- E. Add an outbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the destination over the ephemeral ports.

Correct Answer: AB

Community vote distribution

BC (76%) AC (24%)

 **masetromain**  1 year, 2 months ago

Selected Answer: BC

The correct combination of steps to meet these requirements is B and C.

B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port. This allows the instances to make outbound connections to the DB cluster on the default Aurora port.

C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port. This allows connections to the DB cluster from the EC2 instances on the default Aurora port.

upvoted 26 times

 **masetromain** 1 year, 2 months ago

A. Adding an inbound rule to the EC2 instances' security group would allow incoming connections to the instances on the default Aurora port, but it would not allow the instances to connect to the DB cluster.

D. Adding an outbound rule to the DB cluster's security group would allow the DB cluster to make outbound connections to the EC2 instances on the default Aurora port, but it would not allow connections to the DB cluster from the instances.

E. Adding an outbound rule to the DB cluster's security group specifying the EC2 instances' security group as the destination over the ephemeral ports would allow the DB cluster to make outbound connections to the instances on ephemeral ports, but it would not allow connections to the DB cluster from the instances on the default Aurora port.

upvoted 3 times

 **vjp_training** 6 months, 3 weeks ago

Security group is stateful. So you just need to set up inbound

upvoted 2 times

 **HussamShokr** 9 months, 3 weeks ago

why we should add an outbound rule to the EC2 instances' security group??? it is already allowed by default in the EC2 security group because all outbound ports are allowed by default.

upvoted 3 times

 **jainparag1** 4 months, 2 weeks ago

wow..then in that case your EC2 instance can talk to anything. No SG rule is required. You need to establish a connectivity route first.

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

it is the other way around, all connection are denied and you can only allow connection. You need outbound from EC2 to Aurora to allow the app initiate a connection to the database instance

upvoted 1 times

 **c73bf38**  1 year, 1 month ago

Selected Answer: AC

To provide the application with least privilege access to the Aurora DB cluster, the solutions architect should add inbound rules to both the security groups.

For the EC2 instances' security group, an inbound rule should be added that allows traffic from the DB cluster's security group over the default Aurora port. This will allow the EC2 instances to communicate with the Aurora DB cluster.

For the Aurora DB cluster's security group, an inbound rule should be added that allows traffic from the EC2 instances' security group over the default Aurora port. This will allow the Aurora DB cluster to communicate with the EC2 instances.

By default all outbound rules are open, it's only the ingress that needs to allow traffic.

upvoted 12 times

 **c73bf38** 1 year, 1 month ago

B&C after doing a recreate in the AWS Console, stand corrected.

upvoted 6 times

 **c73bf38** 1 year, 1 month ago

To provide the application with least privilege access to the Amazon Aurora DB Cluster, the solutions architect should take the following steps:

Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port (port 3306). This will allow the EC2 instances to connect to the Aurora DB Cluster.

Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port (port 3306). This will allow the EC2 instances to send traffic to the Aurora DB Cluster.

upvoted 3 times

 **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: BC

BC, ec2 -> bd; ec2 outbound rule to allow access to bd; db inbound rule to allow access from ec2

upvoted 1 times

 **igor12ghsj577** 2 months ago

Selected Answer: BC

Tricky question. They say with least privileges, so I think they don't want to use default (allow-all) rule, but limit as much as possible and allow only specific traffic to DB)

"By default, a security group includes an outbound rule that allows all outbound traffic. We recommend that you remove this default rule and add outbound rules that allow specific outbound traffic only."

<https://docs.aws.amazon.com/quicksight/latest/user/vpc-security-groups.html>

upvoted 2 times

 **cox1960** 2 months, 3 weeks ago

CE

- A and B are nonsense, since they talk about aurora port on ec2 SGs. In SG you always put rules on the local ports.
- C obvious
- E over D, always ephemeral on outbound, but at the condition we replace the existing all open rule

upvoted 1 times

 **jpa8300** 3 months, 1 week ago

Selected Answer: BC

I believe that C is enough, we don't need to define the outbound from EC2 to DB, but since we have to choose two, the only other option that is correct is B. And someone say below that have tested this configuration, so I hope he tested defining only what is mentioned in C, to see if it is enough or not. It would be nice.

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

Selected Answer: BC

Answer - B& C

Outbound rule to the EC2 SG with DB SG as destination

Inbound rule to the DB SG with EC2 SG as source

upvoted 1 times

 **eurriola10** 4 months, 1 week ago

Selected Answer: AC

Security Groups are stateful, that means you don't need to specify an outbound rule if you have an inbound rule that permit access to the resource. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html#security-group-basics>

In other hand, the outbound traffic rules typically don't apply to DB clusters. Outbound traffic rules apply only if the DB cluster acts as a client. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.RDSSecurityGroups.html#Overview.RDSSecurityGroups.VPCSec>

Because of that B, D and E are wrong answers

upvoted 1 times

 **uC6rW1aB** 7 months, 1 week ago

Selected Answer: AC

By default, AWS Security Groups allow all outbound traffic. Therefore, in most cases, there's no need to configure outbound rules unless you have specific security requirements.

Add an inbound rule to the EC2 instance's security group, setting the DB cluster's security group as the source over Aurora's default port. This enables interaction between the DB Cluster and the EC2 instances. Corresponds to Option A.

Add an inbound rule to the DB Cluster's security group, setting the EC2 instance's security group as the source over Aurora's default port. This allows the EC2 instances to interact with the DB Cluster. Corresponds to Option C.

upvoted 2 times

 **uC6rW1aB** 7 months, 1 week ago

By the way, the outbound rules are unnecessary in this case because the database cluster does not need to access any data from the application. The database cluster only needs to receive traffic from the application so that the application can read and write to the database.

upvoted 1 times

 **eurriola10** 4 months, 1 week ago

my two cents.

Agree AC are the correct answer.

Security Groups are stateful, that means you don't need to specify an outbound rule if you have an inbound rule that permit access to the resource. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html#security-group-basics>

In other hand, the outbound traffic rules typically don't apply to DB clusters. Outbound traffic rules apply only if the DB cluster acts as a client. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.RDSSecurityGroups.html#Overview.RDSSecurityGroups.VPCs_ec

upvoted 1 times

 **vjp_training** 7 months, 2 weeks ago

Selected Answer: AC

By default, all outbound rules are allow

upvoted 1 times

 **vn_thanh tung** 7 months, 1 week ago

Don't provide wrong answer. Answer is B,C

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

you are providing the wrong answer. The correct answer is AC. Inbound rules are supposed to be added.

upvoted 1 times

 **vn_thanh tung** 7 months, 1 week ago

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB Cluster.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: BC

BC of course

upvoted 2 times

 **jainparag1** 4 months, 2 weeks ago

AC is correct.

upvoted 1 times

 **bcx** 9 months, 3 weeks ago

Selected Answer: BC

It is outbound from the clients to the db server listening port. And inbound to the db server listening ports from the clients.

upvoted 2 times

 **Jonalb** 10 months, 2 weeks ago

Selected Answer: BC

"My choice relies on the fact that the security groups are stateful, so we only need to allow the outbound traffic for the ec2 instances to pass and the return will also be allowed. Same for the RDS. This combination is also based on the standard traffic flow initiated from instance to DB"

upvoted 1 times

 **Maria2023** 11 months, 2 weeks ago

Selected Answer: BC

My choice relies on the fact that the security groups are stateful, so we only need to allow the outbound traffic for the ec2 instances to pass and the return will also be allowed. Same for the RDS. This combination is also based on the standard traffic flow initiated from instance to DB.

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: BC

BC gets my vote

upvoted 2 times

 **zejou1** 1 year ago

Selected Answer: BC

Look at the traffic - from the instances EC2 -> DB Cluster I need to go to it as the destination and port (outbound, nothing more or less); so that DB responses needs to see my Security group (since they are shared) coming inbound on that port; any other port deny.

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/working-with-security-groups.html>

upvoted 3 times

 **Gabehcoud** 1 year, 1 month ago

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/security-group-rules.html>

By default, security groups contain outbound rules that allow all outbound traffic. So why do we even need a outbound rule? Guys common. lets not confuse each other.

upvoted 5 times

 **Sarutobi** 1 year, 1 month ago

That is a really good point, keep in mind that is when you create a security group using the GUI/Console when you use API the SG outbound does not have that allow-all. But again this is not part of the question. If we add that outbound rule, should we need to add others like DNS???

upvoted 1 times

 **zejou1** 1 year ago

"You can delete these rules..."

Practice Security Best Practices - although default why are you leaving all outbound traffic open?

Besides, to go w/ least privilege access would delete the outbound all rule and only allow outbound to DB cluster.

upvoted 3 times

Question #88

Topic 1

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold.

Which solution is the MOST cost-effective way to meet these requirements?

- A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in each account to create monthly reports for each business unit.
- B. Configure AWS Budgets in the organization's management account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's management account to create monthly reports for each business unit.
- C. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- D. Enable AWS Cost and Usage Reports in the organization's management account and configure reports grouped by application, environment, and owner. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

Correct Answer: B

Community vote distribution

B (100%)

✉  **masetromain**  1 year, 2 months ago

Selected Answer: B

B. Configure AWS Budgets in the organization's management account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's management account to create monthly reports for each business unit.

This option is the most cost-effective because it utilizes the organization's management account to set budgets and configure alerts for all accounts in the organization, rather than having to configure budgets and alerts individually in each account. Additionally, using Cost Explorer in the management account allows the cloud governance team to view the consolidated spending for all accounts in the organization and create reports for each business unit. This eliminates the need to access each individual account to view costs and create reports.

upvoted 23 times

✉  **masetromain** 1 year, 2 months ago

Option A is not the most cost-effective solution because it requires configuring budgets and reports in multiple accounts, which increases the complexity and cost of managing the cloud spending for each business unit.

Option C is not the most cost-effective solution because it requires the cloud governance team to access the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit, which increases the complexity and cost of managing the cloud spending for each business unit.

Option D is not the most cost-effective solution because it requires creating an AWS Lambda function to process AWS Cost and Usage Reports, which increases the complexity and cost of managing the cloud spending for each business unit.

upvoted 3 times

✉  **NikkDicky**  9 months, 1 week ago

Selected Answer: B

B for sure

upvoted 1 times

✉  **Maria2023** 9 months, 3 weeks ago

"configure budget alerts that are grouped by application, environment, and owner" - I just literally tried to create a budget alert and I am not able to see any option for grouping by tags. Another nonsense question

upvoted 2 times

✉  **b3llman** 8 months ago

Billing > Budgets > Create budget > Customize (advanced) > Budget scope > Filter specific AWS cost dimensions

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword = AWS Budgets in the organization's management
other more overhead each by account

upvoted 1 times

 **yama234** 11 months, 4 weeks ago

B
centralized solution = management account
send notifications for any cloud spending that exceeds a set threshold = AWS Budgets
<https://aws.amazon.com/blogs/mt/manage-cost-overruns-part-1/>

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: B
B. Configure AWS Budgets in the organization's management account

upvoted 1 times

Question #89

Topic 1

A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted.

How can the company prevent users from accidentally deleting data in this way?

- A. Modify the CloudFormation templates to add a `DeletionPolicy` attribute to RDS and EBS resources.
- B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
- C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.
- D. Use AWS Config rules to prevent deleting RDS and EBS resources.

Correct Answer: A

Community vote distribution

A (85%) B (15%)

✉  **zejou1**  1 year ago

Selected Answer: A

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

With the `DeletionPolicy` attribute you can preserve, and in some cases, backup a resource when its stack is deleted. You specify a `DeletionPolicy` attribute for each resource that you want to control. If a resource has no `DeletionPolicy` attribute, AWS CloudFormation deletes the resource by default.

Retain

CloudFormation keeps the resource without deleting the resource or its contents when its stack is deleted. You can add this deletion policy to any resource type. When CloudFormation completes the stack deletion, the stack will be in `Delete_Complete` state; however, resources that are retained continue to exist and continue to incur applicable charges until you delete those resources.

upvoted 15 times

✉  **8608f25**  1 month, 3 weeks ago

Selected Answer: A

Option A is the correct approach because CloudFormation allows you to specify a `DeletionPolicy` attribute for resources within your templates. This attribute can prevent resources like Amazon RDS databases and Amazon EBS volumes from being deleted when the stack is deleted. You can set the `DeletionPolicy` to "Retain" for specific resources, ensuring they are not automatically removed alongside the stack.

upvoted 1 times

✉  **Maygam** 3 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html>

upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A, basic `DeletionPolicy` use case

upvoted 2 times

✉  **aviathor** 7 months, 1 week ago

Yes but should be supplemented with deletion protection on the database.

upvoted 2 times

✉  **Maria2023** 9 months, 3 weeks ago

Selected Answer: A

Although that I would preferably use both A and B - this is an exam and the truth is in the wording - "important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted" - we don't care if the resources are deleted but the data, which makes me believe they want us to set up a deletion policy at a resource level to "Retain"

upvoted 2 times

✉  **zak340** 10 months, 1 week ago

Selected Answer: B

Explanation:

Stack policies are a powerful feature of AWS CloudFormation that allows you to control fine-grained permissions for resources within a stack. By configuring a stack policy that disallows the deletion of RDS and EBS resources, you can prevent users from accidentally deleting these critical resources and the associated data.

Option A (Modifying CloudFormation templates with `DeletionPolicy` attribute) is not the best solution in this case. While the `DeletionPolicy` attribute can be used to control resource behavior during stack deletion, it is not applicable to Amazon RDS instances or Amazon EBS volumes.

upvoted 2 times

✉ **bcx** 9 months, 3 weeks ago

The correct answer is A, not because what you say is wrong, but because the question states that the stacks can be deleted, you cannot prevent the deletion of the stack (as required by the question). So the `DeletionPolicy` will let you delete the stack and retain or take a snapshot of the Database/BUCKET/... (whichever is applicable). You will not lose any data in that case and the stack would have been successfully deleted.

upvoted 3 times

✉ **rbm2023** 11 months ago

Selected Answer: A

Check the differences and use cases where to use a stack policy or add a deletion policy (retain):

Stack policy and deletion policy are both ways to protect resources created by CloudFormation stacks, but they have different functions.

Stack policy is a feature that allows you to specify a JSON policy document that restricts what actions can be taken on a CloudFormation stack. Stack policies are used to prevent accidental or intentional updates or deletions of critical resources in your stack, by specifying which resources can be modified and by whom. Stack policies can be used to allow specific teams or individuals to modify specific resources in a stack while preventing them from modifying others.

upvoted 3 times

✉ **rbm2023** 11 months ago

Deletion policy, on the other hand, is a property of certain AWS resources that determines what happens to the resource when the stack is deleted. The deletion policy can be set to one of three values: "Delete", "Retain", or "Snapshot". When the deletion policy is set to "Delete", the resource is deleted when the stack is deleted. When the deletion policy is set to "Retain", the resource is not deleted when the stack is deleted, but must be deleted manually. When the deletion policy is set to "Snapshot", the resource is deleted when the stack is deleted, but a snapshot of the resource is retained.

In summary, stack policies are used to control what changes can be made to a stack, while deletion policies are used to determine what happens to resources when a stack is deleted.

upvoted 1 times

✉ **OCHT** 11 months, 3 weeks ago

Selected Answer: B

ption B, which suggests configuring a stack policy that disallows the deletion of RDS and EBS resources, is better in this scenario. While using `DeletionPolicy` attribute (Option A) can be helpful for preserving and backing up the resource, it does not address the problem of accidental deletion of resources or control access to delete the resource.

On the other hand, a Stack Policy can be used to prevent accidental deletion of resources by specifying which actions can be performed on the resources within in the stack, thereby adding an essential layer of protection.

By implementing a Stack Policy, a company can limit updating the resources in the stack, control who can make changes to the stack, and prevent accidental deletion of resources. Therefore, configuring a Stack Policy is necessary and more satisfactory to protect data from accidental deletion while using AWS CloudFormation.

upvoted 1 times

✉ **Sarutobi** 11 months, 3 weeks ago

You are correct about the process of the UPDATE stack action. What happens to the resources created by the CloudFormation stack when the stack itself is deleted?

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

A for sure

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: B

A stack policy is a document that defines the update and deletion actions that can be performed on resources in a CloudFormation stack. By default, all resources in a CloudFormation stack can be deleted by users with appropriate permissions. However, you can use a stack policy to restrict the deletion of certain resources, such as Amazon RDS databases or Amazon EBS volumes.

In this case, the company can create a stack policy that explicitly disallows the deletion of any RDS or EBS resources in the production CloudFormation stack. This will prevent users from accidentally deleting important data stored in these resources.

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

For RDS instances, you can set the `DeletionPolicy` attribute to "Retain". This will ensure that when the stack is deleted, the RDS instance will not be deleted and its data will be retained.

For EBS volumes, you can use the `DeletionPolicy` attribute in combination with the `SnapshotId` attribute to create a snapshot of the volume before deleting it. This will allow you to restore the data later if need

Yaml examples for RDS and EBS :

Resources:

MyDB:

Type: AWS::RDS::DBInstance

Properties:

RDS instance properties go here
DeletionPolicy: Retain

Resources:
MyVolume:
Type: AWS::EC2::Volume
Properties:
Volume properties go here
DeletionPolicy: Snapshot
SnapshotId: my-snapshot-id
upvoted 1 times

✉ **spd** 1 year, 1 month ago

Selected Answer: A

Clear A

upvoted 1 times

✉ **lunt** 1 year, 1 month ago

Selected Answer: A

AC1984 do your homework.

Stack policy can protect against deletion but not against actual entire CFN stack template being deleted. DeletionPolicy = if I was to delete the entire CFN stack, the CFN process will delete all elements and skip over RDS and EBS due to protections. 20 second Google search could of confirmed this.

upvoted 2 times

✉ **AC1984** 1 year, 1 month ago

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html>

upvoted 1 times

✉ **AC1984** 1 year, 1 month ago

Selected Answer: B

B. Configure a stack policy that disallows the deletion of RDS and EBS resources.

A stack policy is a JSON-based document that defines the actions that can be performed on a CloudFormation stack, and can be used to prevent users from accidentally deleting critical resources. By configuring a stack policy that disallows the deletion of RDS and EBS resources, the company can prevent users from accidentally deleting important data stored in those resources.

Option A (adding a DeletionPolicy attribute) does not prevent users from deleting the resources, but rather determines what happens to the resources when the stack is deleted. Option C (modifying IAM policies) is not sufficient because it only affects the permissions of specific users or groups, and does not prevent accidental deletions. Option D (using AWS Config rules) can help detect deletions of RDS and EBS resources, but it does not prevent them from being deleted.

upvoted 1 times

✉ **sambb** 1 year, 1 month ago

"Option A (adding a DeletionPolicy attribute) does not prevent users from deleting the resources, but rather determines what happens to the resources when the stack is deleted." This is actually what the question is asking !

upvoted 1 times

✉ **moota** 1 year, 1 month ago

Selected Answer: A

I go for A because I assume that the CF stack is allowed to be deleted in some deployment scenarios.

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: A

Option A

upvoted 1 times

Question #90

Topic 1

A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.

A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.

Which set of steps should the solutions architect take to meet these requirements?

- A. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- B. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- C. Open the AWS CloudTrail console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- D. Open the Amazon CloudWatch console. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

Correct Answer: D

Community vote distribution

B (63%)

D (37%)

 **vsk12**  1 year, 2 months ago

I would go with option B. Source will be public IP like 198.51.100.2.
upvoted 18 times

 **kiran15789**  1 year, 1 month ago

Selected Answer: B
<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway/>

Refer Reason 1

Run the query below.

```
filter (dstAddr like 'xxx.xxx' and srcAddr like 'public IP')
| stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
| limit 10
```

Note: You can use just the first two octets in the search filter to analyze all network interfaces in the VPC. In the example above, replace xxx.xxx with the first two octets of your VPC classless inter-domain routing (CIDR). Also, replace public IP with the public IP that you're seeing in the VPC flow log entry.

Query results show traffic on the NAT gateway private IP from the public IP, but not traffic on other private IPs in the VPC. These results confirm that the incoming traffic was unsolicited. However, if you do see traffic on the private instance's IP, then follow the steps under Reason #2.

upvoted 15 times

 **zejou1** 1 year ago

For those that are choosing D - this is why D is incorrect and needs to be B
upvoted 2 times

 **Vongolatt**  2 days, 17 hours ago

Selected Answer: D
the solution architect want to check if it's unsolicited traffic or not, so we need to check the if the request is sent by us. which means 198.51.100.2 should be the destination.
upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: B
B, CloudWatch & destination address 203.0
upvoted 1 times

 **ajeeshb** 4 weeks, 1 day ago

Selected Answer: D

The question is "Solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet". The NAT gateway does not allow any inbound traffic from an internet other than response to a traffic it sent out to internet which came from a VPC resource (eg, EC2). So to find out if the inbound traffic to NAT Gateway from internet IP 198.51.100.2 is unsolicited or not, check the VPC flowlog to see if there was an original request from source IP 203.0 to destination 198.51.100.2. This is what option D says.

upvoted 2 times

 **8608f25** 1 month, 3 weeks ago

Selected Answer: B

Option B is correct because VPC flow logs are stored in Amazon CloudWatch Logs. Analyzing these logs in CloudWatch allows you to filter and examine specific traffic patterns, such as traffic coming from a public IP address to a private instance. The query specified in this option correctly aims to identify traffic from the public IP (198.51.100.2) to the private IP range of the VPC (beginning with 203.0), which aligns with the requirement to investigate unsolicited inbound connections.

upvoted 1 times

 **master9** 2 months, 2 weeks ago

Selected Answer: D

Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 --> Destination

upvoted 2 times

 **cox1960** 2 months, 3 weeks ago

B is what "the company is seeing", so D to see if it was first initiated from EC2.

upvoted 4 times

 **bjexamprep** 4 months, 1 week ago

I would say this question is wrong, even we ignore the 203.0 is a public IP.

Both B and D can do the job.

With B: if the return value is bigger than 0, that means the traffic was initiated from internal so that NAT GW wouldn't drop that traffic. While, if the return is 0, that means the traffic was dropped by NAT after ACCEPTed, which means it was not initiated from internal.

With D: if the return value is bigger than 0, obviously the traffic was initiated from internal. If the return value is 0, that means the traffic was initiated from internet.

upvoted 2 times

 **ninomfr64** 2 months, 3 weeks ago

You need first to query traffic from public IP to private IP, check if the NAT Gateway is the only private IP. If not then you query traffic (from private IP to public IP) OR (from public IP to private IP) and this will show bi-directional traffic allowing you to determine whether the private instance or external public IP address is the initiator. Thus B and not D

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: B

see kiran15789's answer

upvoted 2 times

 **AMohanty** 7 months ago

D

At NAT GW VPC flow logs will destination be VPC Private IP or will it be NAT GW IP

upvoted 1 times

 **study_aws1** 8 months, 1 week ago

I was inclined towards Reason #2 in <https://repost.aws/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway>.

However, the striking point is the VPC CIDR 203.0.... which is not a private addressing and not sure if we require a NAT gateway here at all for translation & check if the traffic was initiated through NAT gateway. Does the definition of unsolicited connection means any inbound connection other than the traffic initiated from VPC via NAT gateway will not be considered as solicited.

Tough one from the unclear definition in the question, it would be Reason 1 (Option B) if the traffic is mentioned as dropped in the question but needs to be analyzed for whether this is unsolicited.

Or if question states inbound traffic is not permitted, but still it is seen and needs to be analyzed then D). Again, point to be noted is why outbound traffic from '203.0...' needs to go via NAT gateway.

upvoted 1 times

 **ggrodsckiy** 8 months, 1 week ago

Correct D.

You need to open the Amazon CloudWatch console, select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface, run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0", and run the stats command to filter the sum of bytes transferred by the source address and the destination address.

upvoted 2 times

 **Jonalb** 9 months ago

Selected Answer: B

bbbbbbbbb

upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

D. see filter expression in <https://repost.aws/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway>, reason #2
upvoted 3 times

✉  **hexie** 9 months, 1 week ago

Selected Answer: B

B.
No clue of why you guys that voted D are convinced. Destination will be your VPC octets, source is the IP that is making the requests.
upvoted 5 times

✉  **swadeey** 4 months, 1 week ago

But isn't Nat gateway to stop incoming traffic and allow ec2 to reach outside. One was external traffic. So when we filter from AWS prespectivr source is our machine and destination is outside as that is functioning of NAT Gateway
upvoted 1 times

✉  **hogtrough** 1 month, 3 weeks ago

NAT Gateway does not stop incoming traffic, it simply allows to reach outside. Regardless, NAT Gateway is irrelevant to the answer of which is the source IP and which is the destination IP. "Inbound traffic from" by itself suggests that it's the source IP.
upvoted 1 times

✉  **hogtrough** 1 month, 3 weeks ago

I should clarify that NAT Gateway is considered egress only so while it technically prevents incoming traffic it's only use is for outbound traffic.
upvoted 1 times

✉  **Maria2023** 9 months, 3 weeks ago

I have the feeling that this question is missing the "Choose 2" option. Ideally, I would run both queries (B and D) to see if the outbound matches the inbound

upvoted 5 times

Question #91

Topic 1

A company consists of two separate business units. Each business unit has its own AWS account within a single organization in AWS Organizations. The business units regularly share sensitive documents with each other. To facilitate sharing, the company created an Amazon S3 bucket in each account and configured low-way replication between the S3 buckets. The S3 buckets have millions of objects.

Recently, a security audit identified that neither S3 bucket has encryption at rest enabled. Company policy requires that all documents must be stored with encryption at rest. The company wants to implement server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

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

- A. Turn on SSE-S3 on both S3 buckets. Use S3 Batch Operations to copy and encrypt the objects in the same location.
- B. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- C. Turn on SSE-S3 on both S3 buckets. Encrypt the existing objects by using an S3 copy command in the AWS CLI.
- D. Create an AWS Key Management Service (AWS KMS) key in each account. Turn on server-side encryption with AWS KMS keys (SSE-KMS) on each S3 bucket by using the corresponding KMS key in that AWS account. Use S3 Batch Operations to copy the objects into the same location.

Correct Answer: C

Community vote distribution



✉ **testingaws123** Highly Voted 1 year ago

Selected Answer: A

Answer is A

Keyword is "The S3 buckets have millions of objects"

If there are million of objects then you should use Batch operations.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 22 times

✉ **forceli** 1 year ago

good point, changing my answer to A

upvoted 1 times

✉ **ajeeshb** Most Recent 4 weeks, 1 day ago

I understand S3 Batch operations is required. But why no one is choosing SSE-KMS?

upvoted 1 times

✉ **StevePace** 3 weeks, 2 days ago

Because the question states the company wants to use SSE-S3, nowhere does it mention SSE-KMS

upvoted 1 times

✉ **TonytheTiger** 1 month ago

To encrypt your existing unencrypted Amazon S3 objects, you can use Amazon S3 Batch Operations. You provide S3 Batch Operations with a list of objects to operate on, and Batch Operations calls the respective API to perform the specified operation. You can use the Batch Operations Copy operation to copy existing unencrypted objects and write them back to the same bucket as encrypted objects. A single Batch Operations job can perform the specified operation on billions of objects. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html>

upvoted 2 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: A

A = correct (see <https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>)

B = KMS is for SSE-KMS not for the requested SSE-S3

C = CLI is less efficient than S3 Batch

D = see answer B

upvoted 2 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: A

A is the right answer

upvoted 1 times

 **jainparag1** 4 months, 2 weeks ago

Selected Answer: A

Correct answer should be A. But this question seem too old to be true now since SSE-S3 based encryption is by default enabled and can't be disabled (you can change however) since Jan 2023.

upvoted 3 times

 **covabix879** 6 months, 1 week ago

Selected Answer: D

Since SSE-S3 does not support cross-account replication, answer should be D

upvoted 1 times

 **deivid83** 6 months, 4 weeks ago

In a cross-account scenario, where the source and destination buckets are owned by different AWS accounts, you can use a KMS key to encrypt object replicas. However, the KMS key owner must grant the source bucket owner permission to use the KMS key.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html#replication-kms-cross-acct-scenario>

S3 Batch operation:

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 3 times

 **uC6rW1aB** 7 months, 1 week ago

Selected Answer: A

S3 Batch operation is the MOST operationally efficient way for millions objects

upvoted 1 times

 **sachstarinfoaws** 8 months, 4 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A more efficient

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: A

I vote for A. Batch operations is better for such a high number of objects

upvoted 1 times

 **rbm2023** 11 months ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

The launch of S3 default encryption feature automate the work of encrypting new objects, and you asked for similar, straightforward ways to encrypt existing objects in your buckets. While tools and scripts exist to do this work, each one requires some development work to set up. S3 batch operations gives you a solution for encrypting large number of archived files.

This can also be done by CLI, Option C, however, the same article refers to Batch Operations in case you have a large bucket with millions of objects.

<https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/>

Option A should be the most efficient, even though it has more operational cost to implement but the question is the about efficiency, it would take to much time to complete this using CLI (Option C).

upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: A

A is much more efficient

upvoted 1 times

 **forceli** 1 year, 1 month ago

Selected Answer: C

A and C seems to be correct but using batch requires more steps.

<https://aws.amazon.com/blogs/storage/encrypting-existing-amazon-s3-objects-with-the-aws-cli/>

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

C is wrong. How can S3 copy encrypt ? A is correct. Refer how S3 batch operations are used to encrypt here -

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

upvoted 2 times

 **Sarutobi** 1 year, 1 month ago

I guess A and/or C can be because they are pretty close; after reading everything here, they are a lot of good points.

upvoted 1 times

Question #92

Topic 1

A company is running an application in the AWS Cloud. The application collects and stores a large amount of unstructured data in an Amazon S3 bucket. The S3 bucket contains several terabytes of data and uses the S3 Standard storage class. The data increases in size by several gigabytes every day.

The company needs to query and analyze the data. The company does not access data that is more than 1 year old. However, the company must retain all the data indefinitely for compliance reasons.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Select to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- B. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.
- D. Use Amazon Redshift Spectrum to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Intelligent-Tiering.

Correct Answer: A
Community vote distribution


masetromain Highly Voted 1 year, 2 months ago

Selected Answer: C

The correct answer is C. Use an AWS Glue Data Catalog and Amazon Athena to query the data. Create an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive.

This solution allows you to use Amazon Athena and the AWS Glue Data Catalog to query and analyze the data in an S3 bucket. Amazon Athena is a serverless, interactive query service that allows you to analyze data in S3 using SQL. The AWS Glue Data Catalog is a managed metadata repository that can be used to store and retrieve table definitions for data stored in S3. Together, these services can provide a cost-effective way to query and analyze large amounts of unstructured data. Additionally, by using an S3 Lifecycle policy to transition data that is more than 1 year old to S3 Glacier Deep Archive, you can retain the data indefinitely for compliance reasons while also reducing storage costs.

upvoted 15 times

masetromain 1 year, 2 months ago

The other options are not correct because:

A. Using S3 Select is good for filtering data in S3, but it may not be a suitable solution for querying and analyzing large amounts of data.

B. Amazon Redshift Spectrum can be used to query data stored in S3, but it may not be as cost-effective as using Amazon Athena for querying unstructured data

D. Using Amazon Redshift Spectrum with S3 Intelligent-Tiering could be a good solution, but S3 Intelligent-Tiering is designed to optimize storage costs based on access patterns and it would not be the best solution for compliance reasons as S3 Intelligent-Tiering will move data to other storage classes according to access patterns.

upvoted 7 times

Japanese1 4 months, 1 week ago

This is a nonsense explanation.

In the first place, Redshift cannot handle unstructured data.

upvoted 3 times

dankositze 1 month, 4 weeks ago

Amazon Redshift is designed for structured data. However, Amazon Redshift Spectrum enables you to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required.

upvoted 2 times

Untamables Highly Voted 1 year, 2 months ago

Selected Answer: C

Generally, unstructured data should be converted structured data before querying them. AWS Glue can do that.

<https://docs.aws.amazon.com/glue/latest/dg/schema-relationalize.html>

<https://docs.aws.amazon.com/athena/latest/ug/glue-athena.html>

upvoted 6 times

gofavad926 Most Recent 3 weeks, 2 days ago

Selected Answer: C

C, aws glue + amazon athena
upvoted 1 times

 **AimarLeo** 2 months, 1 week ago

Many comments were not convincing of not using Redshift Spectrum.. the only reason I see it to exclude that option is a Redshift Spectrum MUST have a Redshift Cluster available to start the query to S3..

upvoted 1 times

 **djeong95** 1 month ago

This question is actually pretty difficult since both Redshift Spectrum and AWS Glue + Athena could query unstructured data. Redshift Spectrum and Athena actually cost about the same per TB. However, with Athena, you could lower the cost by compressing the data. Glue doesn't seem to cost that much either.

<https://aws.amazon.com/redshift/pricing/>
<https://aws.amazon.com/athena/pricing/>
<https://aws.amazon.com/glue/pricing/>

upvoted 1 times

 **ninomfr64** 2 months, 3 weeks ago

Selected Answer: C

A = S3 Select good for filtering and retrieve subset of data, not enough to analyze

B = need a Redshift instance that is expensive

C = correct (Glue Data Catalog can help putting some structure to data and Athena is good for both query and analytics, transition to Deep Archive after 1 year)

D = see answer B + Intelligent-Tiering not the best option here

upvoted 1 times

 **nzin4x** 3 months ago

redshift spectrum vs athena: <https://www.upsolver.com/blog/aws-serverless-redshift-spectrum-athena>

Both are good solutions to query s3 data. However, redshift spectrum is useful for joining S3 data with other data in Redshift, and if the data is only in S3, it would be preferable to choose athena.

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: C

C is the right answer as Data needs to be queried and Analyzed.

upvoted 1 times

 **subupro** 4 months ago

Athena and aws glue is more cost , so better go with A . and what is the purpose for aws glue here. AWS glue is for ETL purpose unnecessary upvoted 1 times

 **Andy16240** 4 months, 2 weeks ago

C correct: S3 copy command in AWS CLI is less operational processes than the batch operation.

upvoted 1 times

 **uC6rW1aB** 7 months, 1 week ago

Selected Answer: C

In this particular scenario, using Amazon Athena and AWS Glue Data Catalog might be a better fit due to the large amount of data stored in S3 buckets and growing every day. Athena can query data across an entire S3 bucket or across multiple buckets, which is useful when parsing multiple files and large amounts of data.

upvoted 2 times

 **chico2023** 8 months, 1 week ago

Selected Answer: C

Answer: C

Criminally tricky question. S3 Select does the same thing as Athena but there are some differences. The key here is "...a large amount of unstructured data..."

If wasn't this, S3 Select hands down.

upvoted 3 times

 **chico2023** 8 months, 1 week ago

Using an Olabiba to explain the differences between the two:

1. Query Capability: Amazon Athena is a fully managed interactive query service that allows you to run SQL queries directly on your data in S3. It supports complex queries, joins, aggregations, and even nested data structures. Athena is designed for ad-hoc querying and analysis of large datasets.

On the other hand, S3 Select is a feature of Amazon S3 that allows you to retrieve a subset of data from an object using SQL expressions. It is primarily used for selective retrieval of specific data within an object, rather than running complex queries across multiple objects.

upvoted 2 times

 **chico2023** 8 months, 1 week ago

2. Data Format: Amazon Athena supports various data formats such as CSV, JSON, Parquet, Avro, and more. It can automatically infer the schema of your data or you can provide a schema explicitly. Athena can handle structured, semi-structured, and unstructured data.

S3 Select, on the other hand, is limited to querying CSV, JSON, and Parquet files. It requires the data to be in a specific format and does not support nested data structures.

upvoted 2 times

✉️  **chico2023** 8 months, 1 week ago

3. Performance: Amazon Athena is optimized for running queries on large datasets and can parallelize the query execution across multiple nodes. It automatically scales resources based on the query complexity and data size, providing fast and efficient query performance.

S3 Select, on the other hand, is designed for retrieving a subset of data from an object. It can significantly reduce the amount of data transferred over the network and improve query performance by only retrieving the necessary data.

4. Cost: Both Amazon Athena and S3 Select have different pricing models. Amazon Athena charges based on the amount of data scanned by your queries, while S3 Select charges based on the amount of data selected and returned by your queries. The cost will depend on the size of your data and the complexity of your queries.

upvoted 3 times

✉️  **Jonalb** 9 months ago

Selected Answer: C

its a C , true question!

upvoted 1 times

✉️  **NikkyDicky** 9 months, 1 week ago

C for sure

upvoted 1 times

✉️  **johnballs221** 10 months, 2 weeks ago

Selected Answer: B

redshift spectrum can run sql queries directly on s3

upvoted 1 times

✉️  **rxhan** 9 months, 2 weeks ago

Not the best for cost.

upvoted 1 times

✉️  **mfsec** 1 year ago

Selected Answer: C

C is the best choice for unstructured data

upvoted 3 times

✉️  **God_Is_Love** 1 year, 1 month ago

Selected Answer: C

S3 select only to select few parts of the data and here its lot of unstructured data. So A is wrong. Use Athena console to create Glue crawler as referred here -

<https://docs.aws.amazon.com/athena/latest/ug/data-sources-glue.html>

upvoted 4 times

✉️  **sambb** 1 year, 1 month ago

I think "semi-structured" is the right word here, because unstructured can be videos, images or text that has no schema.

Assuming that we want to query semi-structured data :

I don't understand why everyone is voting Athena.

Athena is fast in certain cases and has more features for aggregation, but we are just asking querying here (and analyzing is very vague).

In terms of cost, S3 select is around 2\$ by TB scanned, and Athena is 5\$.

Glue data catalog brings ease of use, but is not required for querying with athena.

S3 select is not limited in the amount of scanned data, only in the row size (1MB)

Can someone explain ?

upvoted 3 times

Question #93

Topic 1

A video processing company wants to build a machine learning (ML) model by using 600 TB of compressed data that is stored as thousands of files in the company's on-premises network attached storage system. The company does not have the necessary compute resources on premises for ML experiments and wants to use AWS.

The company needs to complete the data transfer to AWS within 3 weeks. The data transfer will be a one-time transfer. The data must be encrypted in transit. The measured upload speed of the company's internet connection is 100 Mbps. and multiple departments share the connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS.
- B. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.
- C. Create a VPN connection between the on-premises network attached storage and the nearest AWS Region. Transfer the data over the VPN connection.
- D. Deploy an AWS Storage Gateway file gateway on premises. Configure the file gateway with a destination S3 bucket. Copy the data to the file gateway.

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

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: A

The correct answer is A. Order several AWS Snowball Edge Storage Optimized devices by using the AWS Management Console. Configure the devices with a destination S3 bucket. Copy the data to the devices. Ship the devices back to AWS.

This option will meet the requirements to complete the data transfer within 3 weeks, as the Snowball Edge devices can transfer large amounts of data quickly and securely. The data will be encrypted in transit and at rest. The company's internet connection speed is not a bottleneck as the data transfer will happen on the devices and not over the internet.

upvoted 10 times

✉️  **masetromain** 1 year, 2 months ago

Option B is not a cost-effective solution, as setting up and maintaining a 10 Gbps Direct Connect connection can be quite expensive, especially if it's only needed for a one-time data transfer.

Option C is not a cost-effective solution, as creating a VPN connection between the on-premises storage and the nearest AWS region would require significant networking configuration and maintenance, and would likely be more expensive than using Snowball Edge devices.

Option D is not a cost-effective solution, as deploying an AWS Storage Gateway file gateway on premises would require additional hardware and ongoing maintenance costs, and may not be necessary for a one-time data transfer.

upvoted 3 times

✉️  **ninomfr64**  2 months, 3 weeks ago

Selected Answer: A

A = correct
B = takes a month or more to setup DX
C = this would take more than 3 weeks for transferring data
D = this would take more than 3 weeks for transferring data

upvoted 1 times

✉️  **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A
upvoted 1 times

✉️  **yorkicurke** 5 months, 1 week ago

Selected Answer: A

wish all the questions were like this. happy days :)
upvoted 1 times

✉️ **xplusfb** 8 months ago

Selected Answer: A

as we know snowball storage optimized NVMe up to 210 TB <3 A is the best and easy answer

upvoted 4 times

✉️ **xplusfb** 8 months ago

like several sorry for any confision :)

upvoted 1 times

✉️ **chikorita** 7 months, 1 week ago

several thanks too :)

upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A - basic snowball use case

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

Selected Answer: A

Given the deadline (3 weeks) and the amount of data I would use Snowball Edge

upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: A

A obviously

upvoted 3 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

Around 8 devices and snowball (actually a Rectangular box)

Snowball Edge Storage Optimized device is equipped with up to 80 terabytes (TB) of storage capacity, as well as 40 vCPUs and 80 GB of memory for running compute-intensive applications. It also includes an optional GPU for accelerated computing workloads.

Built-in security features such as tamper-resistant enclosures, an E Ink shipping label, and 256-bit encryption for data at rest and in transit.

upvoted 4 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: A

3 weeks + cost effective ==> Snowball Edge Storage

upvoted 1 times

Question #94

Topic 1

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

- A. Develop custom libraries to perform optical character recognition (OCR) on the forms. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier. Use this tier to process the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table. Submit the data to the target system's API. Host the new application tier on EC2 instances.
- B. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- C. Host a new application tier on EC2 instances. Use this tier to call endpoints that host artificial intelligence and machine learning (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the forms. Store the output in Amazon ElastiCache. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.
- D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

Correct Answer: D

Community vote distribution

D (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: D

The correct answer is D. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API.

This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead. Amazon Textract and Amazon Comprehend are fully managed and serverless services that can perform OCR and extract relevant data from the forms, which eliminates the need to develop custom libraries or train and host models. Using AWS Step Functions and Lambda allows for easy automation of the process and the ability to scale as needed.

upvoted 12 times

 **masetromain** 1 year, 2 months ago

Option A:

This option would require significant development and maintenance effort and would not take advantage of fully managed services, resulting in increased operational overhead.

Option B:

This option is similar to option A in that it would require significant development and maintenance effort to train and host the models, and would not take advantage of fully managed services resulting in increased operational overhead.

Option C:

This option is similar to option B in that it would require significant development and maintenance effort to train and host the models, and would not take advantage of fully managed services resulting in increased operational overhead.

upvoted 2 times

✉  **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: D

D. This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead
upvoted 1 times

✉  **career360guru** 3 months, 2 weeks ago

Selected Answer: D

Option D
upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

D - basic use case for textract
upvoted 1 times

✉  **Maria2023** 9 months, 3 weeks ago

Selected Answer: D

An easy one - if AWS has a service for something - do not reinvent the wheel - use Textract and Comprehend
upvoted 1 times

✉  **SkyZeroZx** 10 months ago

Selected Answer: D

D : Managed AWS Services
upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: D

Amazon Textract..
upvoted 1 times

✉  **God_Is_Love** 1 year, 1 month ago

Selected Answer: D

Textract can analyze different types of documents such as forms, invoices, receipts, and tables, and can extract information such as text, tables, and key-value pairs.

Comprehend provides a set of APIs that can be used to analyze text data in real-time. The service can identify the language of the text, extract entities such as people, organizations, and locations, and detect the sentiment expressed in the text. It can also extract key phrases that summarize the meaning of the text, and can classify the text into predefined categories.

upvoted 1 times

✉  **sambb** 1 year, 1 month ago

Selected Answer: D

D : Managed AWS Services
upvoted 1 times

Question #95

Topic 1

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs, RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application.

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

- A. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- B. Create a custom AWS Lambda runtime to mimic the web server environment. Create an Amazon API Gateway API to replace the front-end web servers. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- C. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend.
- D. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.

Correct Answer: A

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: A

Option A is the correct answer. In this solution, the company creates an Amazon Machine Image (AMI) of the web server VM, which can be used to launch EC2 instances that are identical to the on-premises web servers. The company then creates an EC2 Auto Scaling group that uses the AMI and an Application Load Balancer (ALB) to provide automatic scaling and high availability for the web front end. The company also replaces the on-premises messaging queue (RabbitMQ) with Amazon MQ, which is a managed message broker service that is fully compatible with RabbitMQ. Finally, the company uses Amazon Elastic Kubernetes Service (EKS) to host the order-processing backend, which allows them to run their existing Kubernetes cluster in the AWS cloud without making any major changes to the application. This approach allows the company to lift and shift their existing platform with minimal operational overhead.

upvoted 18 times

masetromain 1 year, 2 months ago

Option B, using a custom AWS Lambda runtime and Amazon API Gateway, would require significant changes to the application and may not be compatible with the current codebase.

Option C, installing Kubernetes on a fleet of different EC2 instances, would also require significant changes to the application and may not be compatible with the current codebase.

Option D, using Amazon Simple Queue Service (Amazon SQS) instead of Amazon MQ, would not provide the same level of messaging capabilities as Amazon MQ and may not be sufficient for the needs of the order-processing platform.

upvoted 3 times

sambb 1 year, 1 month ago

Your justification for option C is wrong.

Option C is valid, as Kubernetes on EC2 is very similar as the existing Kubernetes environment on-premises. But EKS is a safe bet and reduces operational overhead, while keeping the same API as previously. Hence, A is a better choice.

upvoted 9 times

gofavad926 Most Recent 3 weeks, 2 days ago

Selected Answer: A

A, is the only option to don't involve a rearchitected solution

upvoted 1 times

AimarLeo 2 months, 1 week ago

AWS exams got more 'sarcastic' with the ways of formulating questions.. E.g here: _A company is refactoring its on-premises order-processing platform in the AWS Cloud'

BUT '

The company does not want to make any major changes to the application.

Replatforming and Rehosting is not real refactoring.. but the closest answer as an architect with least operational overhead is A obviously.. aws questions sometimes can be ultra vague

upvoted 4 times

 **jpa8300** 3 months, 1 week ago

Selected Answer: A

A better explanation to choose between option A and D is that Amazon MQ responds to the requirement of not changing the app, because it accepts the same protocol as RabbitMQ (Supports AMQP, MQTT, STOMP, OpenWire, and JMS) while SQS has its own API, so it would need more changes to the app.

upvoted 3 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **Mikado211** 4 months, 4 weeks ago

Selected Answer: A

a bunch of keywords for this migration here :

Kubernetes == EKS

RabbitMQ == Amazon MQ

A fleet of VM == AMI + ec2 instances

The answer A proposes all those points, so it's perfect here.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A no doubt

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: A

A is the best choice.

upvoted 1 times

 **Musk** 1 year, 1 month ago

Selected Answer: B

Option A is re-hosting or maybe re-platforming. The question says the purpose is re-factoring, then it's B.

upvoted 2 times

 **c73bf38** 1 year, 1 month ago

It says the company does not want to make changes to the application in the problem statement. B would require significant code changes to the application.

upvoted 5 times

Question #96

Topic 1

A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.

The solutions architect created the following IAM policy and attached it to an IAM role:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DownloadUpload",  
            "Action": [  
                "s3:GetObject",  
                "s3:GetObjectVersion",  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::BucketName/*"  
        },  
        {  
            "Sid": "KMSAccess",  
            "Action": [  
                "kms:Decrypt",  
                "kms:Encrypt"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:kms:Region:Account:key/Key ID"  
        }  
    ]  
}
```

During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden.

Which action must the solutions architect add to the IAM policy to meet all the requirements?

- A. kms:GenerateDataKey
- B. kms:GetKeyPolicy
- C. kms:GetPublicKey
- D. kms:Sign

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: A

A. kms:GenerateDataKey

The solutions architect needs to add the "kms:GenerateDataKey" action to the IAM policy in order to generate a data key for client-side encryption. Without this action, the IAM role does not have the necessary permissions to generate a data key, which causes the error message when attempting to upload a new object.

upvoted 12 times

 **masetromain** 1 year, 2 months ago

The other options are not correct because they are not required for this use case. kms:GetKeyPolicy allows for the retrieval of the key policy for a CMK but it does not have any relation to client-side encryption of S3 objects, kms:GetPublicKey allows for the retrieval of the public key of a CMK, but it does not have any relation to client-side encryption of S3 objects and kms:Sign allows for signing a message using a CMK but it does not have any relation to client-side encryption of S3 objects.

upvoted 1 times

 **ninomfr64**  2 months, 3 weeks ago

Selected Answer: A

A = correct (you encrypt data with KMS Data Key and not KMS Key directly, unless data is < 4K)
B = getting the policy would allow to get the data key needed for encryption
C = client side encryption uses symmetric key not asymmetric keys
D = sign allows for signing messages, API calls, etc.

upvoted 3 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A - need data key for client-side encr

upvoted 1 times

✉ **Jesuisleon** 10 months, 4 weeks ago

I don't understand since it's client side encryption, it means both encryption and key and tools are maintained in client side before submitting to aws s3, why we need add kms:GenerateDatakey ? We don't need kms to do anything since it's client-side encryption all is done outside of aws.
upvoted 4 times

✉ **venvig** 7 months, 2 weeks ago

When you want to do the client side encryption, your files are most likely above 4K in size. So, you would be performing envelope encryption. For that, you need a data key.
You ask KMS to generate and give you the data key, supplying the kms CMK.
KMS would generate a new data key, encrypt it with the CMK and return you both the encrypted and plain data key. AWS would never retain the data key; they will immediately discard it.
You would now encrypt your data using the plain data key and immediately delete the plain data key (unencrypted). You store the encrypted data key that you got from KMS along with the encrypted data, which is then uploaded to s3. Note that AWS does NOT know about the data key at this point; only you know. KMS just holds the kms CMK that was used to encrypt the data key.
So, you need access to KMS to decrypt the data key before using that decrypted data key to unencrypt your data.
Similarly AWS cannot read your data, even though it has the KMS CMK and also the encrypted data key stored in s3.
This is why you need the generateDataKey permission. Hope this helps.

upvoted 8 times

✉ **venvig** 7 months, 2 weeks ago

Of course the answer is A

upvoted 1 times

✉ **bcx** 9 months, 3 weeks ago

Indeed, the question says client side encryption but the answer is all about S3-KMS.

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: A

A for sure

upvoted 1 times

✉ **Untamables** 1 year, 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/kms/latest/cryptographic-details/client-side-encryption.html>

upvoted 3 times

✉ **massa** 1 year, 2 months ago

Selected Answer: A

I Vote A.

<https://repost.aws/ja/knowledge-center/s3-large-file-encryption-kms-key>

Adding kms:GenerateDataKey is necessary.

upvoted 1 times

Question #97

Topic 1

A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.

How should a solutions architect configure the web ACLs to meet these requirements?

- A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.
- B. Use only rate-based rules in the web ACLs, and set the throttle limit as high as possible. Temporarily block all requests that exceed the limit. Define nested rules to narrow the scope of the rate tracking.
- C. Set the action of the web ACL rules to Block. Use only AWS managed rule groups in the web ACLs. Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.
- D. Use only custom rule groups in the web ACLs, and set the action to Allow. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Allow to Block.

Correct Answer: A

Community vote distribution



A (100%)

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: A

AWS WAF allows you to create web ACL (Access Control List) rules in "Count" mode, which allows you to monitor traffic without actually blocking it. In Count mode, AWS WAF counts the number of requests that match a particular rule, but doesn't take any action to block those requests.

Count mode can be useful in several ways:

Testing new rules: You can create new rules and test them in Count mode before enabling them to block traffic. This allows you to evaluate the effectiveness of your rules without risking false positives or false negatives.

Analyzing traffic: You can use Count mode to analyze traffic patterns and identify potential security threats. By monitoring the number of requests that match a particular rule, you can detect patterns that may indicate an attack or vulnerability.

Compliance reporting: Count mode can be used for compliance reporting, where you need to demonstrate that certain rules are being enforced. By counting the number of requests that match a rule, you can provide evidence that your security policies are being followed.

upvoted 18 times

 **masetromain**  1 year, 2 months ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/74273-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answer is A. Set the action of the web ACL rules to Count. Enable AWS WAF logging. Analyze the requests for false positives. Modify the rules to avoid any false positive. Over time, change the action of the web ACL rules from Count to Block.

This approach allows for monitoring of the incoming traffic and its behavior before taking any action that can affect the legitimate traffic. By setting the action to count, the web ACL will only log the requests that match the conditions of the rules, but it will not block them. This way, the company can analyze the requests and check for any false positives. Once they identify and correct any false positives, they can gradually change the action of the web ACL rules from count to block, thus improving the security posture of the application without adversely affecting legitimate traffic.

upvoted 5 times

 **masetromain** 1 year, 2 months ago

Option B is not correct because using only rate-based rules can lead to false positives and blocking of legitimate traffic. Option C is not correct because using only AWS managed rule groups can limit the flexibility and specificity of the web ACLs. Option D is not correct because using only custom rule groups with action set to allow can lead to security vulnerabilities.

upvoted 1 times

 **gofavad926**  3 weeks, 2 days ago

Selected Answer: A

A, configure the rules on COUNT

upvoted 1 times

 **Explorer_30** 7 months, 3 weeks ago

vote A

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

Its an A

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: A

A. Set the action of the web ACL rules to Count. Enable AWS WAF logging.

upvoted 1 times

 **Untamables** 1 year, 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html>

upvoted 1 times

Question #98

Topic 1

A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.

The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network. Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.

The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account. Deploy an AWS Lambda function in each AWS account. Configure the Lambda function to run every time an SNS topic receives a message. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account. Instruct the security team to distribute changes by publishing messages to its SNS topic.
- B. Create new customer-managed prefix lists in each AWS account within the organization. Populate the prefix lists in each account with all internal CIDR ranges. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups. Instruct the security team to share updates with each AWS account owner.
- C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.
- D. Create an IAM role in each account in the organization. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account. Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

Correct Answer: C

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: C

C. Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

This solution meets the requirements with the least amount of operational overhead as it requires the security team to create and maintain a single customer-managed prefix list, and share it with the organization using AWS Resource Access Manager. The owners of each AWS account are then responsible for allowing the prefix list in their security groups, which eliminates the need for the security team to manually notify each account owner when changes are made. This solution also eliminates the need for a separate AWS Lambda function in each account, reducing the overall complexity of the solution.

upvoted 10 times

masetromain 1 year, 2 months ago

Option A is not correct because it requires setting up an SNS topic in the security team's AWS account, and deploying an AWS Lambda function in each AWS account. This increases the operational overhead as it requires setting up and maintaining the SNS topic, and deploying and configuring the Lambda function in each account.

Option B is not correct because it requires creating new customer-managed prefix lists in each AWS account within the organization, which increases the operational overhead as it requires the security team to create and maintain multiple prefix lists.

Option D is not correct because it requires creating an IAM role in each account in the organization, which increases the operational overhead as it requires the security team to set up and maintain multiple roles. Additionally, it also deploys an AWS Lambda function in the security team's AWS account, which increases complexity and operational overhead.

upvoted 1 times

bur4an Highly Voted 7 months ago

masetromain is ChatGPT and might have outdated answers since it doesn't know AWS latest update to services

upvoted 7 times

AlbertC Most Recent 2 weeks, 3 days ago

Human cost is major overhead. I will go A. This is one time setup.

upvoted 1 times

✉ **StevePace** 3 weeks, 2 days ago

Selected Answer: C

Centralised management and standard use case for prefix lists and RAM

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C - basic RAM use case

upvoted 1 times

✉ **bcx** 9 months, 3 weeks ago

Selected Answer: C

Typical use case for RAM. It is the typical question that leads you to the solution without even finishing reading the question.

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: C

KEYWORD = AWS Resource Access Manager

Then C

upvoted 1 times

✉ **johnballs221** 10 months, 2 weeks ago

Selected Answer: D

operational overhead

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: C

Prefix lists + RAM

upvoted 2 times

✉ **God_Is_Love** 1 year, 1 month ago

Prefix lists + Resource Access Manager RAM is the solution.

upvoted 4 times

✉ **Musk** 1 year, 2 months ago

Selected Answer: C

Clearly

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: C

Create a new customer-managed prefix list in the security team's AWS account

upvoted 1 times

✉ **Untamables** 1 year, 2 months ago

Selected Answer: C

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>

upvoted 3 times

✉ **zhangyu20000** 1 year, 2 months ago

C is correct. The prefix list is managed by security team and shared with other accounts. Other accounts can directly use it.

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: D

The correct answer is D.

Option D creates an IAM role in each account in the organization which grants permissions to update security groups. Then, it deploys an AWS Lambda function in the security team's AWS account, this lambda function is able to assume the IAM roles in each account and update the security groups with the new IP CIDR ranges. This solution allows the security team to easily distribute and update the common set of IP CIDR ranges across all accounts with minimal operational overhead.

Option A, uses an SNS topic, where the security team would need to notify all account owners every time an update is made to the allow list and would require the developers in each account to run a Lambda function which updates the security group. This solution would require a lot of manual work, and is not automated.

upvoted 2 times

 **masetromain** 1 year, 2 months ago

Option B, requires the security team to notify the owners of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security groups, this solution would not provide a centralized control of the IP CIDR ranges and would require a lot of manual work.

Option C, uses a customer-managed prefix list in the security team's AWS account. But, it still requires the owners of each account to allow the new customer-managed prefix list ID in their security groups, this solution would not provide a centralized control of the IP CIDR ranges and would require a lot of manual work.

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Create an IAM role in each account in the organization. this does not add up to operational overhead right.

upvoted 1 times

 **BabaP** 10 months, 1 week ago

It's ChatGPT talking

upvoted 1 times

Question #99

Topic 1

A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN. The company is hosting internal applications with VPCs in multiple AWS accounts. Currently, the applications are accessible from the company's on-premises office network through an AWS Site-to-Site VPN connection. The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts.

A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home.

What is the MOST cost-effective solution that meets these requirements?

- A. Create a Client VPN endpoint in each AWS account. Configure required routing that allows access to internal applications.
- B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications.
- C. Create a Client VPN endpoint in the main AWS account. Provision a transit gateway that is connected to each AWS account. Configure required routing that allows access to internal applications.
- D. Create a Client VPN endpoint in the main AWS account. Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN.

Correct Answer: B*Community vote distribution*

C (51%)

B (49%)

 **hexie**  9 months, 1 week ago

Selected Answer: C

C.

Have you guys worked in a place where the configuration of B works?

The question clearly ask to design something scalable, and on C, the Transit Gateway serves as a network transit hub, allowing VPN connections to access resources across multiple VPCs in different AWS accounts.

VPC peering connections do not support transitive peering relationships, which means that if a user is connected to one VPC via AWS Client VPN, they cannot access resources in another VPC that's connected via a peering connection.

upvoted 26 times

 **vn_thanh tung** 7 months, 1 week ago

The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts => no need transit gw
upvoted 8 times

 **Impromptu** 3 months, 3 weeks ago

The question asks a scalable Client VPN solution (i.e. no openvpn on an EC2 instance or something like that), and asks for the most cost-effective. So AWS Client VPN is the scalable option. Reusing the current VPC peering is the most cost-effective compared to the far more expensive transit gateway solution.

I do agree that the peering does not support transitive peering. But for AWS Client VPN you get an ENI in the main account VPC and using the ENI you can access the VPCs over the VPC peering. So that does really work (in contrast to the Site-To-Site VPN):

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

upvoted 6 times

 **masetromain**  1 year, 2 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80782-exam-aws-certified-solutions-architect-professional-topic-1/>

B. Create a Client VPN endpoint in the main AWS account. Configure required routing that allows access to internal applications is the MOST cost-effective solution that meets these requirements. This solution allows employees to connect to the main AWS account using a Client VPN endpoint, and then use peering connections established with other AWS accounts to access the internal applications. This eliminates the need for additional Client VPN endpoints in each AWS account, reducing costs.

Option A, creating a Client VPN endpoint in each AWS account, would be more expensive as it would require multiple endpoints.

Option C, creating a transit gateway, would also add unnecessary costs.

Option D, connecting the Client VPN endpoint to the Site-to-Site VPN, may not provide a scalable solution for remote employees.

upvoted 17 times

 **red_panda**  4 days, 11 hours ago

Selected Answer: C

For me the question clearly wants to test our scalability solution. And for sure C is the best answer in my mind

upvoted 1 times

✉ **TonytheTiger** 5 days, 11 hours ago

Selected Answer: B

Option B: - the question is asking for " MOST cost-effective" solution. AWS Transit gateway charged for the number of connections that you make to the Transit Gateway per hour and the amount of traffic that flows through AWS Transit Gateway. AWS Site-to-Site VPN connection pricing still applies in addition to AWS Transit Gateway VPN attachment pricing.

<https://aws.amazon.com/transit-gateway/pricing/>

AWS Client VPN is a fully-managed remote access VPN solution used by your remote workforce to securely access resources within both AWS and your on-premises network. Fully elastic, it automatically scales up, or down, based on demand.

<https://aws.amazon.com/vpn/client-vpn/>

upvoted 1 times

✉ **TonytheTiger** 5 days, 11 hours ago

We (AWS) recommend this configuration if you need to give clients access to the resources inside an on-premises network only.

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-onprem.html>

upvoted 1 times

✉ **VerRi** 1 week, 2 days ago

Selected Answer: B

No need TGW...

upvoted 1 times

✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: C

C, This setup leverages a central point of access through the transit gateway, minimizing the need to manage multiple VPN endpoints across accounts and simplifying network administration

upvoted 1 times

✉ **k23319** 3 weeks, 3 days ago

Selected Answer: C

it's C

upvoted 1 times

✉ **TonytheTiger** 1 month ago

Not B - Not Transit Gateway, not the most cost-effective. In AWS Transit Gateway you are charged for the number of connections that you make to the Transit Gateway per hour and the amount of traffic that flows through AWS Transit Gateway. - <https://aws.amazon.com/transit-gateway/pricing/>

upvoted 1 times

✉ **Adzz** 1 month ago

Selected Answer: B

In the case of client VPN, your device is considered as an ENI inside the VPC, due to which you get the private IP from the VPC CIDR Block. If your VPC is peered with another VPC, then just edit the route tables appropriately just like you do, and your client VPN's ENI will be able to communicate with the peered VPC resources.

upvoted 2 times

✉ **a54b16f** 1 month, 1 week ago

Selected Answer: B

Read "The VPC in the company's main AWS account has peering connections established with VPCs in other AWS accounts." , so no need for TG

upvoted 1 times

✉ **VerRi** 1 month, 2 weeks ago

Selected Answer: B

Choose B for cost-effectiveness, though both B & C work.

upvoted 1 times

✉ **marszalekm** 1 month, 2 weeks ago

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

upvoted 2 times

✉ **AimarLeo** 2 months, 1 week ago

Selected Answer: B

No need for TGW.. Simple VPN client --> VPN endpoint --> Routing (Peering already)

upvoted 2 times

✉ **Mungi** 2 months, 2 weeks ago

Selected Answer: B

Client VPN, unlike Site to Site VPN, allows communication between peered VPCs. The requirement here is to add Client VPN at the minimum cost. Consequently, there's no need to alter the already peered architecture by adding a Transit Gateway (TGW). Although it's possible to configure with TGW, it's entirely feasible and more cost-efficient to configure with the current peering status simply by changing routing.

upvoted 2 times

 **ninomfr64** 2 months, 3 weeks ago

Selected Answer: B

A = no need for a Client VPN for each account, expensive

B = correct (see <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>)

C = no need for TGW, expensive

D = we need client to access app in the peered VPC not the on-premise <https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-professional-sap-c02/view/10/#>

upvoted 1 times

 **learnwithaniket** 3 months, 1 week ago

Selected Answer: C

Even though VPCs are peered there is no transitive communication possible. A <-> B, B <-> C then VPC A can not access resources in VPC C. This is not possible.

As a reason you need Transit Gateway.

upvoted 2 times

 **wmp7039** 3 months, 1 week ago

Selected Answer: C

Scaleable = TGW

upvoted 2 times

Question #100

Topic 1

A company is running an application in the AWS Cloud. Recent application metrics show inconsistent response times and a significant increase in error rates. Calls to third-party services are causing the delays. Currently, the application calls third-party services synchronously by directly invoking an AWS Lambda function.

A solutions architect needs to decouple the third-party service calls and ensure that all the calls are eventually completed.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.
- B. Use an AWS Step Functions state machine to pass events to the Lambda function.
- C. Use an Amazon EventBridge rule to pass events to the Lambda function.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic to store events and Invoke the Lambda function.

Correct Answer: A

Community vote distribution

A (100%)

✉  **masetromain**  1 year, 2 months ago

Selected Answer: A

The correct answer is A. Using an Amazon Simple Queue Service (SQS) queue to store events and invoke the Lambda function is a good solution to decouple the third-party service calls and ensure that all the calls are eventually completed. SQS is a fully managed, reliable, and highly scalable message queuing service that allows applications to send, store, and receive messages between distributed components. By sending the third-party service calls to an SQS queue, it allows the application to continue processing without waiting for the third-party services to respond, which can result in faster response times and lower error rates.

upvoted 5 times

✉  **masetromain** 1 year, 2 months ago

Other options like AWS Step Functions state machine, Amazon EventBridge, and Amazon Simple Notification Service (SNS) topic are not appropriate for this use case. AWS Step Functions is a service that makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated SaaS applications, and AWS services. Amazon SNS is a fully managed messaging service for both application-to-application and application-to-person (A2P) communication. These services are not focused on providing message queues and would not be the best fit for this use case.

upvoted 1 times

✉  **career360guru**  3 weeks, 2 days ago

Selected Answer: A

Option A

upvoted 1 times

✉  **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 2 times

✉  **HC888** 4 months, 2 weeks ago

Selected Answer: A

SQS support dead letter queue and retry if the event processed fails

upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A no brainer

upvoted 1 times

✉  **rbm2023** 11 months ago

Selected Answer: A

step functions would not help on the decoupling if you are not using an asynchronous element in this architecture which is SQS. the application need to have the ability to move out from synchronous calls to the third party services. correct answer is A.

upvoted 2 times

✉  **hpipit** 1 year ago

Selected Answer: A

A : SQS QUEUE

upvoted 1 times

  **mfsec** 1 year ago**Selected Answer: A**

SQS for decoupling

upvoted 2 times

  **c73bf38** 1 year, 1 month ago**Selected Answer: A**

SQS ---> Lambda is the correct option

upvoted 2 times

  **zozza2023** 1 year, 2 months ago**Selected Answer: A**

decouple ==> SQS

upvoted 1 times

  **Untamables** 1 year, 2 months ago**Selected Answer: A**

The application needs to pass the initiative to the next step. That means the application does not wait the response from the Lambda function, it should have the responsibility only to call the Lambda function. To do so, the application only throw the job information to Amazon SQS queue and finish. After that, AWS Lambda function can pull the job information from SQS queue and start processing actively.

<https://docs.aws.amazon.com/lambda/latest/dg/invocation-async.html>

upvoted 2 times

  **Qing** 1 year, 2 months ago

I vote for C - use Step Functions with its callback feature to throttle the third party api call.

upvoted 1 times

Question #101

Topic 1

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

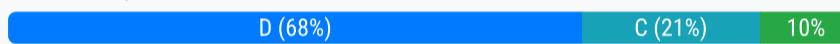
The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

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

- A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

Correct Answer: D

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: D

The correct answer is D. Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role to create a trust relationship with the new IAM role in the sales account.

This solution meets the requirements by allowing the marketing team to access the data in the S3 bucket in the sales account through assuming an IAM role, which eliminates the need to copy the data or share the KMS key, and also eliminates the need to modify the S3 bucket policy or create a KMS grant. This solution allows to use the same access to the bucket without duplicating data and re-encrypting it.

upvoted 20 times

masetromain 1 year, 2 months ago

A. Create a new S3 bucket in the marketing account. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket is not correct because it would create unnecessary data duplication and increased storage costs.

B. Create an SCP to grant access to the S3 bucket to the marketing account. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket is not correct because it does not provide a secure way to share the KMS key between accounts and also it would create unnecessary data duplication and increased storage costs.

upvoted 4 times

masetromain 1 year, 2 months ago

C. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket is not correct because the Sales team's S3 bucket is in a different account, so the Marketing team cannot update the policy on the Sales team's S3 bucket.

upvoted 2 times

Maria2023 Highly Voted 9 months, 3 weeks ago

Selected Answer: D

The catch is in the answers - "Update the S3 bucket policy in the marketing account". We don't need to access a bucket in the marketing but the sales account.

upvoted 7 times

djeong95 Most Recent 1 month ago

I think this is a great question with poorly phrased answers. If I have to choose between C and D, it would be neither since they both do not provide complete answers. Let me explain:

For C, you are updating the S3 bucket policy for the marketing account, when you should be doing that for the sales account. So, C is wrong. However, if that were fixed to the sales account, everything would make sense, since the sales account would be providing the right policy, granting the correct KMS key permission, and the marketing account would be tweaking its permission in QuickSight.

For D, it is wrong simply because it says nothing about providing KMS key grant. Not only do you have to establish trust policy in the QuickSight role to access S3 bucket, you have to allow Decrypt to happen. You have to explicitly spell this out (read the permission part in the link below).

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html>

upvoted 2 times

✉ **djeong95** 1 month ago

<https://repost.aws/knowledge-center/quicksight-cross-account-s3>

upvoted 1 times

✉ **VerRi** 1 month, 2 weeks ago

Selected Answer: D

Option C: Update the S3 bucket policy in the "marketing account"lol

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: C

The answer is C. Update the S3 bucket policy in the sales account to grant access to the QuickSight role in the marketing account. Create a KMS grant for the encryption key that is used in the S3 bucket. Grant decrypt access to the QuickSight role. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.

Option C correctly identifies the need to update the S3 bucket policy to grant access specifically to the QuickSight IAM role in the marketing account, which directly addresses the requirement for cross-account access to S3 data. Additionally, creating a KMS grant for the encryption key to allow decrypt access by the QuickSight role aligns with best practices for secure, cross-account access to encrypted S3 data. This approach minimizes operational overhead by using existing roles and permissions without the need for replication or additional resource sharing mechanisms.

upvoted 2 times

✉ **AimarLeo** 2 months ago

the question is badly formulated.. with all given options missing each a spec .. none of the answers are fully convincing

upvoted 2 times

✉ **tmlong18** 2 months, 4 weeks ago

Selected Answer: C

All answers are wrong:

- A. No KMS, not necessary replication
- B. No IAM
- C. No KMS

But the most likely answer is C.

"Update the S3 bucket policy in the marketing account"

The question was never asked marketing s3 team bucket and all the data store in sales team S3 bucket.

I think it's a typing error (marketing-> sales).

upvoted 4 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

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

Selected Answer: D

Answer is D - see: <https://medium.com/codebyte/cross-account-s3-object-copying-with-kms-encrypted-buckets-5ebabef8aa03>

upvoted 1 times

✉ **bjexamprep** 4 months ago

none of the answers is correct.

A: no mention of role granted to quicksight and no permission to KMS is granted.

B: SCP is not designed for this.

C: no mentioning of creating S3 bucket in marketing account. QuickSight role is created in Marketing account, while the decryption access is required in sales account.

D: Lack of decryption access to KMS is granted to the new created IAM role in sales account.

upvoted 1 times

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

Selected Answer: A

looks like the answer is D, but take a look on Hyperdanny's answer

upvoted 1 times

✉ **rsn** 7 months ago

Selected Answer: A

D is not correct. Trust relationship must be established in the role in Sales account to grant access to Marketing account..

upvoted 2 times

✉ **ele** 5 months ago

Trust relationship must be established on both sides. From Marketing account, the role must have allow to assume the IAM role in Sales account. In Sales account IAM role must have Principle == to Marketing account.

D is correct.

upvoted 1 times

✉ **uC6rW1aB** 7 months ago

Selected Answer: B

The problems with option D are mainly that it adds more operational burden and complexity relative to the other options, and does not explicitly address how KMS keys are shared.

Option B use AWS Resource Access Manager (AWS RAM) to share the KMS key and access to S3 bucket looks more reasonable

upvoted 1 times

✉ **softarts** 7 months, 3 weeks ago

Selected Answer: D

D for sure

upvoted 2 times

✉ **Hyperdanny** 8 months, 4 weeks ago

Selected Answer: A

All answers seem to be a little bit off.

What confuses me about answer D is "Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account." Why would you update the Quicksight role?

Looking at all the answers, I think only A is actually feasible, although it is not a good solution to replicate everything....

upvoted 3 times

✉ **rsn** 7 months ago

I agree

upvoted 1 times

✉ **chikorita** 7 months, 1 week ago

i am also inclined towards A but D is also correct here but i believe it;s poorly worded

cuz Sales account needs to be the one who maintains "trust relationship" with Marketing account; Marketing accounts needs to edit its policy to "assume Sales role"

upvoted 4 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

It's C, although the wording about s3 bucket being in the marketing dept is probably off.

Other options make even less sense

upvoted 3 times

✉ **Jesuisleon** 10 months, 3 weeks ago

Selected Answer: D

D Is right and C is wrong.

I have read the link <https://repost.aws/knowledge-center/quicksight-cross-account-s3>

I found C is really badly worded "Update the S3 bucket policy in the marketing account to grant access to the QuickSight role", you should update the S3 bucket policy in the sale account NOT marketing account because S3 is inside sale account not market account.

Correct this sentence and based on the link above, I think C is right answer.

upvoted 2 times

Question #102

Topic 1

A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.

Which solution will meet these requirements?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
- B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.
- C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.
- D. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **xplusfb**  8 months ago

Selected Answer: C

This question quietly smell weird to me but no problem answer is C

Exp : AWS Schema Conversion Tool (SCT) can automatically convert the database schema from Microsoft SQL Server to Amazon RDS for MySQL. This allows for a smooth transition of the database schema without any manual intervention. AWS DMS can then be used to migrate the data from the on-premises databases to the newly created Amazon RDS for MySQL instance. This service can perform a one-time migration of the data or can set up ongoing replication of data changes to keep the on-premises and AWS databases in sync.

upvoted 7 times

✉️  **TonytheTiger**  1 month ago

Selected Answer: C

This process becomes easier with services like AWS DMS and AWS Schema Conversion Tool (AWS SCT), which help you migrate your commercial database to an open-source database on AWS with minimal downtime.

In heterogeneous database migrations, the source and target databases engines are different, as in Oracle to Amazon Aurora, or Oracle to PostgreSQL, MySQL, or MariaDB migrations. The schema structure, data types, and database code in the source and target databases can be quite different, so the schema and code must be transformed before the data migration starts. For this reason, heterogeneous migration is a two-step process:

Step 1. Convert the source schema and code to match that of the target database. You can use AWS SCT for this conversion.

Step 2. Migrate data from the source database to the target database. You can use AWS DMS for this process.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-oracle-database/heterogeneous-migration.html>

upvoted 1 times

✉️  **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

✉️  **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: C

My 2 cents, Heterogeneous database migration and SCT go with each other

upvoted 3 times

✉️  **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C of course

upvoted 1 times

✉️  **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: C

keyword = AWS Schema Conversion Tool

upvoted 1 times

✉️ **rbm2023** 11 months ago

Selected Answer: C

The question is about heterogenous database migration so in this case we need to convert the DB to a new schema. Therefore, answer is C

upvoted 2 times

✉️ **mfsec** 1 year ago

Selected Answer: C

Use the AWS Schema Conversion Tool

upvoted 1 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: C

For heterogenous DBs, SCT is apt.

upvoted 1 times

✉️ **Appon** 1 year, 2 months ago

Selected Answer: C

<https://aws.amazon.com/blogs/database/migrating-a-sql-server-database-to-a-mysql-compatible-database-engine/>

upvoted 2 times

✉️ **Musk** 1 year, 2 months ago

Selected Answer: C

heterogenous -> from one DB engine to another

upvoted 2 times

✉️ **MasterP007** 1 year, 2 months ago

Straightforward - C

upvoted 2 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is the answer

upvoted 3 times

✉️ **masetromain** 1 year, 2 months ago

Selected Answer: C

The correct answer is C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.

AWS Schema Conversion Tool (SCT) can automatically convert the database schema from Microsoft SQL Server to Amazon RDS for MySQL. This allows for a smooth transition of the database schema without any manual intervention.

AWS DMS can then be used to migrate the data from the on-premises databases to the newly created Amazon RDS for MySQL instance. This service can perform a one-time migration of the data or can set up ongoing replication of data changes to keep the on-premises and AWS databases in sync.

upvoted 4 times

✉️ **masetromain** 1 year, 2 months ago

Option A is not correct because while Amazon RDS for MySQL supports SQL Server databases, it is not a good fit for migrating business-critical applications. The data model and architecture are different and would require significant re-engineering.

Option B is not correct because AWS Snowball Edge Storage Optimized devices are used for transferring large amounts of data to and from AWS, but they do not support SQL Server.

Option D is not correct because AWS DataSync can only transfer files and folders, it does not support SQL Server databases.

upvoted 2 times

Question #103

Topic 1

A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.

After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.

Which combination of steps will meet these requirements? (Choose three.)

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
- C. In the production account, create a role. Attach the new policy to the role. Define the development account as a trusted entity.
- D. In the development account, create a role. Attach the new policy to the role. Define the production account as a trusted entity.
- E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account.
- F. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account.

Correct Answer: ADE

Community vote distribution



masetromain 1 year, 2 months ago

Selected Answer: ACE

The correct answer is A, C, and E.

A: In the production account, creating a new IAM policy that allows read and write access to the S3 bucket is correct because it allows the design team to upload and update the static assets in the S3 bucket in the production account.

C: In the production account, creating a role and attaching the new policy to the role, and defining the development account as a trusted entity is correct because it allows the design team from the development account to assume the role and access the S3 bucket in the production account, while limiting their access to only the specific resources and actions defined in the policy.

upvoted 12 times

masetromain 1 year, 2 months ago

E: In the development account, creating a group that contains all the IAM users of the design team and attaching a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account is correct because it allows the users in the group to assume the role created in the production account, which gives them access to the S3 bucket in the production account.

The other choices are not correct because:

B: In the development account, creating a new IAM policy that allows read and write access to the S3 bucket is not correct because the design team needs to access the S3 bucket in the production account, not the development account.

upvoted 4 times

masetromain 1 year, 2 months ago

D: In the development account, creating a role, attaching the new policy to the role and defining the production account as a trusted entity is not correct because the design team needs to assume a role in the production account to access the S3 bucket, not create a role in the development account.

F: In the development account, creating a group that contains all the IAM users of the design team and attaching a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account is not correct because the design team needs to assume a role in the production account to access the S3 bucket, not the development account.

upvoted 2 times

zejou1 1 year ago

Selected Answer: ACE

Step 1: Create a role in the Production Account; create the role in the Production account and specify the Development account as a trusted entity. You also limit the role permissions to only read and write access to the productionapp bucket. Anyone granted permission to use the role can read and write to the productionapp bucket.

Step 2: Grant access to the role. Sign in as an administrator in the Development account and allow the AssumeRole action on the UpdateApp role.

in the Production account.

So, recap, production account you create the policy for S3, and you set development account as a trusted entity. Then on the development account you allow the sts:assumeRole action on the role in production account.

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

upvoted 8 times

✉️ **Dgix** Most Recent 2 weeks, 5 days ago

Selected Answer: ACE

ACE. F is a trap.

upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: ACE

A, C and E

upvoted 1 times

✉️ **AMohanty** 5 months ago

BCE

Need to provide Account in Dev S3 Read Write Access

We define the permissions of the user in the Account it was created in

upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: ACE

ACE in this case

upvoted 1 times

✉️ **MoussaNoussa** 9 months, 4 weeks ago

ACE is the correct choice of course

upvoted 1 times

✉️ **leehjworking** 10 months, 4 weeks ago

Selected Answer: ACE

Vote for ACE

upvoted 2 times

✉️ **mfsec** 1 year ago

Selected Answer: ACE

ACE is the best choice

upvoted 3 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: ACE

Make Dev account as trusted entity. create a role in prod account. attache IAM policy of prod account and let development account assume this role to access prod s3 bucket.

upvoted 2 times

✉️ **Musk** 1 year, 2 months ago

Selected Answer: ACE

I think it's clear

upvoted 1 times

✉️ **tatdatpham** 1 year, 2 months ago

Selected Answer: ACE

ACE is correct answer

upvoted 2 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: ACE

ACE should works

upvoted 2 times

✉️ **zhangyu20000** 1 year, 2 months ago

ACE is my answer

upvoted 2 times

✉️ **masetromain** 1 year, 2 months ago

Selected Answer: ADE

A, D, and E are the correct steps that would meet the requirements.

A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket. This will allow the design team to read and write to the S3 bucket that holds the assets in the production account.

D. In the development account, create a role. Attach the new policy to the role. Define the production account as a trusted entity. This will allow the design team to assume a role in the development account that has permissions to access the S3 bucket in the production account.

E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account. This will allow the users in the design team group to assume the role created in step D and access the S3 bucket in the production account.

upvoted 2 times

 **masetromain** 1 year, 2 months ago

Option B is not required because the design team needs to access the S3 bucket in the production account, not in the development account.

Option C is not required because the design team needs to access the S3 bucket in the production account and this can be done by assuming a role in the development account.

Option F is not required because the design team needs to access the S3 bucket in the production account and this can be done by assuming a role in the development account that is trusted by the production account.

upvoted 1 times

Question #104

Topic 1

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

A solutions architect must mitigate the performance issues before the company launches the application to production.

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

- A. Create a new Elastic Beanstalk application. Select a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the maximum CPU utilization is over 85% for 5 minutes.
- B. Create a second Elastic Beanstalk environment. Apply the traffic-splitting deployment policy. Specify a percentage of incoming traffic to direct to the new environment if the average CPU utilization is over 85% for 5 minutes.
- C. Modify the existing environment's capacity configuration to use a load-balanced environment type. Select all Availability Zones. Add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes.
- D. Select the Rebuild environment action with the load balancing option. Select an Availability Zones. Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

Correct Answer: A
Community vote distribution


Untamables Highly Voted 1 year, 2 months ago

Selected Answer: C

I think AWS wants you to know is the below.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 19 times

ninomfr64 Most Recent 2 months, 3 weeks ago

A = you don't need to create a new application (instead you could create a new environment in the existing application)

B = traffic-split is used to deploy a new version of the app, not to scale out

C = correct

D = rebuild does not allow to change environment configuration <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environment-management-rebuild.html>

upvoted 1 times

Maygam 3 months, 2 weeks ago

Selected Answer: C

You can change the existing environment from single instance to load balanced.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 2 times

career360guru 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

yuliaqwerty 3 months, 3 weeks ago

C here <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/GettingStarted.EditConfig.html>

upvoted 1 times

severlight 4 months, 3 weeks ago

Selected Answer: C

you can change existing Beanstalk environment type from a single instance to load-balanced

upvoted 2 times

CuteRunRun 8 months ago

Selected Answer: C

I prefer C

upvoted 1 times

Spaco 8 months, 2 weeks ago

Selected Answer: C

Option C is very correct. See <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html> for confirmation
upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

its a C
upvoted 1 times

✉ **leehjworking** 10 months, 4 weeks ago

Anybody know why we should select all AZs?
upvoted 3 times

✉ **mfsec** 1 year ago

Selected Answer: C

Modify the existing environment's capacity configuration to use a load-balanced environment type.
upvoted 1 times

✉ **zejou1** 1 year ago

Selected Answer: C

You can change your environment type to a single-instance or load-balanced, scalable environment by editing your environment's configuration. In some cases, you might want to change your environment type from one type to another. For example, let's say that you developed and tested an application in a single-instance environment to save costs. When your application is ready for production, you can change the environment type to a load-balanced, scalable environment so that it can scale to meet the demands of your customers.
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

upvoted 4 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: C

A is wrong. no need to re create new EB env when the question is asking to mitigate probable performance issues based on current compute consumption of >=85%
upvoted 2 times

✉ **spd** 1 year, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>
upvoted 2 times

✉ **Musk** 1 year, 2 months ago

Selected Answer: C

It's C. <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html#using-features.managing.changetype>
upvoted 1 times

✉ **vsk12** 1 year, 2 months ago

A: Elastic Beanstalk environment can not be changed.

upvoted 2 times

✉ **mikeshop** 1 year, 2 months ago

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html>

Yes they can.

upvoted 2 times

✉ **romidan** 1 year, 2 months ago

I think C does make sense as per the link below -

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/GettingStarted.EditConfig.html>

As per this link, a change would automatically initiate the new instance as per the ASG min attribute.

upvoted 1 times

Question #105

Topic 1

A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Correct Answer: B

Community vote distribution



masetromain Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.

This is the optimal solution as migrating the database to Amazon RDS will provide the ability to easily scale read replicas for handling increased read traffic during the end of the month. Additionally, RDS will manage the underlying infrastructure and provide automatic backups, software patching, and monitoring, which will reduce the operational overhead for the company.

Option A may help but it will not be sufficient to handle the heavy load, option C and D are not efficient solutions to han
upvoted 14 times

gofavad926 Most Recent 3 weeks, 2 days ago

Selected Answer: B

B, include read replicas

upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: B

Option B -> Reporting workload = higher read operation ==> Solution RDS read replica.

upvoted 1 times

hansean 5 months, 3 weeks ago

Selected Answer: D

I go with D

upvoted 1 times

uC6rW1aB 7 months ago

Selected Answer: D

I vote D

To solve heavy IO issue, I think both option B and D both works. But the question demands for to "handle the month-end load with the LEAST impact on performance" , Option B create the new read replicas during end of month seems too complicated, you'll need to separate read/write traffic from application at the end of the month.

upvoted 1 times

venvig 7 months, 1 week ago

Selected Answer: B

Reporting is also an important hint. Only read operations are needed here; so read replicas would serve the purpose

upvoted 2 times

xplusfb 8 months ago

Selected Answer: B

all other sections not applicable i guess specially D its so funny. Each month none of technical person doesnt want to do like this task.
upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

B of cpourse

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

it slows down during the final three days of each month due to month-end reporting
then

hight read in database == solution add read replicas

B

upvoted 2 times

 **nexus2020** 9 months, 1 week ago

month end reporting is to submit the financial data, aka write the new data to DB

upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: B

Performing a one-time migration

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: B

B is the best solution

upvoted 2 times

Question #106

Topic 1

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable, but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission to access the ECR image repository. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- B. Migrate the application code to a container that runs in AWS Lambda. Build an Amazon API Gateway REST API with Lambda integration. Use API Gateway to interact with the application.
- C. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Container. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository. Use Amazon API Gateway to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

Correct Answer: B

Community vote distribution

A (93%)

✉️ **masetromain** 1 year, 2 months ago

Selected Answer: A

The correct answer would be A, as migrating the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container and storing container images in Amazon Elastic Container Registry (Amazon ECR) would minimize the code changes and administrative overhead required to maintain the servers. This option would allow the company to use the Application Load Balancer (ALB) to interact with the application and the ECS task execution role permission to access the ECR image repository.

Option B would require the application code to be migrated to a container that runs in AWS Lambda, which would require more code changes.

Option C would require migrating the application to Amazon Elastic Kubernetes Service (Amazon EKS) which would require more administrative overhead.

Option D would require configuring Lambda to use an Application Load Balancer (ALB), which is not a native feature of Lambda.

upvoted 15 times

✉️ **Musk** 1 year, 2 months ago

B does not say anything about Lambda. Where have you read that?

upvoted 1 times

✉️ **Musk** 1 year, 2 months ago

You are right, I mixed A with B

upvoted 1 times

✉️ **rbm2023** 11 months ago

There is another problem with Option B, it suggests using EKS with managed node groups and not Fargate, which breaks the requirement for reducing administrative overhead

upvoted 1 times

✉️ **masetromain** 1 year, 2 months ago

This solution allows for the existing application code to be packaged into a container, which can then be deployed to ECS on Fargate. The use of AWS App2Container will help automate the containerization process, minimizing the need for code changes. Additionally, by using ECR to store container images, the application can continue to use the same images and dependencies that it currently relies on. The use of an Application Load Balancer (ALB) to interact with the application further simplifies the migration process by allowing the use of the existing application's endpoint.

upvoted 4 times

✉️ **zejou1** 1 year ago

Selected Answer: A

AWS App2Container (A2C) is a command line tool to help you lift and shift applications that run in your on-premises data centers or on virtual machines, so that they run in containers that are managed by Amazon ECS, Amazon EKS, or AWS App Runner.

Moving legacy applications to containers is often the starting point toward application modernization. There are many benefits to

containerization:

- Reduces operational overhead and infrastructure costs
- Increases development and deployment agility
- Standardizes build and deployment processes across an organization

<https://docs.aws.amazon.com/app2container/latest/UserGuide/what-is-a2c.html>

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers. AWS Fargate is compatible with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

<https://aws.amazon.com/fargate/>

upvoted 7 times

✉ **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: A

A, ECS Fargate

upvoted 1 times

✉ **AimarLeo** 2 months, 1 week ago

Selected Answer: A

If the keyword 'Java' has not been mentioned, Answer A would have been considered as A2C (App2Container) is valid only for Java and .Net web applications

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: A

A = correct

B = migrating app to container to be executed in a Lambda requires more code changes

C = EKS with managed node group requires more operations than ECS with Fargate

D = see B

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A. Option C EKS not not valid because as using API Gateway is not needed and may require more code changes.

upvoted 1 times

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

Selected Answer: A

in the case of fargate capacity provider you should grant permissions to access ecr to task execution role, otherwise to ec2 instance roles which you run containers on

upvoted 1 times

✉ **CVDON** 5 months, 3 weeks ago

Sorry is A

upvoted 1 times

✉ **CVDON** 5 months, 3 weeks ago

C on eks because of complex VM dependecies

upvoted 1 times

✉ **CVDON** 5 months, 3 weeks ago

D because of complex vm dependencies

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

it's an A

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

Did anyone notice that part "has complex dependencies on VMs that are in the company's data center."? If the application has complex dependencies on VMs then how do we migrate it to containers or lambda? Another awkward question.

upvoted 1 times

✉ **Sarutobi** 11 months, 2 weeks ago

Selected Answer: A

I still select A, but as someone that has migrated Java applications to AWS using AWS App2Container and RedHat S2i, this is a lot of pain.

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: A

Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container.

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: A

least code changes

upvoted 2 times

 **keonlee** 1 year, 1 month ago

Selected Answer: A

Fargate, Modernize stack

upvoted 2 times

 **spd** 1 year, 1 month ago

Selected Answer: A

Least code changes

upvoted 2 times

Question #107

Topic 1

A company has an asynchronous HTTP application that is hosted as an AWS Lambda function. A public Amazon API Gateway endpoint invokes the Lambda function. The Lambda function and the API Gateway endpoint reside in the us-east-1 Region. A solutions architect needs to redesign the application to support failover to another AWS Region.

Which solution will meet these requirements?

- A. Create an API Gateway endpoint in the us-west-2 Region to direct traffic to the Lambda function in us-east-1. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure API Gateway to direct traffic to the SQS queue instead of to the Lambda function. Configure the Lambda function to pull messages from the queue for processing.
- C. Deploy the Lambda function to the us-west-2 Region. Create an API Gateway endpoint in us-west-2 to direct traffic to the Lambda function in us-west-2. Configure AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints.
- D. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.

Correct Answer: B

Community vote distribution



✉ **masetromain** 1 year, 2 months ago

Selected Answer: D

The correct answer is D. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints. This solution meets the requirement of having a failover to another region by having a copy of the Lambda function and API Gateway endpoint in a different region, and using Route 53's failover routing policy to route traffic between the two regions.

Option A is not correct because it only creates an additional API Gateway endpoint in us-west-2 and relies on Route 53's failover routing policy to direct traffic to the correct endpoint. But it does not deploy the Lambda function to the new region and this makes the failover incomplete.

upvoted 19 times

✉ **testingaws123** 1 year ago

You always use ChatGPT to paste answers. Most of the time ChatGPT gives wrong answers do you know this?

upvoted 8 times

✉ **masetromain** 1 year, 2 months ago

Option B is not correct because it uses a SQS queue as a buffer between the API Gateway and the Lambda function, but this does not provide failover to another region. In addition, it would also increase the latency of the system as the SQS will act as an additional layer.

Option C is not correct because it deploys the Lambda function to the us-west-2 Region and creates an API Gateway endpoint in the same region. But it uses AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints. However, this is not a failover solution as both regions will be active and serving traffic at the same time.

upvoted 3 times

✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: D

D, deploy everything in the second region and configure the failover routing policy

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **venvig** 7 months, 1 week ago

Selected Answer: D

Refer <https://aws.amazon.com/blogs/architecture/implementing-multi-region-disaster-recovery-using-event-driven-architecture/>

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

clearly D

upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: D

Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region

upvoted 1 times

✉  **zejou1** 1 year ago

Selected Answer: D

Currently, the default API endpoint type in API Gateway is the edge-optimized API endpoint, which enables clients to access an API through an Amazon CloudFront distribution. This typically improves connection time for geographically diverse clients. By default, a custom domain name is globally unique and the edge-optimized API endpoint would invoke a Lambda function in a single region in the case of Lambda integration. You can't use this type of endpoint with a Route 53 active-active setup and fail-over.

The new regional API endpoint in API Gateway moves the API endpoint into the region and the custom domain name is unique per region. This makes it possible to run a full copy of an API in each region and then use Route 53 to use an active-active setup and failover.

<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 2 times

✉  **God_Is_Love** 1 year, 1 month ago

Selected Answer: D

B is wrong, cannot direct traffic to SQS Queue ? it does not even mention posting messages to queue.

upvoted 1 times

✉  **zozza2023** 1 year, 2 months ago

Selected Answer: D

The correct answer is D

upvoted 2 times

✉  **zhangyu20000** 1 year, 2 months ago

D is correct

A is not because the Lambda is in us-east-1 but api gateway is in us-west-2. cannot cross regions

upvoted 4 times

✉  **masetromain** 1 year, 2 months ago

Selected Answer: A

The correct answer is A.

In this solution, an API Gateway endpoint is created in the us-west-2 Region. This new endpoint is configured to direct traffic to the Lambda function in us-east-1. If a failure occurs in the us-east-1 Region, Amazon Route 53's failover routing policy automatically routes traffic to the us-west-2 Region. This ensures that traffic is directed to a healthy endpoint, providing failover support for the application.

B, C and D does not meet the requirement of having failover routing policy.

In B, SQS is not a failover mechanism, it is a messaging service and it does not provide failover routing.

In C, Global Accelerator and Application Load Balancer does not provide failover routing.

In D, While creating a second endpoint in the us-west-2 Region and using Amazon Route 53 to route traffic to it, it still does not provide failover routing.

upvoted 2 times

✉  **CProgrammer** 6 months, 2 weeks ago

D CLEARLY States: Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints. You claimed it did not , and the moderator ALLOWED IT ?!?!?

upvoted 1 times

✉  **CProgrammer** 6 months, 2 weeks ago

Gateway VPC endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.

<https://docs.aws.amazon.com/vpc/latest/privateLink/gateway-endpoints.html>

=> IN CONTRAST

These are the ENDPOINTS for API Gateway:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html>

Gateway endpoint DOES NOT DIRECT TRAFFIC PERIOD

upvoted 1 times

Question #108

Topic 1

A retail company has structured its AWS accounts to be part of an organization in AWS Organizations. The company has set up consolidated billing and has mapped its departments to the following OUs: Finance, Sales, Human Resources (HR), Marketing, and Operations. Each OU has multiple AWS accounts, one for each environment within a department. These environments are development, test, pre-production, and production.

The HR department is releasing a new system that will launch in 3 months. In preparation, the HR department has purchased several Reserved Instances (RIs) in its production AWS account. The HR department will install the new application on this account. The HR department wants to make sure that other departments cannot share the RI discounts.

Which solution will meet these requirements?

- A. In the AWS Billing and Cost Management console for the HR department's production account turn off RI sharing.
- B. Remove the HR department's production AWS account from the organization. Add the account to the consolidating billing configuration only.
- C. In the AWS Billing and Cost Management console, use the organization's management account to turn off RI Sharing for the HR department's production AWS account.
- D. Create an SCP in the organization to restrict access to the RIs. Apply the SCP to the OUs of the other departments.

Correct Answer: C

Community vote distribution



✉ **kiran15789** 1 year, 1 month ago

Selected Answer: C

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing
upvoted 6 times

✉ **Dgix** 4 weeks ago

Selected Answer: C

It is indeed C.
upvoted 1 times

✉ **Dgix** 1 month ago

Selected Answer: A

RI sharing is done for the whole Org. It's all or nothing, and it's done in the Billing and Cost Management console in the Org account.
upvoted 1 times

✉ **JOKERO** 1 month ago

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

C

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: A

Option A is correct because AWS allows the management of RI sharing settings at the account level within the AWS Billing and Cost Management console. By turning off RI sharing in the HR department's production account, the RI benefits (such as the discounted rate) are applied only to instances within that account, preventing other accounts, even within the same organization, from accessing these discounts. This directly addresses the requirement.

Option C suggests using the organization's management account to turn off RI sharing for the HR department's production AWS account. While the management account controls many aspects of AWS Organizations, including consolidated billing, RI sharing preferences are managed at the individual account level within the Billing and Cost Management console, not directly through the management account for specific accounts.
upvoted 2 times

✉ **horyoryo** 3 months, 2 weeks ago

Selected Answer: C

option C

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

surely C

upvoted 3 times

✉ **mfsec** 1 year ago

Selected Answer: C

C is the way to go

upvoted 1 times

✉ **sambb** 1 year, 1 month ago

Selected Answer: C

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 3 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: C

Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing

<https://us-east-1.console.aws.amazon.com/billing/home#/preferences>

upvoted 3 times

✉ **testingaws123** 1 year, 1 month ago

Selected Answer: D

How can you restrict access from AWS billing console? Can you show me please??

Option D is the correct solution because an SCP (Service Control Policy) can be created in the AWS Organizations service to restrict access to specific resources or actions across the entire organization or specific OUs. In this case, an SCP can be created to restrict other departments from accessing the RIs purchased by the HR department's production account. This ensures that the discounts are not shared with other departments.

upvoted 3 times

✉ **God_Is_Love** 1 year, 1 month ago

Bro, Go to Management account --> Billing Dashboard --> Billing preferences, this option is there to choose enable/disable RI discounts sharing

<https://us-east-1.console.aws.amazon.com/billing/home#/preferences>

upvoted 4 times

✉ **chikorita** 7 months, 4 weeks ago

initially i thought the same....but the catch here is that RIs are purchased in HR Prod department

So, we have to work on disabling discount sharing wrt that account so that IT IS NOT SHARED W OTHERS and this actions can only be performed from Management account

upvoted 1 times

✉ **SK_Tyagi** 7 months, 3 weeks ago

Restricting the access to RI's is not the ask in the question, only "restricting the RI discounts" from HR to other departments is the ask, and that you could be done by Management Account (as identified by others in this forum). Hope that helps!

upvoted 2 times

✉ **jojom19980** 1 year, 2 months ago

Selected Answer: C

The correct answer is C

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: C

The correct answer is C.

In this solution, the organization's management account can be used to turn off RI sharing for the HR department's production AWS account in the AWS Billing and Cost Management console. This will ensure that the other departments cannot share the RI discounts and the HR department can use the RIs for their new system without any interruption.

upvoted 3 times

✉ **masetromain** 1 year, 2 months ago

A, B and D does not meet the requirement of turning off RI sharing for the HR department's production AWS account.

In A, Turning off RI sharing in the HR department's production account will not prevent other departments from sharing the RI discounts.

In B, Removing the HR department's production AWS account from the organization may cause issues in consolidated billing and it does not prevent other departments from sharing the RI discounts.

In D, Creating an SCP in the organization to restrict access to the RIs is not necessary because the management account can directly turn off the RI sharing, it also does not prevent other departments from sharing the RI discounts.

upvoted 3 times

Question #109

Topic 1

A large company is running a popular web application. The application runs on several Amazon EC2 Linux instances in an Auto Scaling group in a private subnet. An Application Load Balancer is targeting the instances in the Auto Scaling group in the private subnet. AWS Systems Manager Session Manager is configured, and AWS Systems Manager Agent is running on all the EC2 instances.

The company recently released a new version of the application. Some EC2 instances are now being marked as unhealthy and are being terminated. As a result, the application is running at reduced capacity. A solutions architect tries to determine the root cause by analyzing Amazon CloudWatch logs that are collected from the application, but the logs are inconclusive.

How should the solutions architect gain access to an EC2 instance to troubleshoot the issue?

- A. Suspend the Auto Scaling group's HealthCheck scaling process. Use Session Manager to log in to an instance that is marked as unhealthy.
- B. Enable EC2 instance termination protection. Use Session Manager to log in to an instance that is marked as unhealthy.
- C. Set the termination policy to OldestInstance on the Auto Scaling group. Use Session Manager to log in to an instance that is marked as unhealthy.
- D. Suspend the Auto Scaling group's Terminate process. Use Session Manager to log in to an instance that is marked as unhealthy.

Correct Answer: D*Community vote distribution*

zozza2023 1 year, 2 months ago

Selected Answer: D

The correct answer is D.

upvoted 10 times

God_Is_Love 1 year, 1 month ago

Selected Answer: D

Disabling health check wont let SA know which instance is un healthy. So A is certainly wrong. D is correct.

upvoted 8 times

gofavad926 3 weeks, 2 days ago

Selected Answer: D

D, stop the autoscaling process

upvoted 1 times

AWSLord32 2 months, 1 week ago

Why not B? Can the ASG override the Ec2 termination protection?

upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

severlight 4 months, 3 weeks ago

Selected Answer: D

you can stop auto-scaling processes, here you need to stop termination, you need health checks to know which instance to check

upvoted 2 times

venvig 7 months, 1 week ago

Selected Answer: D

If ASG terminates the instances because they are unhealthy there is no way we can login to the instance using session manager or otherwise to investigate the problem. So, suspend the termination.

upvoted 3 times

NikkyDicky 9 months, 1 week ago

Selected Answer: D

d of course

upvoted 1 times

✉️  **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: D

keyword == Auto Scaling group's Terminate process.

upvoted 1 times

✉️  **Alando** 7 months ago

Have you cleared the exam?

upvoted 1 times

✉️  **mfsec** 1 year ago

Selected Answer: D

Suspend the Auto Scaling group's Terminate process.

upvoted 2 times

✉️  **zejou1** 1 year ago

Selected Answer: D

Amazon EC2 Auto Scaling stops marking instances unhealthy as a result of EC2 and Elastic Load Balancing health checks. Your custom health checks continue to function properly. After you suspend HealthCheck, if you need to, you can manually set the health state of instances in your group and have ReplaceUnhealthy replace them.

Suspending the Terminate process doesn't prevent the successful termination of instances using the force delete option with the delete-auto-scaling-group command.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html>

<https://docs.aws.amazon.com/systems-manager/latest/userguide/incident-manager.html>

We want the health checks to continue failing, just stop terminating to identify root cause

upvoted 4 times

✉️  **testingaws123** 1 year, 1 month ago

Selected Answer: A

Answer is A

If you do not want instances to be replaced, we recommend that you suspend the ReplaceUnhealthy and HealthCheck process for individual Auto Scaling groups. For more information, see Suspend and resume a process for an Auto Scaling group.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-health-checks.html>

upvoted 3 times

✉️  **zejou1** 1 year ago

That does not solve, it removes the healthcheck process, but also removes the ones that are being marked as unhealthy. The issue now is that one it is tagged as unhealthy they are being terminated. So, any that are already marked get terminated and you just removed the health checks to find remaining. you can't troubleshoot what you don't know.

upvoted 5 times

✉️  **masetromain** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/51249-exam-aws-certified-solutions-architect-professional-topic-1/>

The correct answer is D.

In this solution, the architect can suspend the Auto Scaling group's Terminate process, which will prevent the instances marked as unhealthy from being terminated. This will allow the architect to log in to the instance using Session Manager and troubleshoot the issue without losing access to the instance.

upvoted 5 times

✉️  **masetromain** 1 year, 2 months ago

Option A is incorrect because suspending the HealthCheck scaling process will not prevent instances from being terminated.

Option B is incorrect because enabling EC2 instance termination protection will not prevent instances from being terminated by Auto Scaling group.

Option C is incorrect because setting the termination policy to OldestInstance on the Auto Scaling group will not prevent instances marked as unhealthy from being terminated.

upvoted 3 times

Question #110

Topic 1

A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.

Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage. Update the parameter as needed to add or remove accounts or OUs. Use an Amazon EventBridge rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account.
- B. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rules. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
- C. Create AWS WAF rules in the management account of the organization. Use AWS Lambda environment variables to store account numbers and OUs to manage. Update environment variables as needed to add or remove accounts or OUs. Create cross-account IAM roles in member accounts. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
- D. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage. Update AWS KMS as needed to add or remove accounts or OUs. Create IAM users in member accounts. Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts.

Correct Answer: D

Community vote distribution

A (100%)

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: A

The correct answer is A.

In this solution, AWS Firewall Manager is used to manage AWS WAF rules across accounts in the organization. An AWS Systems Manager Parameter Store parameter is used to store account numbers and OUs to manage. This parameter can be updated as needed to add or remove accounts or OUs. An Amazon EventBridge rule is used to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account. This solution allows for easy management of AWS WAF rules across multiple accounts with minimal operational overhead.

upvoted 16 times

 **masetromain** 1 year, 2 months ago

Option B does not meet the requirement of being able to add or remove accounts or OUs from managed AWS WAF rule sets as needed.

Option C is not the best approach as it requires manual configuration of the cross-account IAM roles and assume-role calls in the Lambda function, increasing the operational overhead.

Option D does not meet the requirement of providing a centralized management console to manage the WAF rules across multiple accounts.

upvoted 3 times

 **Untamables** Highly Voted 1 year, 2 months ago

Selected Answer: A

<https://aws.amazon.com/solutions/implementations/automations-for-aws-firewall-manager/>

upvoted 6 times

 **career360guru** Most Recent 3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **venvig** 7 months, 1 week ago

Selected Answer: A

AWS Firewall Manager is a security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations

Firewall Manager supports wide variety of services, including:

- AWS WAF
- VPC Security Groups
- AWS Network Firewall
- Route53 DNS Firewall
- AWS Shield Advanced
- Palo Alto Cloud Next-generation firewalls

The Prerequisites are: AWS Organizations + AWS Config.

upvoted 4 times

✉ **CuteRunRun** 7 months, 4 weeks ago

Selected Answer: A

I have to say A is right.

please take a look at this:

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/>

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A is a good option

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: A

keyword == AWS Firewall Manager

upvoted 2 times

✉ **tromyunpak** 10 months, 1 week ago

the correct answer is A <https://docs.aws.amazon.com/solutions/latest/automations-for-aws-firewall-manager/architecture-overview.html>

upvoted 2 times

✉ **rbm2023** 11 months ago

Selected Answer: A

This is a complex question. But I voted A because the Firewall manager seems to be the correct way to centralize the rules across accounts.

Below are some interesting references I could find

<https://catalog.us-east-1.prod.workshops.aws/workshops/4cbaea3b-ceba-48e3-bd56-eca138f7a66c/en-US>

<https://aws.amazon.com/blogs/security/use-aws-firewall-manager-vpc-security-groups-to-protect-applications-hosted-on-ec2-instances/>

<https://aws.amazon.com/blogs/security/automatically-updating-aws-waf-rule-in-real-time-using-amazon-eventbridge/>

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: A

Use AWS Firewall Manager to manage AWS WAF rules

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

Not D, KMS to store account numbers ?

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: A

The correct answer is A.

upvoted 2 times

Question #111

Topic 1

A solutions architect is auditing the security setup of an AWS Lambda function for a company. The Lambda function retrieves the latest changes from an Amazon Aurora database. The Lambda function and the database run in the same VPC. Lambda environment variables are providing the database credentials to the Lambda function.

The Lambda function aggregates data and makes the data available in an Amazon S3 bucket that is configured for server-side encryption with AWS KMS managed encryption keys (SSE-KMS). The data must not travel across the Internet. If any database credentials become compromised, the company needs a solution that minimizes the impact of the compromise.

What should the solutions architect recommend to meet these requirements?

- A. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- B. Enable IAM database authentication on the Aurora DB cluster. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication. Enforce HTTPS on the connection to Amazon S3 during data transfers.
- C. Save the database credentials in AWS Systems Manager Parameter Store. Set up password rotation on the credentials in Parameter Store. Change the IAM role for the Lambda function to allow the function to access Parameter Store. Modify the Lambda function to retrieve the credentials from Parameter Store. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- D. Save the database credentials in AWS Secrets Manager. Set up password rotation on the credentials in Secrets Manager. Change the IAM role for the Lambda function to allow the function to access Secrets Manager. Modify the Lambda function to retrieve the credentials from Secrets Manager. Enforce HTTPS on the connection to Amazon S3 during data transfers.

Correct Answer: D

Community vote distribution

A (85%) D (15%)

✉  **zozza2023**  1 year, 2 months ago

Selected Answer: A

a little bit confused between A and D but as said by others members D doesn't address the question of "data must not travel across the Internet" ==> A is the answer

upvoted 15 times

✉  **AWSPro1234**  1 week, 5 days ago

Selected Answer: A

Key is data must not travel across the internet mean use VPC gateway

upvoted 1 times

✉  **gofavad926** 3 weeks, 2 days ago

Selected Answer: A

A, "data must not travel across the internet". This setup ensures internal network use only, meeting the security and networking requirements efficiently

upvoted 1 times

✉  **a54b16f** 1 month, 1 week ago

Selected Answer: A

The data must not travel across the Internet.

upvoted 2 times

✉  **8608f25** 1 month, 3 weeks ago

Selected Answer: D

Option D offers a comprehensive solution by leveraging AWS Secrets Manager for storing and automatically rotating database credentials, which directly addresses the concern of minimizing the impact if credentials become compromised. Changing the Lambda function to retrieve credentials from Secrets Manager enhances security by not storing credentials within environment variables. Enforcing HTTPS for S3 data transfers ensures the data in transit is encrypted. While deploying a gateway VPC endpoint for S3 (as mentioned in other options) is a best practice to keep traffic within the AWS network, enforcing HTTPS also contributes to securing data transfers without explicitly stating the need to avoid Internet travel. Secrets Manager inherently provides secure access to secrets without needing to travel across the Internet when accessed from AWS services within the same region.

Option A does not address the requirement for securing and rotating database credentials stored as Lambda environment variables.

upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: A

Answer is A as S3 VPC endpoint is needed to avoid data going over internet.

upvoted 1 times

task_7 6 months, 2 weeks ago

Selected Answer: D

AWS Secrets Manager is meant for this job, why go with any other option

upvoted 1 times

task_7 6 months, 2 weeks ago

My bad its A

D is not addressing this point

The data must not travel across the Internet

upvoted 6 times

CuteRunRun 7 months, 4 weeks ago

I prefer A

upvoted 2 times

Jonalb 8 months, 2 weeks ago

Selected Answer: A

A

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

upvoted 3 times

Jonalb 9 months, 1 week ago

Selected Answer: D

https://docs.aws.amazon.com/pt_br/secretsmanager/latest/userguide/vpc-endpoint-overview.html

upvoted 1 times

NikkyDicky 9 months, 1 week ago

Selected Answer: A

A for sure

upvoted 1 times

rbm2023 11 months ago

Selected Answer: A

I was about to chose D however just enforcing the HTTP will not avoid the data to travel across internet. You will need the option where the gateway VPC endpoint is deployed for access the S3. The answer is A.

A will also solve the issue related to authenticate the lambda to aurora without needing to store passwords, refer to -

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

upvoted 1 times

OCHT 11 months, 2 weeks ago

Selected Answer: D

However, Option A is not the best choice for the given scenario because:

It doesn't address the requirement to minimize the impact of compromised database credentials. IAM database authentication eliminates traditional user credentials, but it doesn't implement password rotation for the remaining IAM credentials.

While the VPC endpoint keeps traffic within the AWS network, it doesn't enforce encryption during data transfers to Amazon S3.

Option D, on the other hand, addresses both the requirement of minimizing the impact of compromised credentials through password rotation using AWS Secrets Manager and ensuring encrypted data transfers to Amazon S3 by enforcing HTTPS. That's why Option D is the better choice for this scenario.

upvoted 2 times

rbm2023 11 months ago

I was also choosing D however just enforcing the HTTP will not avoid the data to travel across internet. You will need the option where the gateway VPC endpoint is deployed for access the S3. The answer is A

upvoted 3 times

MikelH93 11 months, 3 weeks ago

Selected Answer: A

B and D are out because you need the VPC endpoints.

C is out because you cannot enable rotation in Parameter Store

(https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_parameterstore.html)

upvoted 4 times

mfsec 1 year ago

Selected Answer: A

A for sure due to VPC endpoints.

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: A

I had a strong opinion about D but after reading and doing some research convience about A

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

upvoted 3 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

Key is - Data must not travel on the internet. Only S3 VPC Endpoints have this feature.

A VPC endpoint allows you to connect privately to S3 from within your Amazon Virtual Private Cloud (VPC) without the need for an internet gateway, NAT device, or VPN connection. Instead, the endpoint provides a direct and secure connection between your VPC and S3 over the Amazon network backbone.

upvoted 4 times

Question #112

Topic 1

A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework.

While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types.

The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch.

Which solution will meet these requirements?

- A. Create a desired-instance-type managed rule in AWS Config. Configure the rule with the instance types that are allowed. Attach the rule to an event to run each time a new EC2 instance is launched.
- B. In the EC2 console, create a launch template that specifies the instance types that are allowed. Assign the launch template to the developers' IAM accounts.
- C. Create a new IAM policy. Specify the instance types that are allowed. Attach the policy to an IAM group that contains the IAM accounts for the developers
- D. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

Correct Answer: C

Community vote distribution

C (100%)

✉  **masetromain**  1 year, 2 months ago

Selected Answer: C

The correct answer is C.

In this solution, a new IAM policy is created that specifies the allowed instance types. This policy is then attached to an IAM group that contains the IAM accounts for the developers. This will ensure that the developers can only launch instances of the specified types, thus limiting the costs associated with the creation and termination of large instances.

upvoted 14 times

✉  **masetromain** 1 year, 2 months ago

A. Creating a desired-instance-type managed rule in AWS Config is not a sufficient solution, as it only identifies when an instance is launched with an unauthorized type, it does not prevent it.

B. Creating a launch template that specifies the instance types that are allowed is not a sufficient solution, because it limits the instances types that can be launched in the EC2 console, but it does not prevent the launch of instances through the AWS SDK, AWS CLI, or other AWS services.

D. Using EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image is not a direct solution to the problem of limiting the instance types that only the developers can launch. It can be useful for creating standardize images for the developers, but it does not provide the necessary control mechanism to limit the instance types.

upvoted 8 times

✉  **gagol14**  2 months, 2 weeks ago

Selected Answer: C

```
{
  "Sid": "limitedSize",
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:instance/*",
  "Condition": {
    "ForAnyValue:StringNotLike": {
      "ec2:InstanceType": [
        "*.nano",
        "*.small",
        "*.micro",
        "*.medium"
      ]
    }
  }
}
```

```
}
```

upvoted 4 times

✉ **cox1960** 2 months, 3 weeks ago

"an IAM group that contains the IAM accounts" ???

upvoted 1 times

✉ **igor12ghsj577** 2 months, 2 weeks ago

yes, in IAM group you have user IAM accounts.

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

Its a C

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

Selected Answer: C

The only technical achievable choices are A and C. However A will only identify the issue and will not prevent it. Even if we set up a remediation rule to terminate the instances immediately - that will cause more issues for the developers and unclear signals that something is wrong with the testing. So A remains the only possible option.

upvoted 2 times

✉ **Parimal1983** 9 months, 2 weeks ago

C is the correct solution remained. Typo mistake in the comments.

upvoted 1 times

✉ **easystoo** 9 months, 3 weeks ago

C-C-C-C-C-CC-C-C-CC-C-C-C-CC-

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: C

IAM policy..

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: C

answer is C

upvoted 3 times

Question #113

Topic 1

A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.

Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Choose three.)

- A. Create an AWS Config rule in each account to find resources with missing tags.
- B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

Correct Answer: CDE

Community vote distribution



✉ **gofavad926** 3 weeks, 2 days ago

Selected Answer: ABE

ABE, SCP + Config + Config Aggregator

upvoted 1 times

✉ **Dgix** 1 month ago

Selected Answer: BE

B and E handle the requirements in a centralised manner, giving least operational overhead, without anything needing to be added. The question is plainly wrongly stated. If three options have to be selected, then A is the least absurd one.

upvoted 2 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: ABE

A. Create an AWS Config rule in each account to find resources with missing tags. AWS Config can evaluate the configuration of your AWS resources and identify resources that do not comply with specified requirements, such as missing specific tags. This helps in identifying existing resources with the issue.
 B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing. Service Control Policies (SCPs) can enforce permissions across all accounts in an organization. By creating an SCP that denies launching EC2 instances without the required Project tag, you can prevent the problem from occurring in the future at the organization level.
 E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag. An AWS Config aggregator can aggregate compliance data from multiple accounts and regions. This allows for centralized visibility of instances lacking the required tags, making it easier to address and resolve the issue across the entire organization.

upvoted 2 times

✉ **AWSLord32** 2 months, 1 week ago

Selected Answer: BDE

A is not needed if you have D. Correct answer is BDE.

upvoted 1 times

✉ **AWSLord32** 2 months, 1 week ago

I meant E, not D

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

It is not D. Create an IAM policy in each account with a deny action for ec2:RunInstances if the Project tag is missing. IAM policies do not directly support conditional denies based on tag presence during the resource creation process in the same way SCFs do. This enforcement is better handled at the organization level with SCPs.

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: ABE

Option A, B and E

upvoted 1 times

✉ **Sandeep_B** 5 months, 2 weeks ago

Selected Answer: ABE

Inspector checks for Vulnerabilities but not the tags.

upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: ABE

its ABE

upvoted 2 times

 **youngmanaws** 11 months, 3 weeks ago

A. AWS Config allows you to remediate noncompliant resources that are evaluated by AWS Config Rules. AWS Config applies remediation using AWS Systems Manager Automation documents. These documents define the actions to be performed on noncompliant AWS resources evaluated by AWS Config Rules. You can associate SSM documents by using AWS Management Console or by using APIs.

AWS Config provides a set of managed automation documents with remediation actions. You can also create and associate custom automation documents with AWS Config rules.

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions using SSM documents. AWS Config provides a recommended list of remediation action in the AWS Management Console.

In the AWS Management Console, you can either choose to manually or automatically remediate noncompliant resources by associating remediation actions with AWS Config rules. With all remediation actions, you can either choose manual or automatic remediation.

upvoted 3 times

 **OCHT** 1 year ago

Selected Answer: ABE

A. Create an AWS Config rule in each account to find resources with missing tags.

By creating an AWS Config rule in each account, you can check if resources are missing tags or have tags that are not conforming to your organization's standards. You can also use AWS Config to automatically remediate non-compliant resources by applying tags. This can help ensure that resources are properly tagged for cost allocation purposes. Here is the AWS Config documentation for creating rules:

https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html

upvoted 4 times

 **OCHT** 1 year ago

E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.

By creating an AWS Config aggregator, you can collect a list of EC2 instances across multiple accounts in the organization that are missing the required Project tag. This can help you identify instances that need to be tagged properly for cost allocation. Here is the AWS Config documentation for creating aggregators:

<https://docs.aws.amazon.com/config/latest/developerguide/config-aggregator.html>

upvoted 6 times

 **AWSLord32** 2 months, 1 week ago

So what is the point of having A if you have E at an Org level?

upvoted 2 times

 **OCHT** 1 year ago

B. Create an SCP in the organization with a deny action for ec2:RunInstances if the Project tag is missing.

By creating a Service Control Policy (SCP) in the organization, you can enforce a deny action for EC2 instances that do not have the required Project tag. This can prevent users from launching instances that are not tagged correctly and ensure that new instances are tagged properly for cost allocation. Here is the AWS Organizations documentation for creating SCPs:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

upvoted 5 times

 **mfsec** 1 year ago

Selected Answer: ABE

ABE is the better choice

upvoted 1 times

 **Damijo** 1 year ago

what's the value of A and E together- it's either or ? the outcome is the same - thoughts?

upvoted 4 times

 **AWSLord32** 2 months, 1 week ago

Fully agree, BDE

upvoted 1 times

 **AWSLord32** 2 months, 1 week ago

Did some research..

Aggregators provide a read-only view into the source accounts and regions that the aggregator is authorized to view. Aggregators do not provide mutating access into the source account or region. For example, this means that you cannot deploy rules through an aggregator or pull snapshot files from the source account or region through an aggregator.

<https://docs.aws.amazon.com/config/latest/developerguide/config-concepts.html#multi-account-multi-region-data-aggregation>

So ABE seems correct

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: ABE

If config rule is added (A) it can be seen in AWS Config aggregator (E) Using SCP in as aws organization is used here in question. So, A,B,E
upvoted 4 times

 **God_Is_Love** 1 year, 1 month ago

If there are no organizations used, D can be used to prevent EC2 run instances too,
C is for vulnerabilities checking..F for all security issues consolidated..

upvoted 2 times

 **jaysparky** 1 year, 1 month ago

ABE makes sense

upvoted 1 times

 **spd** 1 year, 1 month ago

Selected Answer: ABE

Config, SCP and IAM policy may not require in each account but it says to select three options so going with ABE

upvoted 1 times

 **Musk** 1 year, 2 months ago

Selected Answer: AE

BE makes sense

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: ABE

the best way to deploy config rules accross accounts= SCP

upvoted 2 times

 **masssa** 1 year, 2 months ago

Selected Answer: ABE

In adding tag, the keywords are config, scp, aggregator.

upvoted 2 times

Question #114

Topic 1

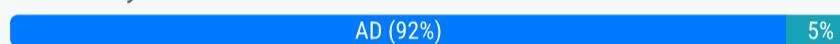
A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events. The database is unable to scale due to heavy ingestion and it frequently runs out of storage.

The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:

- Managed AWS services to minimize operational complexity.
- A buffer that automatically scales to match the throughput of data and requires no ongoing administration.
- A visualization tool to create dashboards to observe events in near-real time.
- Support for semi-structured JSON data and dynamic schemas.

Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.
- B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.
- D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.
- E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

Correct Answer: AD
Community vote distribution


God_Is_Love Highly Voted 1 year, 1 month ago

Selected Answer: AD

Amazon Kinesis Data Firehose (A) allows you to buffer events in two ways: through buffering size or buffering time. With buffering size, you can configure the maximum size of the buffer in MB or the maximum number of records in the buffer. Once the buffer is full, it will automatically deliver the data to the destination.

Amazon ES (D) has its ability to receive events from various sources in real-time. Amazon ES can ingest data from a variety of sources, such as Amazon Kinesis Data Firehose, Amazon CloudWatch Logs, and Amazon S3, making it a powerful tool for organizations looking to analyze and visualize real-time streaming data. (Kibana dashboards)

upvoted 13 times

OCHT Highly Voted 1 year ago

Selected Answer: AD

Option B includes using an Amazon Kinesis data stream to buffer events, which is a valid solution for a streaming data use case. However, it requires more ongoing administration compared to using Amazon Kinesis Data Firehose, which is a fully managed service. Additionally, the use of Amazon Kinesis Data Firehose allows the company to take advantage of built-in data transformation and processing capabilities, which can reduce the amount of code required to implement the solution. Therefore, I selected option A over option B as it better meets the requirement of minimizing operational complexity.

upvoted 11 times

TonytheTiger Most Recent 5 days, 10 hours ago

Selected Answer: AD

Option A NOT Option B - Amazon Data Firehose buffers incoming streaming data in memory to a certain size (buffering size) and for a certain period of time (buffering interval) before delivering it to the specified destinations.

<https://docs.aws.amazon.com/firehose/latest/dev/buffering-hints.html>

upvoted 1 times

Dgix 4 weeks ago

Selected Answer: AD

On second thought: A because B requires manual shard configuration.

upvoted 1 times

Dgix 4 weeks ago

Selected Answer: BE

Also, Streams is more real-time.

upvoted 1 times

✉ **Dgix** 4 weeks ago

Selected Answer: BD

B rather than A because B integrates the lambda functionality for transformation of the data, which must be done as an added step in A, thereby increasing operational overhead.

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

Selected Answer: AD

A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events. Amazon Kinesis Data Firehose provides a fully managed service for effortlessly loading streaming data into AWS services such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. It scales automatically to match the throughput of data and requires no ongoing administration. AWS Lambda can be used in conjunction with Kinesis Data Firehose to process and transform the data before it's loaded into the destination, supporting dynamic schemas and semi-structured JSON data. Additionally, Amazon Kinesis Data Firehose has built-in buffering capabilities and can be used to observe events in near-real time, making it a more appropriate choice for the given scenario.

upvoted 1 times

✉ **8608f25** 1 month, 3 weeks ago

D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards. Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time. Kibana is an open-source visualization tool designed to work with Elasticsearch, providing powerful and easy-to-use features to create dashboards that can visualize data in near-real-time.

upvoted 1 times

✉ **AimarLeo** 2 months, 1 week ago

ElasticSearch is the ex name of new OpenSearch

upvoted 1 times

✉ **ninomfr64** 2 months, 3 weeks ago

Selected Answer: BD

I choose Data Stream (KDS) over Data Firehose (KDF) in this scenario:

- KDS allows to you store events up to 1 year, allowing to achieve buffering with no constraints on size and with a very large time limit. KDS support on-demand capacity mode
- KDF transport mechanism is based on buffering, but here buffering is limited on size (max 128MiB) and time (up to 900 sec)

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

✉ **AMohanty** 7 months, 1 week ago

BD

Question states near-Real time

Thats the differentiating factor between Kinesis data stream and Firehose

I would go for B and D

upvoted 2 times

✉ **chikorita** 7 months ago

but about "• Managed AWS services to minimize operational complexity."

i believe Kinesis Firehose is managed solution whereas DataStream required operational overhead

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: AD

AD for unstructured data

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: AD

AD is my vote

upvoted 1 times

✉ **Zek** 1 year, 1 month ago

A,D seem correct. <https://www.examtopics.com/discussions/amazon/view/47625-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

✉ **zhangyu20000** 1 year, 2 months ago

AD are correct

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: AD

The combination of components that will enable the company to create a monitoring solution that will satisfy these requirements is:

A. Use Amazon Kinesis Data Firehose to buffer events. This service can automatically scale to match the throughput of data, and it requires no ongoing administration. With Firehose, it's possible to use a Lambda function to process and transform events as well as to store them in other services like S3 or Redshift.

D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. With Amazon Elasticsearch Service, it's possible to create an index for the events, making them searchable and queryable. This service is a fully managed service so it minimizes operational complexity. Also, it's possible to use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.

upvoted 6 times

 **masetromain** 1 year, 2 months ago

Option B: Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events. is incorrect because Kinesis Data Stream is a different service than Kinesis Data Firehose and does not have the buffer feature.

Option C: Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards. is incorrect because Amazon Aurora is a relational database service and does not support JSON data or dynamic schemas.

Option E: Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards. is incorrect because Amazon Neptune is a graph database service and does not support JSON data or dynamic schemas.

upvoted 3 times

 **Sarutobi** 1 year, 1 month ago

We use the Kinesis data stream specifically for its capability to store data "aka buffer events". Firehouse also has some resemblance of this feature but is more of a transportation service.

upvoted 3 times

 **jpa8300** 3 months ago

What does it mean? You choose Kinesis data stream over Forehose?

upvoted 1 times

Question #115

Topic 1

A team collects and routes behavioral data for an entire company. The company runs a Multi-AZ VPC environment with public subnets, private subnets, and an internet gateway. Each public subnet also contains a NAT gateway. Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads run in private subnets.

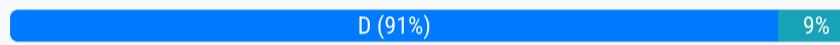
A solutions architect must review the infrastructure. The solution architect needs to reduce costs and maintain the function of the applications. The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high. A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

What should the solutions architect do to meet these requirements?

- A. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

Correct Answer: D

Community vote distribution



≡ **God_Is_Love** Highly Voted 1 year, 1 month ago

Selected Answer: D

VPC endpoints to mitigate NAT gateway huge data transfer costs especially in Kinesis usecase where large data is passed thru

With a VPC endpoint policy, you can define rules to control access to the VPC endpoint. You can specify the source IP address or IP address range that is allowed to access the endpoint, as well as the type of traffic that is allowed, such as HTTP, HTTPS, or custom TCP ports. You can also specify the resources that can be accessed through the VPC endpoint, such as an Amazon S3 bucket or an Amazon DynamoDB table.

upvoted 11 times

≡ **Maria2023** Highly Voted 9 months, 3 weeks ago

Selected Answer: D

B is a distractor. You don't need IAM permissions to use a service via an endpoint. You only need to set up proper routing to that endpoint

upvoted 5 times

≡ **gofavad926** Most Recent 3 weeks, 2 days ago

Selected Answer: D

D, VPC endpoint

upvoted 1 times

≡ **gofavad926** 3 weeks, 2 days ago

Selected Answer: D

D, VPC endpoint

upvoted 1 times

≡ **career360guru** 3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

≡ **rif** 5 months, 3 weeks ago

Answer is D.

An endpoint policy is a resource-based policy that you attach to a VPC endpoint to control which AWS principals can use the endpoint to access an AWS service.

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html>

upvoted 1 times

≡ **NikkyDicky** 9 months ago

Selected Answer: D

It's a d

upvoted 1 times

 SkyZeroZx 9 months, 3 weeks ago**Selected Answer: D**

reduce cost == interface VPC endpoint

upvoted 2 times

 SkyZeroZx 9 months, 3 weeks ago

A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.

upvoted 1 times

 Anonymous9999 11 months, 3 weeks ago**Selected Answer: D**

D is the answer.

It's not B because user's/applications doesn't need permissions to use an endpoint:

https://docs.aws.amazon.com/vpc/latest/privatelink/security_iam_id-based-policy-examples.html

upvoted 2 times

 romiao106 10 months, 3 weeks ago

No. in your document it says "By default, users and roles don't have permission to create or modify AWS PrivateLink resources". Users and roles don't have permissions so they do need permissions to use an interface endpoint

upvoted 1 times

 mfsec 1 year ago**Selected Answer: D**

D is the best choice.

upvoted 1 times

 Sarutobi 1 year, 1 month ago

If this is a cost-saving question is very hard to answer, you pay for both, and depending on the region one can be cheaper than the other. There is a cost for a NAT GW and also for a VPC endpoint per AZ plus the traffic you generate over them. In my experience, because you need a VPC endpoint for each service NAT-GW is cheaper.

upvoted 1 times

 c73bf38 1 year, 1 month ago**Selected Answer: D**

Allowing traffic from the application using the VPC endpoint is key to bypassing NAT Gateway.

upvoted 3 times

 moota 1 year, 1 month ago**Selected Answer: D**

Which is which?

A VPC endpoint policy is an IAM resource policy that you attach to a VPC endpoint. It determines which principals can use the VPC endpoint to access the endpoint service. The default VPC endpoint policy allows all actions by all principals on all resources over the VPC endpoint.

<https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html#vpc-endpoints-policies>

upvoted 1 times

 Musk 1 year, 2 months ago**Selected Answer: B**

B seems correct too.

upvoted 3 times

 zhangyu20000 1 year, 2 months ago

D: by pass internet to save cost on NAT GW

upvoted 1 times

 masetromain 1 year, 2 months ago**Selected Answer: D**

The correct answer is D. Adding an interface VPC endpoint for Kinesis Data Streams to the VPC will allow the applications to access the service without the need for a NAT gateway. This will reduce the cost associated with NatGateway-Bytes charges, which are increasing the cost in the EC2-Other category.

Option A is not correct because enabling VPC Flow Logs and reviewing the logs for traffic that can be removed is not a direct solution for reducing NatGateway-Bytes charges. Additionally, security groups are used to control access to resources, not to optimize network traffic.

upvoted 3 times

 masetromain 1 year, 2 months ago

Option B is not correct because it does not address the specific issue of high NatGateway-Bytes charges. Additionally, ensuring that applications have the correct IAM permissions is a best practice but it is not directly related to reducing costs.

Option C is not correct because while reviewing Detective findings for traffic that is not related to Kinesis Data Streams can help identify potential issues, it does not directly address the issue of high NatGateway-Bytes charges. Additionally, Configuring security groups to block that traffic is not a solution for reducing costs associated with NatGateway-Bytes charges.

upvoted 3 times

Question #116

Topic 1

A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network.

The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region.

Which solution will meet these requirements?

- A. Create a private VIF from the DX-A connection into a Direct Connect gateway. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.
- B. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Associate the eu-west-1 transit gateway with this Direct Connect gateway. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway. Associate the us-east-1 transit gateway with this separate Direct Connect gateway. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
- C. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Configure the Direct Connect gateway to route traffic between the transit gateways.
- D. Create a transit VIF from the DX-A connection into a Direct Connect gateway. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway. Peer the transit gateways with each other to support cross-Region routing.

Correct Answer: A

Community vote distribution



God_Is_Love Highly Voted 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/images/whitepapers/latest/hybrid-connectivity/images/dx-dxgw-transit-gateway-multi-region-public-vif.png>
 B is wrong as it says, two DX Gateways contradictory
 C is wrong as it says to configure DXG to route traffic. infact Transit gateway peering need to be done between two transit gateways of each region.
 A is wrong because Private VIF is not apt in mentioned config of the question. Public VIF is correct (Transit public VIF)
 If you are using a single DX Gateway
 upvoted 11 times

God_Is_Love 1 year, 1 month ago

Whichever option has this text is correct - "Peer the transit gateways with each other to support cross-Region routing"
 upvoted 3 times

Dgix Most Recent 2 weeks, 5 days ago

Selected Answer: D

Don't let "No single points of failure can exist on the network" mislead you into thinking that you need two DCGWs. DCGWs are not part of the region they connect to. Therefore, no SPOF translates to a double DC connection to a single DCGW. Hence, D.
 upvoted 1 times

gofavad926 3 weeks, 2 days ago

Selected Answer: D

D, this approach ensures high availability and robust network connectivity across the specified AWS regions and the on-premises data center.
 upvoted 1 times

Jassybanga 1 month, 2 weeks ago

Answer D - As per from AWS

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-more-than-3.html>

upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: D

Choice is between C and D. Better the two D is the right option.

upvoted 1 times

subupro 4 months ago

D is correct ref architecture <https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

upvoted 3 times

shaaam80 4 months, 1 week ago

Selected Answer: D

Answer D. Peer the transit gateways for cross-region routing.

upvoted 1 times

severlight 4 months, 3 weeks ago

Selected Answer: D

to connect to transit gateways through the dx gateway you should use transit VIF

upvoted 1 times

frfavoredo 7 months, 1 week ago

I agree 'D' is a good answer to the problem, but isn't the DXGW a single point of failure?

Question says "No single points of failure can exist on the network."

upvoted 2 times

NikkyDicky 9 months, 1 week ago

Selected Answer: D

it's D

upvoted 1 times

happystrawberry 10 months, 3 weeks ago

Would it be C for the answer? A Direct Connect gateway supports communication between attached transit virtual interfaces and associated transit gateways only and may enable a virtual private gateway to another virtual private gateway.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html>

upvoted 1 times

happystrawberry 10 months, 3 weeks ago

Actually, D is a proper answer.

upvoted 1 times

rbm2023 10 months, 4 weeks ago

Selected Answer: D

I agree with option D

Refer to the diagram below which explains in detail the use of Transit VIF and Public VIF. Also demonstrates the necessity for peering the transit gateways to allow the cross-region routing.

<https://docs.aws.amazon.com/images/whitepapers/latest/hybrid-connectivity/images/dx-dxgw-transit-gateway-multi-region-public-vif.png>

The only options that are using the cross-region routing are A and D. Option A mentions the use of Private VIF and not the Transit VIF. Hence A is incorrect.

upvoted 4 times

rbm2023 10 months, 4 weeks ago

Refer to the following article

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

upvoted 3 times

dev112233xx 1 year ago

Selected Answer: D

Transit VIF required to connect to Transit Gateway, and Transit peering is required to connect multi regions...

Here is the full diagram:

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

upvoted 3 times

mfsec 1 year ago

Selected Answer: D

D is the answer

upvoted 2 times

zejou1 1 year ago

Selected Answer: D

This model is constructed of the following:

- Multi AWS Regions

- Dual Direct Connect connections to independent DX locations
- Single on-premises data center with dual connections to AWS
- AWS DXGW with AWS Transit Gateway
- High scale of VPCs per Region

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-and-aws-public-peering.html>

upvoted 2 times

 **Sarutobi** 1 year, 1 month ago

Selected Answer: D

Yeah, a single DX-GW tied to TGW on different regions that further connect to the VPCs on those regions.

upvoted 2 times

 **Yowie351** 1 year, 1 month ago

Selected Answer: B

Multiple dynamically routed AWS Direct Connect connections are necessary to support high availability.

Refer to the second diagram:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html>

upvoted 1 times

Question #117

Topic 1

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- D. Invoke an AWS Step Functions state machine to remove access.
- E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- F. Use Amazon Pinpoint to notify the security team.

Correct Answer: ADE

Community vote distribution



✉️ **God_Is_Love** Highly Voted 1 year, 1 month ago

Selected Answer: ADE

Event Bus (EventBridge) system to receive event notification (Option A). Step function can get triggered with workflow of doing steps like removing access and sending email etc..(Option D, E)

EventBridge enables you to create event rules that match events from different sources, such as AWS services, SaaS applications, custom applications, and other AWS accounts. Once an event rule is triggered, EventBridge can route the event to one or more targets, such as AWS Lambda functions, Amazon SNS topics, Amazon SQS queues, or custom HTTP endpoints.

AWS Step Functions supports several AWS services, such as AWS Lambda, Amazon Simple Notification Service (SNS), and Amazon Simple Queue Service (SQS). You can use these services to trigger actions and pass data between steps in your state machine.

Pinpoint is chat system which question did not ask, F is wrong. Not C as
upvoted 12 times

✉️ **Jay_2pt0_1** 11 months, 1 week ago

I agree with this.
upvoted 1 times

✉️ **hobokabobo** 1 year ago

this explanation makes sense to me.
upvoted 1 times

✉️ **TonytheTiger** Most Recent 5 days, 9 hours ago

Selected Answer: ACE

Option ADE: Most people agree with option AE. There can be situations where human intervention is required before the workflow can progress. For example, approving a substantial credit increase may require human approval

<https://docs.aws.amazon.com/step-functions/latest/dg/use-cases-security-automation.html>
upvoted 1 times

✉️ **24Gel** 3 weeks, 2 days ago

Why not BCE? or ACE?

How to use Step Function to remove permission?
upvoted 1 times

✉️ **dankositze** 1 month, 4 weeks ago

Poorly constructed answer choices, but ADE is the least worst option.
upvoted 1 times

✉️ **zanhsieh** 2 months ago

Selected Answer: ADE

I picked ADE. EventBridge, Lambda / Step Function, and SNS are required.
BDE: No. CloudTrail can't trigger Step Function directly.

ABE: No. This solution can't remove the user access automatically.

Choosing B alone without A can't directly trigger Lambda / Step functions to remove the user access. C can't compare with D. F is not relevant.

upvoted 1 times

✉ **AWSLord32** 2 months, 1 week ago

Selected Answer: BDE

Eventbridge is not needed. Cloudtrail can send notifications to SNS directly

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 2 times

✉ **AWSLord32** 2 months, 1 week ago

Also, if you select ADE how would the event ever trigger SNS to send the notification?

upvoted 2 times

✉ **bjexamprep** 2 months, 2 weeks ago

Selected Answer: ACE

Step function is a process/workflow orchestrator. Usually process/workflow orchestrator doesn't do actual task, cause the objective of a orchestrator is to maintain the stage of a process/workflow. Instead, the orchestrator call a service to complete the task and update the stage. So the task of removing access should be done by a Lambda function. Since lambda function is not an option, the only applicable option is C, while ECS introduces too much administration overhead, and is a very bad choice for this task.

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: ADE

A, D and E

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: ADE

ADE. have to assume the step function calls lambda or some such to actually perform action

upvoted 1 times

✉ **Maria2023** 10 months, 3 weeks ago

Selected Answer: ADE

I've chosen the EventBridge option (A) because I really was not able to find a way to set Cloudtrail to trigger SNS on its own. The rest 2 are common sense

upvoted 1 times

✉ **AWSLord32** 2 months, 1 week ago

Here you go <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 1 times

✉ **OCHT** 1 year ago

Selected Answer: ABE

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.

B. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.

E. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.

upvoted 2 times

✉ **OCHT** 1 year ago

By creating an Amazon EventBridge rule, the company can detect the CreateUser event in CloudTrail and use it to trigger actions such as sending notifications or invoking AWS Lambda functions.

Configuring CloudTrail to send a notification for the CreateUser event to an Amazon SNS topic allows the security team to receive a notification whenever a new IAM user is created.

Using Amazon SNS, the security team can receive the notification and approve or deny the new IAM user creation. If the security team denies the creation, access can be automatically removed using AWS Lambda or AWS Step Functions.

Therefore, these three steps will allow the company to meet its requirements for user creation approval and access removal.

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: ADE

ADE is right

upvoted 1 times

✉ **[Removed]** 1 year, 1 month ago

Selected Answer: ADE

ADE Step Functions works.

upvoted 1 times

 **Musk** 1 year, 2 months ago

Selected Answer: ACE

I like ACE better. I am not sure Step Functions would work.

upvoted 1 times

 **moota** 1 year, 1 month ago

According to ChatGPT, AWS Step Functions can interact with AWS APIs in a few different ways. One example is below.

Directly invoking AWS APIs using the "Task" state in Step Functions. This state type allows you to run an AWS Lambda function, which can interact with AWS APIs as part of its logic.

upvoted 1 times

 **zhangyu20000** 1 year, 2 months ago

ADE are correct

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: ADE

This is the correct answer because it follows these steps:

- A: The first step is to create an EventBridge rule that listens for the specific API call to create a new IAM user. This will trigger the next step in the process.

- D: The next step is to use an AWS Step Functions state machine to remove access for the new IAM user. This ensures that access is removed automatically, as required by the security team.

- E: Finally, use Amazon SNS to notify the security team that a new user has been created and access has been removed. This allows the security team to review and approve the user as necessary.

Option B is not correct because CloudTrail alone is not able to remove access for the new user.

Option C is not correct because it is not specified in the question that the company is using Amazon Elastic Container Service and AWS Fargate technology.

Option F is not correct because the question specifies that the company should use Amazon SNS to notify the security team, not Amazon Pinpoint.

upvoted 2 times

 **hobokabobo** 1 year ago

"the question specifies that the company should use Amazon SNS " -> no, it does not specify anything like that.

"because it is not specified in the question that the company is using Amazon Elastic Container"-> so? is it specified that they use step function., can't find that either.

The question must have changed, it does not match your explanations.

upvoted 1 times

 **Jesuisleon** 10 months, 4 weeks ago

He just copied the answer from chatgpt for every question, really made me sick

upvoted 6 times

 **BabaP** 10 months, 1 week ago

it is annoying, I don't bother with reading them even if the answer they picked is correct

upvoted 3 times

Question #118

Topic 1

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups.

The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account must have connectivity to all accounts. The development account and the staging account must have access only to each other.

Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Deploy a landing zone environment by using AWS Control Tower. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- B. Enable AWS Security Hub in all accounts to manage cross-account access. Collect findings through AWS CloudTrail to force MFA login.
- C. Create transit gateways and transit gateway VPC attachments in each account. Configure appropriate route tables.
- D. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- E. Enable AWS Control Tower in all accounts to manage routing between accounts. Collect findings through AWS CloudTrail to force MFA login.
- F. Create IAM users and groups. Configure MFA for all users. Set up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts.

Correct Answer: BDF

Community vote distribution

ACD (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: ACD

The correct answer would be options A, C and D, because they address the requirements outlined in the question.

- A. Deploying a landing zone environment using AWS Control Tower and enrolling accounts in an organization in AWS Organizations allows for a centralized management of access to all accounts and applications.
- C. Creating transit gateways and transit gateway VPC attachments in each account and configuring appropriate route tables allows for private network traffic, and ensures that the production account and shared network account have connectivity to all accounts, while the development and staging accounts have access only to each other.
- D. Setting up and enabling AWS IAM Identity Center (AWS Single Sign-On) and creating appropriate permission sets with required MFA for existing accounts allows for multi-factor authentication at login and specific roles to be assigned to user groups.

upvoted 13 times

 **masetromain** 1 year, 2 months ago

The other options are not correct because:

- B. Enabling AWS Security Hub in all accounts to manage cross-account access and collecting findings through AWS CloudTrail to force MFA login is not enough to meet the requirement of creating separate accounts for development, staging, production, and shared network. It can be used in addition to the other steps, but not as a standalone solution.
- E. Enabling AWS Control Tower in all accounts to manage routing between accounts and collecting findings through AWS CloudTrail to force MFA login is not enough to meet the requirement of creating separate accounts for development, staging, production, and shared network. It can be used in addition to the other steps, but not as a standalone solution.

upvoted 3 times

 **masetromain** 1 year, 2 months ago

F. Creating IAM users and groups and configuring MFA for all users and setting up Amazon Cognito user pools and Identity pools to manage access to accounts and between accounts does not address the requirement of creating separate accounts for development, staging, production, and shared network. Additionally, it does not address the requirement of keeping the traffic on a private network.

upvoted 2 times

 **ajeeshb**  4 weeks, 1 day ago

Selected Answer: ACD

A, C and D are right answers. Option C is though not clear. Transit gateway needs to be created in shared network account and tgw vpc attachment in all accounts. But option C says "create tgw and tgw vpc attachment in all accounts", which is a bit confusing

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: ACD

A, C and D

upvoted 1 times

 **shaam80** 4 months, 1 week ago

Selected Answer: ACD

Answer - ACD

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: ACD

ACD easy

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: ACD

ACD seems like the only technically achievable solution. B and E appear to be completely wrong and for F - I am not sure whether Cognito will do the job but for sure it would be extremely hard to implement that way.

upvoted 2 times

 **OCHT** 1 year ago

Selected Answer: ACD

Option E is not the most appropriate choice because it suggests enabling AWS Control Tower in all accounts to manage routing between accounts. However, AWS Control Tower is not primarily designed for managing routing between accounts; it is intended to set up and govern a secure, multi-account AWS environment. The transit gateways and VPC attachments in Option C are better suited for managing routing and connectivity between accounts.

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: ACD

ACD are the best choice

upvoted 1 times

 **spd** 1 year, 1 month ago

Selected Answer: ACD

By Elimination Rule

upvoted 3 times

 **zhangyu20000** 1 year, 2 months ago

ACD are correct.

upvoted 3 times

Question #119

Topic 1

A company runs its application in the eu-west-1 Region and has one account for each of its environments: development, testing, and production. All the environments are running 24 hours a day, 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases. The databases are between 500 GB and 800 GB in size.

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day, 7 days a week. The company wants to reduce costs. All resources are tagged with an environment tag with either development, testing, or production as the key.

What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge rule that runs once every day. Configure the rule to invoke one AWS Lambda function that starts or stops instances based on me tag, day, and time.
- B. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that starts instances based on the tag.
- C. Create an Amazon EventBridge rule that runs every business day in the evening. Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag. Create a second EventBridge rule that runs every business day in the morning. Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
- D. Create an Amazon EventBridge rule that runs every hour. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag, day, and time.

Correct Answer: A

Community vote distribution

B (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: B

The correct answer is B. Creating an Amazon EventBridge rule that runs every business day in the evening to stop instances and another rule that runs every business day in the morning to start instances based on the tag will reduce costs with the least operational effort.

This approach allows for instances to be stopped during non-business hours when they are not in use, reducing the costs associated with running them. It also allows for instances to be started again in the morning when the development and testing teams need to use them.

Option A would require the instances to be stopped and started once a day, which could result in instances being stopped while they are in use or not being stopped when they are not in use.

Option C would terminate instances during non-business hours and restore them again in the morning, which could lead to data loss or longer start up times.

Option D would terminate or restore instances every hour, which could lead to unnecessary costs as well as data loss or longer start up times.
upvoted 9 times

 **zhangyu20000**  1 year, 2 months ago

B is correct. Stop the instance that preserves all data.

C: is incorrect because it terminates instances that will lose data

upvoted 5 times

 **rbm2023** 10 months, 4 weeks ago

with the addition to the fact that to recreate those DBs from scratch would take a long time.

upvoted 1 times

 **AWSLord32**  2 months, 1 week ago

Selected Answer: B

Voted B, but C seems to be more cost effective. Any idea to why it wouldn't work?

upvoted 1 times

 **pangchn** 1 month, 4 weeks ago

C will terminate the instance which may potentially work on the disk

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

  **NikkyDicky** 9 months, 1 week ago**Selected Answer: B**

B for sure

upvoted 1 times

  **Maria2023** 9 months, 3 weeks ago**Selected Answer: B**

A cannot complete the requirement since it runs once a day and we need to stop the non-prod instances in the evening and start them in the morning. A would potentially work if we set up the rule to run every hour and then determine the appropriate action based on the time of the day.
C and D are nonsense to me

upvoted 1 times

  **leehjworking** 10 months, 3 weeks ago

Can anyone explain why B has less operational effort than A ?

upvoted 1 times

  **chikorita** 10 months, 1 week ago

cuz we have to schedule Eventbridge to run twice a day [STOP trigger and START trigger]....Option A mentions about "ONCE" which could only be either stop or start so option B is most appropriate

upvoted 1 times

  **dev112233xx** 1 year ago**Selected Answer: B**

B is correct

The keyword here is whether you terminate or stop the instance. ofc you don't want to terminate. stop is enough and company don't pay when the instance is in stop state.

upvoted 4 times

  **mfsec** 1 year ago**Selected Answer: B**

B is the easy choice

upvoted 2 times

  **Musk** 1 year, 2 months ago**Selected Answer: B**

this is easy. I wish I'll have several of this in the exam.

upvoted 5 times

Question #120

Topic 1

A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.

The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked.

What could be the cause of the error messages for these customers?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

Correct Answer: C

Community vote distribution

C (100%)

 **sambb**  1 year, 1 month ago

Selected Answer: C

API Gateway has a limit of 10k requests per second, per account, per region
<https://docs.aws.amazon.com/apigateway/latest/developerguide/limits.html>

upvoted 9 times

 **masetromain**  1 year, 2 months ago

Selected Answer: C

The correct answer is C. The company reached its API Gateway account limit for calls per second. This is because Amazon API Gateway has a default account-level limit of 10,000 requests per second (RPS) and a default per-method limit of 5,000 RPS. If the company's premium tier customers are making more than 10,000 requests per second in total across all API methods and regions, they would be receiving the error message of 429 Too Many Requests. This indicates that the API Gateway account is reaching its capacity limit, and the Lambda function is not being invoked because API Gateway is blocking the requests before they reach the Lambda function.

The other choices are not correct because the Lambda function's concurrency limit and region limit for concurrency would not affect the API Gateway's request rate limit, and the API Gateway's default per-method limit is 5,000 RPS which is less than the premium tier's 3,000 calls per second.

upvoted 5 times

 **masetromain** 1 year, 2 months ago

Option A is incorrect because the error message is not related to the Lambda function reaching its concurrency limit.

Option B is incorrect because the error message is not related to the Lambda function reaching its region limit for concurrency.

Option D is incorrect because the error message is not related to the company reaching its API Gateway default per-method limit for calls per second, but it's related to the account level limit.

upvoted 3 times

 **career360guru**  3 months, 2 weeks ago

Selected Answer: C

429 is API Gateway API throttle default limit.

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C of course

upvoted 1 times

 **dev112233xx** 1 year ago

Selected Answer: C

C

429 error indicates that API calls per second was exceeded ... it's not a Lambda issue

upvoted 2 times

≡  **mfsec** 1 year ago

Selected Answer: C

Company reached its limit

upvoted 1 times

≡  **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is the answer

upvoted 1 times

≡  **zhangyu20000** 1 year, 2 months ago

C is correct answer

upvoted 1 times

Question #121

Topic 1

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC
- B. Deploy the web application behind a Network Load Balancer
- C. Deploy an Application Load Balancer in front of the security tool instances
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool
- E. Provision a transit gateway to facilitate communication between VPCs.

Correct Answer: AD

Community vote distribution

AD (53%) DE (44%)

✉  **OCHT**  1 year ago

Selected Answer: AD

Option B, deploying the web application behind a Network Load Balancer, is not relevant to integrating the third-party security tool with AWS technology.

Option C, deploying an Application Load Balancer in front of the security tool instances, is not necessary because a Gateway Load Balancer is already being used to redirect traffic to the security tool.

Option E, provisioning a transit gateway to facilitate communication between VPCs, is not relevant to integrating the third-party security tool with AWS technology or inspecting packets in and out of the VPC.

In summary, options A and D are the best choices because address the specific requirements stated in the scenario while options B, C and E do not.

upvoted 18 times

✉  **deegadaze1** 10 months, 3 weeks ago

Correct for GLB---> https://www.youtube.com/watch?v=-j2smz_VCH4

upvoted 2 times

✉  **rbm2023**  10 months, 3 weeks ago

Selected Answer: DE

Based on the scenario in question, the requirement is that the security tool will run in an auto scaling group in a dedicated VPC this cannot be changed. This will break Option A. If we look at the usage for the Gateway Load Balancer which is the key for the solution where application cannot have performance hits if you are inspecting the traffic, so you need to TAP the traffic to move into another third-party tool. In the references you will find below the transit gateway will facilitate the VPC-to-VPC communication and as you can see, the security appliances VPC is a segregated from the application VPC, so again, option A is NOT valid.

<https://catalog.workshops.aws/networking/en-US/gwlb>

<https://www.fortinet.com/blog/business-and-technology/highly-scalable-fortigate-next-generation-firewall-security-on-aws-gateway-load-balancer-service>

upvoted 16 times

✉  **failexamonly**  2 weeks ago

Selected Answer: DE

Not A. A does not make sense for D

upvoted 1 times

✉  **gofavad926** 3 weeks, 2 days ago

Selected Answer: AD

AD - ec2 + asg + gateway load balancer

upvoted 2 times

✉  **djeong95** 1 month ago

Selected Answer: DE

I answered AD and searched through these comments' links to seek to understand.

First, the most convincing case is that as @rbm2023 answered, it is not pattern to put security tool in the existing VPC. The financial company in the question is also looking to only have their application migrate into a dedicated VPC.

Second, solution A sounds good and according to this link below, you can use ASG with GWLB. I think key is the fine print of Customer wanting their own dedicated VPC and the pattern of using TWG in front. (However, it is possible to do without)

<https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/>

upvoted 1 times

✉  **yog927** 1 month, 1 week ago

Selected Answer: DE

D and E

Read the question, it says dedicated VPC

upvoted 1 times

✉  **VerRi** 1 month, 2 weeks ago

Selected Answer: AD

Try not to over-interpret the given options. Only D and E won't work because the security tool has not been settled down yet.

upvoted 2 times

✉  **chelbsik** 2 months ago

Selected Answer: DE

Vote for DE, agreed about 15 years old security tool might not be able to support autoscaling, and it has to be in a dedicated VPC, according to the task

Forgot to vote

upvoted 1 times

✉  **chelbsik** 2 months ago

Vote for DE, agreed about 15 years old security tool might not be able to support autoscaling, and it has to be in a dedicated VPC, according to the task

upvoted 1 times

✉  **AWSLord32** 2 months, 1 week ago

Selected Answer: DE

A is not valid as the web application needs to be in a dedicated VPC. Also the security app is 15 years old and likely doesn't support autoscaling natively.

DE is best practice.

upvoted 1 times

✉  **jpa8300** 3 months ago

Selected Answer: DE

I agree with what has been said about D and E option. A could be right, but a better architecture would be to put the security tool in its own VPC, not only for this web application, but also to use to other apps where you want to use the security tool.

upvoted 1 times

✉  **career360guru** 3 months, 2 weeks ago

Selected Answer: AD

A and D are the right options.

It clearly says security tool has no cloud offering so it needs to run on separate EC2 instance.

There is no need to run it on a different VPC and GWLB will take care of mirror and traffic to this security tool so it will not affect the application performance.

upvoted 2 times

✉  **HappyPrince** 3 months, 3 weeks ago

Selected Answer: AD

As the tool must not impact performance of the application, installing it in separate ASG makes sense.

upvoted 2 times

✉  **atirado** 3 months, 3 weeks ago

Selected Answer: DE

There are two main requirements to look after:

The web application will be deployed in a dedicated VPC : This means that the security monitoring tool must be deployed outside of the web application's VPC, i.e. another VPC.

Security monitoring must not affect the performance of the web application : should be straightforward.

The natural fit is to use a Gateway Load Balancer. However, where it gets a bit tricky is to choose either between Option A or Option D: Put the security tool's EC2 instances in an Auto Scaling Group or connect the VPCs using a transit gateway.

Option D ensures traffic will reach the security tool for inspection. The wording in Option A seems off ('Existing VPC'). But in any case, the whitepaper "Building a Scalable and Secure Multi-VPC AWS Network Infrastructure" provides the answer at <https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/welcome.html>

upvoted 1 times

 **ayadmawla** 3 months, 4 weeks ago

Selected Answer: DE

The question requires a combination of steps. A suggests to install the security tool on EC2 in the same VPC and then E talks about a GWLB which is in a different VPC. Logic dictates that we create an Appliance/Shared VPC, route the VPC traffic to it (via transit gw) and inspect the content by gwlb and allow it to continue on its merry way or block it.

upvoted 1 times

 **MRamos** 4 months ago

Selected Answer: DE

DE as described in

<https://aws.amazon.com/pt/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/>

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: DE

Not sure why we need a transit gateway in this case, but at least it is possible. A confront with dedicated VPC requirement.

upvoted 1 times

Question #122

Topic 1

A company has purchased appliances from different vendors. The appliances all have IoT sensors. The sensors send status information in the vendors' proprietary formats to a legacy application that parses the information into JSON. The parsing is simple, but each vendor has a unique format. Once daily, the application parses all the JSON records and stores the records in a relational database for analysis.

The company needs to design a new data analysis solution that can deliver faster and optimize costs.

Which solution will meet these requirements?

- A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.
- B. Migrate the application server to AWS Fargate, which will receive the information from IoT sensors and parse the information into a relational format. Save the parsed information to Amazon Redshift for analysis.
- C. Create an AWS Transfer for SFTP server. Update the IoT sensor code to send the information as a .csv file through SFTP to the server. Use AWS Glue to catalog the files. Use Amazon Athena for analysis.
- D. Use AWS Snowball Edge to collect data from the IoT sensors directly to perform local analysis. Periodically collect the data into Amazon Redshift to perform global analysis.

Correct Answer: C

Community vote distribution

A (81%) B (19%)

⊕  **God_Is_Love**  1 year, 1 month ago

Selected Answer: A

IOT Core communication supports protocols MQTT, HTTPS, MQTT over WSS, and LoRaWAN (but not FTP/SFTP) so C should be wrong.

Rules Engine: AWS IoT Core provides a rules engine that allows users to define and execute business logic on the data generated by their IoT devices. This enables users to automate actions such as sending notifications, triggering alarms, or updating device settings based on real-time data.

Integration with other AWS Services: AWS IoT Core integrates with other AWS services such as AWS Lambda, AWS Kinesis, and AWS S3, allowing users to easily process and store their IoT data, as well as build complex IoT applications using a range of AWS services.

upvoted 10 times

⊕  **gofavad926**  3 weeks, 2 days ago

Selected Answer: A

A, IoT Core

upvoted 1 times

⊕  **career360guru** 3 months, 2 weeks ago

Selected Answer: A

Option A is best(fastest) and most cost effective.

upvoted 1 times

⊕  **GaryQian** 4 months, 1 week ago

Selected Answer: A

Everytime the exam shows IOT sensor, think of IOT Core and aws glue

upvoted 1 times

⊕  **KCjoe** 5 months, 2 weeks ago

Selected Answer: B

How can A satisfy this requirement? "relational database for analysis"

The only option is B with relational database for analysis.

upvoted 4 times

⊕  **heatblur** 4 months, 2 weeks ago

"The company needs to design a new data analysis solution that can deliver faster and optimize costs."

upvoted 1 times

⊕  **uC6rW1aB** 7 months ago

Selected Answer: A

Option A: AWS IoT Core + Lambda

Speed: Near real-time data collection and analysis.

Flexibility: Ability to adapt to different data formats from multiple vendors.

Option C: AWS Transfer for SFTP

Speed: There may be network delays and waiting for all data to be sent.

Development needs: The sensor code needs to be updated, which increases the development workload.

All things considered, option A is better than option C in terms of speed and flexibility, and is especially suitable for real-time or near-real-time requirements.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

A for sure

upvoted 1 times

✉ **Maria2023** 10 months, 3 weeks ago

Selected Answer: A

I go for A on the elimination principle although neither of the answers does not seem to fully cover the requirements. I am not sure what is the "vendors' proprietary formats" and not sure why they assume it's csv. Also there is a requirement to load the data in relational database which excludes B. For A we need to assume that S3 covers this requirement.

upvoted 2 times

✉ **dev112233xx** 1 year ago

Selected Answer: A

A is correct, even though it's not clear from the question if the sensors protocol is MQTT or HTTPS.
but i can't find other suitable answer so i guess A is the correct one.

upvoted 4 times

✉ **mfsec** 1 year ago

Selected Answer: A

Connect the IoT sensors to AWS IoT Core.

upvoted 2 times

✉ **spd** 1 year, 1 month ago

Selected Answer: A

A by Elimination rule

upvoted 3 times

✉ **Musk** 1 year, 2 months ago

Selected Answer: B

I m not convinced about A. It kind of requires changes in the sensors to be compatible with AWS IoT Core.

upvoted 4 times

✉ **Sarutobi** 11 months, 3 weeks ago

I agree with you here. We don't know if IoT Core supports it, so moving the application to AWS Fargate will guarantee compatibility.

upvoted 1 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: A

i'll go for A

upvoted 4 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: A

A. Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis.

This solution meets the requirement of faster analysis and cost optimization by using AWS IoT Core to collect data from the IoT sensors in real-time and then using AWS Glue and Amazon Athena for efficient data analysis.

Option B and D do not optimize the cost of data analysis as they involve use of expensive services like AWS Fargate and Snowball Edge respectively. Option C does not make use of real-time data collection and may not be optimal for faster analysis.

upvoted 4 times

✉ **zhangyu20000** 1 year, 2 months ago

A is correct.

B: it is appliance, impossible to install on Fargate

C: device not use FTP protocol

D: snowball is not real time

upvoted 4 times

✉ **Musk** 1 year, 2 months ago

In B, we don't try to port appliances to Fargate, but only the app that parses the information from the appliances into JSON.

I am doubting about A. Unless you would reprogram the sensors they would not know how to connect to AWS IoT Core.

upvoted 1 times

Question #123

Topic 1

A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connect connection in a central network account.

The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create a Direct Connect gateway in the central account. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- B. Create a Direct Connect gateway and a transit gateway in the central network account. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
- C. Provision an internet gateway. Attach the internet gateway to subnets. Allow internet traffic through the gateway.
- D. Share the transit gateway with other accounts. Attach VPCs to the transit gateway.
- E. Provision VPC peering as necessary.
- F. Provision only private subnets. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.

Correct Answer: BDF

Community vote distribution

BDF (100%)

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: BDF

B and D and F are correct.

B: Creating a Direct Connect gateway and a transit gateway in the central network account will allow the company to connect its on-premises data center to the resources in AWS.

D: Sharing the transit gateway with other accounts will allow the company to communicate with all the VPCs in multiple accounts.

F: Provisioning only private subnets and opening necessary routes on the transit gateway and customer gateway will allow the company to route its cloud resources to the internet through its on-premises data center.

A is incorrect because it would be redundant to use both a Direct Connect gateway and a transit gateway.

C is incorrect because it is not necessary to provision an internet gateway, since the company wants to route traffic through their on-premises data center.

E is incorrect because VPC peering may not be necessary if the company is using a transit gateway to connect all the VPCs.

upvoted 10 times

 **career360guru** Most Recent 3 months, 2 weeks ago

Selected Answer: BDF

BDF is most scalable solution.

upvoted 1 times

 **shaaam80** 4 months ago

Selected Answer: BDF

Answer BDF

DGW and TGW

Share TGW and configure VPC attachments to TGW

Open necessary routes for traffic routing via NAT gw on the on-prem dc

upvoted 1 times

 **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: BDF

Very logical

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: BDF

BDF for sure

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

Selected Answer: BDF

Standard scenario. You connect the Direct Connect Gateway to the Transit Gateway, attach the VPCs, and route the traffic through the On-premise devices

upvoted 2 times

✉️ **SkyZeroZx** 10 months, 3 weeks ago

Selected Answer: BDF

BDF is the right ans

upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: BDF

BDF is the right combo

upvoted 1 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: BDF

VPC Peering does not work as there are hundreds of VPCs, transit gateway is easy to configure and practical.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

upvoted 4 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: BDF

B D and F

upvoted 4 times

✉️ **zozza2023** 1 year, 2 months ago

I agree with BD&F

upvoted 3 times

✉️ **zhangyu20000** 1 year, 2 months ago

BDF are correct

upvoted 2 times

Question #124

Topic 1

A company has hundreds of AWS accounts. The company recently implemented a centralized internal process for purchasing new Reserved Instances and modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement. Previously, business units directly purchased or modified Reserved Instances in their own respective AWS accounts autonomously.

A solutions architect needs to enforce the new process in the most secure way possible.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- C. In each AWS account, create an IAM policy that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action. Attach the SCP to each OU of the organization.
- E. Ensure that all AWS accounts are part of an organization in AWS Organizations that uses the consolidated billing feature.

Correct Answer: AD

Community vote distribution

AD (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: AD

A and D are the correct answer.

A: By ensuring all AWS accounts are part of an organization in AWS Organizations, it allows for centralized management and control of the accounts. This can help enforce the new purchasing process by giving a dedicated team the ability to manage and enforce policies across all accounts.

D: By creating an SCP (Service Control Policy) that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions, it enforces the new centralized purchasing process. Attaching the SCP to each OU (organizational unit) within the organization ensures that all business units are adhering to the new process.

B and C are not the correct answer, because AWS Config and IAM policies are used for monitoring and managing access to resources in an account, respectively. They don't enforce the new process for purchasing reserved instances.

E is not the correct answer as this is not related to the new process for purchasing reserved instances.

upvoted 7 times

 **career360guru**  3 months, 2 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

 **yohaf32543** 3 months, 3 weeks ago

A and D are the correct answer

itexamslab.com

upvoted 2 times

 **atirado** 3 months, 3 weeks ago

A+D achieve the goal of denying access to purchase and to modify Reserved Instances to all OUs. The dedicated team can still perform these actions if they are part of the management account.

C, E don't actually do anything, as in, actually control anything at all. B will trigger on the wrong thing to be alarmed about, if triggering an alarm was the goal.

upvoted 1 times

 **dkcloudguru** 7 months, 1 week ago

A and D : is the best way

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: AD

AD. A so can use SCP

upvoted 1 times

 **Maria2023** 10 months, 3 weeks ago

Selected Answer: AD

I was not confident about enabling all features because I was messing "features" and "services". Yes - you need to enable all features, otherwise you cannot control the accounts in your organization. The rest is common sense

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: AD

AD easy

upvoted 3 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: AD

A and D

upvoted 4 times

 **zhangyu20000** 1 year, 2 months ago

AD are correct

upvoted 2 times

Question #125

Topic 1

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.

A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database
- C. Use RDS Proxy in front of the database.
- D. Migrate the database to Amazon Aurora MySQL.
- E. Create an Amazon Aurora Replica.
- F. Create an RDS for MySQL read replica

Correct Answer: BCF

Community vote distribution



✉️ **RaghavendraPrakash** 11 months, 1 week ago

CDE. RDS Failover typically takes 60-120 seconds, while Aurora failover completes within 30 seconds. ElastiCache is for reducing latency, not for failover.

upvoted 12 times

✉️ **dev112233xx** 1 year ago

Selected Answer: CDE

RDS Proxy with Aurora are the best combination for less than "20 sec" failover time...

According to this article RDS Proxy can reduce the failover time of Aurora by 79% while it can reduce RDS failover time by only 32%:
<https://aws.amazon.com/blogs/database/improving-application-availability-with-amazon-rds-proxy/>

upvoted 8 times

✉️ **Dgix** 2 weeks, 5 days ago

Selected Answer: CDE

A and B don't contribute to reducing response time in failover scenarios.

D is required for faster failover.

E is required to support D.

F doesn't reduce failover time.

C, finally, is the remaining option. It doesn't hurt, and can contribute to faster failover, though it is not the most important factor here - the switch to Aurora with an Aurora read replica is.

upvoted 1 times

✉️ **bjexamprep** 4 weeks, 1 day ago

Anyone can share why choosing E? I know we have to choose 3. isn't it weird? Aurora already has replicas natively. Why creating another one?

upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: CDE

Option C, D and E

upvoted 1 times

✉️ **atirado** 3 months, 3 weeks ago

Selected Answer: CDE

C+D+E provides the 'fastest' failover with the options available:

- Aurora MySQL is Multi-AZ by design: During failover it will promote a Replica to primary or create a Primary instance
- Creating a Replica provides the option to have something to failover to
- Using an RDS Proxy further reduces failover time and provides 'transparent' failovers as well (It manages DNS changes)

The argument against Caching (options A or B) is that it doesn't accelerate failing over to a different instance. Cache misses and write operations will produce exceptions because there is no instance to query. Moreover, there is no information in the question to choose between either caching option, i.e. Both options can be created starting from an Aurora DB Cluster settings -
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/creating-elasticache-cluster-with-RDS-settings.html>

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: CDE

CDE, agree with other comments

upvoted 2 times

✉ **Sarutobi** 11 months, 3 weeks ago

Selected Answer: CDE

The trick seems to be that the RDS proxy handles DNS updates quickly. While if you don't use it, you are at the mercy of the host to update its DNS cache.

upvoted 3 times

✉ **mfsec** 1 year ago

Selected Answer: CDE

CDE is the best choice

upvoted 1 times

✉ **DWsk** 1 year ago

Selected Answer: CDE

CDE. I would have said F, but the question asks for a combination of steps, so its looking for the Aurora replica and not the MySQL RDS replica

upvoted 3 times

✉ **Jay_2pt0_1** 11 months, 4 weeks ago

I agree with your logic.

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Selected Answer: CDE

C for sure as connection pooling helps quick re connect. There is no preference for A or B cache solution based on the question. So, A,B are eliminated. so three correct options should be in others. If you choose Aurora only, three answers will be met :-) C,D,E

upvoted 3 times

✉ **zozza2023** 1 year, 2 months ago

Selected Answer: CDE

C D and E

upvoted 2 times

✉ **nyxs_19** 1 year, 1 month ago

A and B are incorrect options because Amazon ElastiCache is a caching service, not a failover solution. F is also incorrect because RDS read replicas are asynchronous, which means that there may be a delay in replication, leading to the potential loss of data. Additionally, creating a read replica does not improve the failover time.

upvoted 1 times

✉ **AjayD123** 1 year, 2 months ago

Selected Answer: CDE

RDS read replica auto failover takes approx 35 seconds hence, BCF does not satisfy under 20 seconds failover requirement.

<https://aws.amazon.com/rds/features/multi-az/#:~:text=Amazon%20RDS%20Multi%2DAZ%20with%20two%20readable%20standbys,-Automatically%20fail%20over&text=Automatically%20failover%20in%20typically%20under, and%20with%20no%20manual%20intervention.>

upvoted 5 times

✉ **zozza2023** 1 year, 2 months ago

thanks for the information about RDS read replica

upvoted 2 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: CDE

The correct answer is D, E and C:

Migrate the database to Amazon Aurora MySQL.

- Create an Amazon Aurora Replica.
- Use RDS Proxy in front of the database.
- These options are correct because they address the requirement of reducing the failover time to less than 20 seconds.

Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time.

Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure.

Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

upvoted 4 times

✉ **masetromain** 1 year, 2 months ago

Option A and B, Use Amazon ElastiCache for Memcached and Redis in front of the database, are not correct as ElastiCache is a caching service, it doesn't provide a high availability solution for the underlying database.

Option F, Create an RDS for MySQL read replica, is not correct as a read replica can only be used to offload read traffic from the primary instance, it doesn't provide a high availability solution for the underlying database.

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: BCF

The correct answer is B, C and F.

Using Amazon ElastiCache for Redis in front of the database (Option B) will help to reduce the failover time by caching the frequently-used data, so that it can be quickly served from the cache rather than having to be retrieved from the database during a failover.

Using RDS Proxy in front of the database (Option C) will help to reduce the failover time by managing the connections to the RDS DB instance, so that it can quickly route traffic to the new primary instance during a failover.

Creating an RDS for MySQL read replica (Option F) will help to reduce the failover time by having a read-only copy of the database running in parallel with the primary instance, so that it can take over as the primary instance in the event of a failover.

Option A and D are not relevant in this case as the question is asking specifically about reducing failover time for an RDS for MySQL database.

upvoted 3 times

 **spd** 1 year, 1 month ago

C, D and E Correct

upvoted 1 times

 **zhangyu20000** 1 year, 2 months ago

CDE are correct

upvoted 3 times

Question #126

Topic 1

An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account.

What is the MOST secure way to allow org1 to access resources in org2?

- A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.
- B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.
- C. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.
- D. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN), including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **dev112233xx** Highly Voted 1 year ago

Selected Answer: D

D

Well.. "external ID" is the keyword that you should look for in such scenario.

upvoted 5 times

✉️  **career360guru** Most Recent 3 months, 2 weeks ago

Selected Answer: D

Option D is most secure.

upvoted 1 times

✉️  **atirado** 3 months, 3 weeks ago

Selected Answer: D

Sharing credentials will always be a bad idea. In comparison to C and D, options A and B are insecure.

The reason D is the most secure option compared to C is because it addresses the confused deputy problem -
<https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html>

upvoted 2 times

✉️  **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

it's D, but private link would be a better choice

upvoted 2 times

✉️  **mfsec** 1 year ago

Selected Answer: D

With the external ID.

upvoted 2 times

✉️  **God_Is_Love** 1 year, 1 month ago

Selected Answer: D

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "Example Corp's AWS Account ID"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "1122334455-The ID that only Third party and customer knows"
      }
    }
}
```

```
}
```

```
}
```

```
}
```

upvoted 3 times

 Musk 1 year, 2 months ago

Selected Answer: D

Easy. The external ID is for sure the winner.

upvoted 1 times

 zozza2023 1 year, 2 months ago

Selected Answer: D

D seems the correct answer

upvoted 2 times

 Untamables 1 year, 2 months ago

Selected Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

upvoted 2 times

 masetromain 1 year, 2 months ago

Selected Answer: D

The correct answer is D. This is the most secure way to allow org1 to access resources in org2 because it allows for least privilege security access. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) and include the external ID in the IAM role's trust policy when requesting access to perform the required tasks. This ensures that the partner company can only access the resources that it needs and only from the specific customer account.

Option A and B both involve providing the partner company with credentials, which can be easily compromised and could lead to a security breach. Option C also provides the partner company with an IAM role, but it doesn't have any restrictions on when and where the partner company can access the resources in customer account, it could be a security risk.

upvoted 2 times

 zhangyu20000 1 year, 2 months ago

D is correct

upvoted 1 times

Question #127

Topic 1

A delivery company needs to migrate its third-party route planning application to AWS. The third party supplies a supported Docker image from a public registry. The image can run in as many containers as required to generate the route map.

The company has divided the delivery area into sections with supply hubs so that delivery drivers travel the shortest distance possible from the hubs to the customers. To reduce the time necessary to generate route maps, each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area.

The company needs the ability to allocate resources cost-effectively based on the number of running containers.

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

- A. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2. Use the Amazon EKS CLI to launch the planning application in pods by using the --tags option to assign a custom tag to the pod.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on AWS Fargate. Use the Amazon EKS CLI to launch the planning application. Use the AWS CLI tag-resource API call to assign a custom tag to the pod.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. Use the AWS CLI with run-tasks set to true to launch the planning application by using the --tags option to assign a custom tag to the task.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Use the AWS CLI run-task command and set enableECSManagedTags to true to launch the planning application. Use the --tags option to assign a custom tag to the task.

Correct Answer: D

Community vote distribution



✉️ **dev112233xx** Highly Voted 1 year ago

Selected Answer: D

D is the correct answer, When you use the APIs to create a service or run a task, you must set enableECSManagedTags to true for run-task and create-service. (see link below)

B doesn't make sense because EKS is more for complex orchestrated microservices apps, i don't think it needed in such scenario

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-using-tags.html>

upvoted 13 times

✉️ **Jay_2pt0_1** 4 months, 3 weeks ago

Stepped through that same thought process

upvoted 1 times

✉️ **ninomfr64** Most Recent 2 months, 2 weeks ago

Selected Answer: D

A and B = between EKS and ECS if K8s is not required I go for ECS

C = between EC2 and Fargate if nothing points you clearly to Ec2 i would go for Fargate (less overhead, could cost less)

D = correct

upvoted 2 times

✉️ **ele** 3 months ago

Selected Answer: B

D is a trap, even if it's tempting, but '--tags' is not a valid option for tagging ecs tasks/services.

B is the right answer.

upvoted 1 times

✉️ **cox1960** 2 months, 3 weeks ago

--tags is valid

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ecs/run-task.html>

upvoted 1 times

✉️ **cox1960** 2 months, 3 weeks ago

but --enable-ecs-managed-tags is the right option instead of "enableECSManagedTags` to `true`"

upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: D

D is best option with least operational overhead.

upvoted 2 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: D

Options A and C are more operationally complex than B and D because you will need to manage the EC2 instances and underpin the EKS cluster and the ECS service definition. And as if to make the selection easier, B and D explicitly mention using AWS Fargate in a way that works.

Selecting between Options B and D boils down the interpretation of "each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area". The only indication in the question that kind of helps is "The third party supplies a supported Docker image from a public registry": The custom configuration is just for processing orders in the section's area rather something in the docker image itself.

upvoted 1 times

✉ **n_d1** 6 months, 3 weeks ago

Selected Answer: D

As per the Amazon EKS documentation, the following EKS resources support tags:

- clusters
- managed node groups
- Fargate profiles

I think that rules out B in favour of D!

<https://docs.aws.amazon.com/eks/latest/userguide/eks-using-tags.html#tag-resources>

upvoted 2 times

✉ **Ganshank** 7 months, 3 weeks ago

Real-world answer - B.
Certification answer - D.

upvoted 3 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

going with D
upvoted 1 times

✉ **rbm2023** 10 months, 3 weeks ago

Selected Answer: D

Since the question where the requirement is the least operational overhead and we are between EKS and ECS, I would go for ECS, I believe EKS has more operational overhead for deploying and for operating. Also, you would probably have to apply less steps to build this structure using ECS when comparing with EKS.

upvoted 3 times

✉ **iamunstopable** 11 months, 2 weeks ago

B is correct
Anytime you need Docker containers with a custom configuration use EKS
upvoted 2 times

✉ **Jay_2pt0_1** 11 months, 4 weeks ago

Selected Answer: B

Like many have already stated, the debate is between B and D. I think B is the answer as "each section uses its own set of DOcker Containers with a customer configuration," which leads me to believe that EKS orchestration is worthwhile in terms of operational overhead.

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: D

D is easier
upvoted 1 times

✉ **taer** 1 year ago

Selected Answer: D

I vote for D
upvoted 1 times

✉ **rtgfdv3** 1 year, 1 month ago

Selected Answer: B

i still think is B
"each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area."
upvoted 2 times

✉ **Jay_2pt0_1** 11 months, 1 week ago

Agree and for the same reason.

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: D

choosing D based on below tagging information
<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-using-tags.html>

upvoted 1 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: D

EKS with Fargate is a more complex platform than ECS with Fargate. Kubernetes has a steeper learning curve than ECS, and requires more expertise to manage. ECS with Fargate is designed to be simple and easy to use, making it a good choice for organizations that want to quickly deploy containerized applications without having to manage the complexity of Kubernetes.

upvoted 4 times

 **spd** 1 year, 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/cli/latest/reference/ecs/run-task.html>

upvoted 1 times

Question #128

Topic 1

A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure.

Which factors could cause this error? (Choose two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer accepter account does not have the correct permissions

Correct Answer: AE*Community vote distribution*

✉️ **Appon** 1 year, 2 months ago

Selected Answer: AE

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-vpc-peering-error/>
upvoted 7 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: AE

Option A and E
upvoted 1 times

✉️ **m1xa** 4 months, 3 weeks ago

Selected Answer: AE

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
<https://repost.aws/knowledge-center/cloudformation-vpc-peering-error>
upvoted 1 times

✉️ **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: AE

This is correct, per Appon's link
upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: AE

AE for sure
upvoted 1 times

✉️ **ThaiNT** 11 months ago

Selected Answer: BE

VPCs are not in the same Region.
upvoted 3 times

✉️ **ThaiNT** 11 months ago

My bad, option B is incorrect.
upvoted 2 times

✉️ **mfsec** 1 year ago

Selected Answer: AE

AE is the best choice
upvoted 2 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: AE

FYI, Other reasons for issue :
If the IAM role in the accepter account doesn't have the right permissions

If the PeerRoleArn property isn't passed correctly when you create a VPC peering connection between VPCs in different accounts

If the PeerRegion property isn't passed correctly when you're creating a VPC peering connection between VPCs in different AWS Regions
upvoted 3 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: AE

A and E

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: AE

A is correct because the IPv4 CIDR ranges of the two VPCs overlap. The two VPCs have an IP range of 10.10.0.0/16 and 10.10.10.0/24, which means that they share the same 10.10.0.0 network. This causes a conflict in routing and will prevent the VPCs from being able to communicate with each other.

E is correct because the IAM role in the peer accepter account does not have the correct permissions. The role must have permissions to create, modify, and delete VPC peering connections in order for the peering to be established.

B, C, and D are not correct. The VPCs are in the same region, both accounts have access to an internet gateway and both VPCs are not shared through AWS Resource Access Manager.

upvoted 2 times

 **clownfishman** 10 months ago

us-east-1 is in virginia, us-east-2 is in ohio - they are separate regions

upvoted 3 times

 **Arnaud92** 7 months ago

stop asking to ChatGPT

upvoted 6 times

 **m1xa** 4 months, 3 weeks ago

It doesn't matter if both accounts are in the same region or not.

>>> The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

upvoted 1 times

 **zhangyu20000** 1 year, 2 months ago

AE is correct

D is not correct because you cannot share VPC via RAM, subnet can

upvoted 3 times

 **djeong95** 1 month ago

In this link, you can find VPC sharing being described as "In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organization". You can share subnets using AWS RAM. I think it is safe to conclude you can share VPCs using RAM.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html#vpc-share-prerequisites>

upvoted 1 times

Question #129

Topic 1

An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API calls. Create an inventory of the required API calls and resources for each Lambda function. Create new IAM access policies for each Lambda function. Review the new policies to ensure that they meet the company's business requirements.
- B. Turn on AWS CloudTrail logging for the AWS account. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.
- C. Turn on AWS CloudTrail logging for the AWS account. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary report. Review the report. Create IAM access policies that provide more restrictive permissions for each Lambda function.
- D. Turn on AWS CloudTrail logging for the AWS account. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution role. Create a new IAM access policy for each role. Export the generated roles to an S3 bucket. Review the generated policies to ensure that they meet the company's business requirements.

Correct Answer: B

Community vote distribution

B (100%)

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: B

Access Analyzer uses automated reasoning to analyze resource policies and detect issues such as overly permissive access or violations of organizational security policies. It works by examining the policies attached to AWS resources, such as S3 buckets, IAM roles, and KMS keys, and identifying any potential security risks or policy violations.

upvoted 13 times

 **God_Is_Love** 1 year, 1 month ago

fyi

ML tool - CodeGuru has two main components: CodeGuru Reviewer and CodeGuru Profiler.

CodeGuru Reviewer is a code review service that uses machine learning to identify code quality issues and security vulnerabilities in your application's source code. It analyzes the code and provides recommendations for improvements based on best practices, industry standards, and AWS experience.

CodeGuru Profiler is a profiling tool that uses machine learning to identify performance issues in your application code at runtime. It continuously analyzes the performance characteristics of your application code and provides recommendations for optimization.

upvoted 6 times

 **cox1960**  2 months, 3 weeks ago

poor since B only works when functions are actually triggered and all the branches of the code are covered.

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B is obvious choice

upvoted 1 times

 **atirado** 3 months, 3 weeks ago

Selected Answer: B

When approaching questions related to access permissions, it will always help to determine who is accessing what, in this case, it is Lambda functions accessing AWS services (S3 buckets and DynamoDB table).

The choice between A,B and C,D is then based on knowing that Code Guru and Access Analyzer used an automated process to detect issues in

code and to compare actual access versus permissions - least effort than C & D.

That last bit is where the kicker is. The question refers to IAM execution roles with too-broad AWS IAM permissions to access AWS services and resources: You are looking for the option that tightens IAM policies rather than in AWS Lambda Function code.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

B - basic access analyzer use case

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword == Access Management Access Analyzer to generate IAM

upvoted 1 times

 **Alabi** 10 months, 1 week ago

Selected Answer: B

B definitely

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

B - Identity and Access Management Access Analyzer

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: B

Identity and Access Management Access Analyzer

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: B

The correct answer is B. Turn on AWS CloudTrail logging for the AWS account, and use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log. Review the generated policies to ensure that they meet the company's business requirements.

This is the least amount of effort as it makes use of AWS services that can automatically analyze the CloudTrail logs, generate the IAM policies, and provide a report for the review process.

Option A and D both involve additional steps such as running scripts or using Amazon EMR, which would take more effort to set up and maintain.

Option C is similar to option A and D but doesn't use any AWS services to help with the process.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

B is correct

upvoted 1 times

Question #130

Topic 1

A solutions architect must analyze a company's Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine whether the company is using resources efficiently. The company is running several large, high-memory EC2 instances to host database clusters that are deployed in active/passive configurations. The utilization of these EC2 instances varies by the applications that use the databases, and the company has not identified a pattern.

The solutions architect must analyze the environment and take action based on the findings.

Which solution meets these requirements MOST cost-effectively?

- A. Create a dashboard by using AWS Systems Manager OpsCenter. Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.
- D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

Correct Answer: C

Community vote distribution



God_Is_Love Highly Voted 1 year, 1 month ago

Selected Answer: C

AWS Compute Optimizer helps analyze the usage patterns of AWS resources, such as EC2 instances and Auto Scaling groups, and makes recommendations on how to optimize them for performance and cost using machine learning algorithms. It then generates recommendations that can be used to adjust instance types, purchase options, and other parameters. It provides two types of recommendations:
Recommended instance types - recommends instance types that are more cost-effective and better suited to the workload requirements.
Recommended purchase options - recommends purchasing options, such as Reserved Instances or Savings Plans, that can help customers save money on their compute resources.

upvoted 15 times

God_Is_Love 1 year, 1 month ago

A is wrong.

OpsCenter, a capability of AWS Systems Manager, provides a central location where operations engineers and IT professionals can manage operational work items (OpsItems) related to AWS resources. An OpsItem is any operational issue or interruption that needs investigation and remediation. Using OpsCenter, you can view contextual investigation data about each OpsItem, including related OpsItems and related resources. You can also run Systems Manager Automation runbooks to resolve OpsItems.

upvoted 2 times

God_Is_Love 1 year, 1 month ago

fyi Pricing looks cheap too - <https://aws.amazon.com/compute-optimizer/pricing/>

upvoted 2 times

saggy4 Most Recent 1 month, 4 weeks ago

Selected Answer: C

A - Not possible

D - Costliest Option possible

now between B and C

The question mentions high-memory EC2 instances.

You cannot get memory metrics without the Cloudwatch agent installed hence C.

upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: C

Option C is most cost effective choice.

upvoted 1 times

wmp7039 3 months, 2 weeks ago

C is incorrect : When you first opt in Compute Optimizer, it may take up to 24 hours to fully analyze the AWS resources in your account. <https://aws.amazon.com/compute-optimizer/faqs/>

upvoted 1 times

✉ **carpa_jo** 3 months, 1 week ago

You are correct that in the FAQ you've linked it says 24 hours, but in other places of the AWS documentation it says 12 hours, like here: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-getting-recommendations.html#viewing-recommendations> or here: <https://docs.aws.amazon.com/awssupport/latest/user/compute-optimizer-with-trusted-advisor.html> Seems like even AWS doesn't know :D So I would still go with C.

upvoted 1 times

✉ **yohaf32543** 3 months, 3 weeks ago

C is correct

itexamslab.com

upvoted 2 times

✉ **atirado** 3 months, 3 weeks ago

Selected Answer: C

Option A is not in the running because it will require incurring further expense to address the cost issue.

Option D is expensive - the Enterprise Support plan charges a minimum flat fee minimum or a % of your AWS bill. This could be a large amount for the company's hundreds of instances.

Option B is expensive - Detailed monitoring scales based on the number of metrics and the number of resources. The company has hundreds of instances so this option could potentially be more expensive than D.

Option C - Compute Optimizer will provide improvement suggestions based on 14 prior days usage data from the moment it was enabled. Moreover, the default service option is free. Nothing is said about the custom metrics being used for the CloudWatch agent but it could be the most expensive of all options if mis-used. So either cost 0 or incredibly large if used carelessly.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C. need CW agent for RAM util

upvoted 1 times

✉ **Fredonly** 11 months, 3 weeks ago

Selected Answer: C

C- Compute Optimizer is the easiest solution

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: C

C - cost optimizer

upvoted 1 times

✉ **mfsec** 1 year ago

*Compute

upvoted 1 times

✉ **spd** 1 year, 1 month ago

Selected Answer: C

C is correct - Optimizer

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: A

Option C may be a good solution to rightsizing the EC2 instances but may incur additional cost for installing the Amazon CloudWatch agent on each of the EC2 instances.

The MOST cost-effective solution to analyze the company's Amazon EC2 instances and Amazon EBS volumes is to create a dashboard using AWS Systems Manager OpsCenter. The OpsCenter dashboard can be configured to visualize the Amazon CloudWatch metrics associated with the EC2 instances and their EBS volumes. By reviewing the dashboard periodically, usage patterns can be identified, and EC2 instances can be right-sized based on the peaks in the metrics.

upvoted 1 times

✉ **God_Is_Love** 1 year, 1 month ago

Bro, install cost is 0. Simple linux command > sudo yum install amazon-cloudwatch-agent

upvoted 2 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: C

The correct answer is C. Installing the Amazon CloudWatch agent on each of the EC2 instances and turning on AWS Compute Optimizer allows the solutions architect to analyze the environment and make recommendations on the sizing of the EC2 instances in a cost-effective way. AWS Compute Optimizer analyzes the utilization of the instances and recommends the optimal instance types for the workloads. This solution is more

cost-effective than creating a dashboard and reviewing it periodically, or signing up for the AWS Enterprise Support plan and waiting for Trusted Advisor recommendations.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

C is correct, with computer optimizer

upvoted 1 times

Question #131

Topic 1

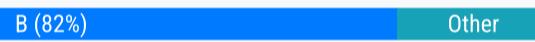
A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account.

The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the shared secrets. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- B. In the application account, create an IAM role that is named DBA-Secret. Grant the role the required permissions to access the secrets. In the DBA account, create an IAM role that is named DBA-Admin. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets
- C. In the DBA account create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account. In the application account, attach resource-based policies to the key to allow access from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- D. In the DBA account, create an IAM role that is named DBA-Admin. Grant the role the required permissions to access the secrets in the application account. Attach an SCP to the application account to allow access to the secrets from the DBA account. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

Correct Answer: A
Community vote distribution


bititan Highly Voted 1 year, 1 month ago

Selected Answer: B

Follow below link. It has both option to be used for this scenarios. But default kms key can not be used so B
<https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>
 upvoted 14 times

Sarutobi Highly Voted 11 months, 3 weeks ago

Selected Answer: B

Although I think B is the best, it is missing to mention of the trust policy in the application account.
 upvoted 5 times

ninomfr64 2 months, 2 weeks ago

Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account. This sounds like a trust policy to me
 upvoted 1 times

ninomfr64 Most Recent 2 months, 2 weeks ago

Selected Answer: B

A = Secret is not a RAM sharable resource. But who can recall this full list? Thus my reasoning is, I would expect more details for sharing via RAM like enable AWS Org sharing, assign permission (actions allowed on the shared resource) and select the external principal.
 B = correct see <https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>
 C = cannot cross-account access AWS managed KMS key as you do not have control on key policy
 D = SCP can only remove permissions. Even though an SCP doesn't prevent you from accessing a secret, you still need to have IAM user permission and/or resource based policy in place to actually access
 upvoted 1 times

 **horyoryo** 3 months, 2 weeks ago

option b

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **bjexamprep** 4 months ago

Selected Answer: B

Even B is the best answer among all the options, actually B is not correct. Without permission to access the KMS key, B cannot decrypt the secret.

upvoted 2 times

 **bjexamprep** 4 weeks ago

I was wrong. It is using AWS managed default encryption key, so it doesn't need the permission to access KMS key. The flaw of B is trust relationship policy.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: B

the Secrets Manager keys cannot be shared with RAM, key policy(resource policy) for the default KMS key managed by AWS cannot be changed, role is identity and can be granted access to assume other role

upvoted 1 times

 **rif** 5 months, 3 weeks ago

Answer is B.

Option A is wrong. AWS RAM can not share AWS Secrets Manager (see shareable resources in <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>)

upvoted 2 times

 **uC6rW1aB** 7 months ago

Selected Answer: A

Both Option A and Option B give repository administrators access to the repository and eliminate the need to manually share secrets.

Option A is a relatively simple process of sharing secrets with AWS RAM and setting up an IAM role within the DBA account.

Option B requires creating an IAM role in two different AWS accounts and setting cross-account permissions, which is a more complicated process.

So, while both A and B accomplish the goal, option A is simpler and more straightforward.

upvoted 1 times

 **chikorita** 7 months ago

who said we can share secrets using RAM??

i just checked under RAM and allowed sharable AWS services

AWS Secrets Manager is NOT one of those

Answer is B

upvoted 4 times

 **venvig** 7 months, 1 week ago

Selected Answer: B

As several people have highlighted, we refer to the blog <https://aws.amazon.com/blogs/database/design-patterns-to-access-cross-account-secrets-stored-in-aws-secrets-manager/>

Want to provide the following comment to emphasize why "C" is NOT even possible.

In Option C, its mentioned that the default AWS Managed CMK is used by the secrets manager.

We cannot provide any custom permissions to the AWS Managed CMK and by extension, its not possible to allow cross account access to it.

So, only Option B is valid.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

its a b

upvoted 1 times

 **Jackhemo** 10 months ago

Guys, you want to know the right answer? Copy paste the whole question to olabiba.ai

The answer is B

upvoted 1 times

 **OCHT** 11 months, 2 weeks ago

Selected Answer: A

Option A is the correct answer because it meets the requirement of giving the database administrators access to the database and eliminates the need to manually share the secrets. AWS Resource Access Manager (AWS RAM) enables you to share AWS resources with other accounts within your organization or organizational units (OUs) in AWS Organizations. By using AWS RAM to share the secrets from the application account with

the DBA account, you can eliminate the need for manual sharing of secrets.

Option B involves creating an IAM role in the application account and another IAM role in the DBA account. The DBA-Admin role in the DBA account would need to assume the DBA-Secret role in the application account to access the secrets. This approach adds complexity and does not eliminate the need for manual sharing of secrets.

In summary, Option A is a simpler and more efficient solution that meets the requirements.

upvoted 2 times

 **Maria2023** 9 months, 3 weeks ago

I couldn't find any option to share Secret Manager resources via RAM, did anyone try it?

upvoted 3 times

 **dev112233xx** 1 year ago

Selected Answer: B

B is correct, D doesn't make sense! SCP doesn't give any permission.. it just defines what can be allowed. you still need an IAM role/policy

upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: B

B is the best choice

upvoted 2 times

 **DWsk** 1 year ago

Selected Answer: B

Has to be B because C is not possible.

I get that you can't share access to the default KMS key, but how does it work to share access through a cross account role? How does the role in the DBA account decrypt the secrets that are encrypted by the default key if the role doesn't have permissions to that key?

upvoted 4 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: B

cross account assume role

upvoted 2 times

Question #132

Topic 1

A company manages multiple AWS accounts by using AWS Organizations. Under the root OU, the company has two OUs: Research and DataOps.

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types.

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create an IAM role in one account under the DataOps OU. Use the ec2:InstanceType condition key in an inline policy on the role to restrict access to specific instance type.
- B. Create an IAM user in all accounts under the root OU. Use the aws:RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
- D. Create an SCP. Use the ec2:Region condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU, the DataOps OU, and the Research OU.
- E. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

Correct Answer: CE
Community vote distribution

 CE (100%)

 **career360guru** 3 months, 2 weeks ago

Selected Answer: CE

Option C & E

upvoted 1 times

 **venvig** 7 months, 1 week ago

Selected Answer: CE

Very straightforward

upvoted 2 times

 **dtha1002** 8 months, 2 weeks ago

Selected Answer: CE

C for all resources region
and E for DataOps OU launch instance type

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: CE

its CE

upvoted 1 times

 **OCHT** 1 year ago

Selected Answer: CE

C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU. This will ensure that all resources deployed in the organization reside in the ap-northeast-1 Region.

E. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU. This will ensure that EC2 instances deployed in the DataOps OU use only the predefined list of instance types.

upvoted 4 times

 **OCHT** 1 year ago

Option D is incorrect because it suggests using the ec2:Region condition key to restrict access to all AWS Regions except ap-northeast-1. However, the ec2:Region condition key is not a valid condition key for EC2 actions. Instead, the aws:RequestedRegion condition key should be used to restrict access to specific AWS Regions.

Additionally, applying the SCP to the root OU, the DataOps OU, and the Research OU is unnecessary because applying the SCP to the root

OU alone will ensure that the restriction applies to all accounts in the organization, including those in the DataOps and Research OUs.

In summary, option D is incorrect because it suggests using an invalid condition key and because applying the SCP to multiple OUs is unnecessary.

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: CE

SCP's are the most efficient here

upvoted 1 times

✉ **tatdatpham** 1 year, 2 months ago

Selected Answer: CE

With AWS Org, consider SCP first.

In this scenario, Only C,D,E are mention about SCP, but D apply for all, not only the DataOps OU

upvoted 4 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: CE

The correct options are C and E.

Option C: Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.

This option is correct because it allows the company to restrict access to all AWS regions except for ap-northeast-1. This ensures that all resources deployed in the organization must reside in the ap-northeast-1 region. By applying the SCP to the root OU, it ensures that all accounts and OUs under the root will be affected.

Option E: Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

This option is correct because it allows the company to restrict access to specific instance types, which is required for the DataOps OU. By applying the SCP to the DataOps OU, it ensures that only resources deployed in the DataOps OU will be affected by the restriction.

upvoted 3 times

✉ **masetromain** 1 year, 2 months ago

Option A is incorrect because it only restricts access to specific instance types, but it does not restrict access to a specific region.

Option B is incorrect because it is applied to IAM users rather than OUs, which would not effectively apply the restriction to all resources in the organization.

Option D is incorrect because it uses the ec2:Region condition key which would not allow to restrict the instances types only in the DataOps OU.

By creating an SCP that uses the aws:RequestedRegion condition key and restricting access to all regions except ap-northeast-1 and applying it to the root OU, this ensures that all resources deployed in the organization will reside in the ap-northeast-1 Region.

By creating an SCP that uses the ec2:InstanceType condition key and restricts access to specific instance types and applying it to the DataOps OU, this ensures that all EC2 instances deployed in the DataOps OU will use the predefined list of instance types.

upvoted 1 times

✉ **zhangyu20000** 1 year, 2 months ago

CE is correct

upvoted 1 times

Question #133

Topic 1

A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket.

The company wants to process each URL in other Regions to compare possible differences in site localization. URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region.

Which combination of changes will produce multi-Region deployment that meets these requirements? (Choose two.)

- A. Deploy the SQS queue with the Lambda function to other Regions.
- B. Subscribe the SNS topic in each Region to the SQS queue.
- C. Subscribe the SQS queue in each Region to the SNS topic.
- D. Configure the SQS queue to publish URLs to SNS topics in each Region.
- E. Deploy the SNS topic and the Lambda function to other Regions.

Correct Answer: AC

Community vote distribution

AC (100%)

✉️  **SeemaDataReader** 2 months, 2 weeks ago

Selected Answer: AC

SNS in Region A, SQS + Lambda in Region A & B, S3 Bucket in Region A
upvoted 1 times

✉️  **career360guru** 3 months, 2 weeks ago

Selected Answer: AC

A and C
upvoted 1 times

✉️  **Passeexam4sure_com** 5 months, 4 weeks ago

Selected Answer: AC

Deploy the SQS queue with the Lambda function to other Regions.
Subscribe the SQS queue in each Region to the SNS topic.
upvoted 3 times

✉️  **rif** 5 months, 4 weeks ago

AC.
Amazon SNS supports cross-region deliveries.
<https://docs.aws.amazon.com/sns/latest/dg/sns-cross-region-delivery.html>
upvoted 4 times

✉️  **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: AC

SNS being the publisher, SQS is subscribing
upvoted 4 times

✉️  **NikkyDicky** 9 months, 1 week ago

Selected Answer: AC

It's an AC
upvoted 2 times

✉️  **Maria2023** 9 months, 3 weeks ago

Selected Answer: AC

Basically, you need to replicate it all except the bucket in the other regions. The question is explained very vaguely however
upvoted 2 times

✉️  **awsleffe** 2 days, 15 hours ago

SNS is the publisher and must stay in same region
upvoted 1 times

✉️ **Parsons** 11 months, 2 weeks ago

Selected Answer: AC

A, C is correct.
It looks like Fan out pattern.
upvoted 3 times

✉️ **Kampton** 11 months, 3 weeks ago

Why would need to deploy SQS with Lambda? Makes no sense! It's BE.
upvoted 1 times

✉️ **Diego1414** 11 months, 1 week ago

It's SNS that publishes not SQS
upvoted 1 times

✉️ **Asagumo** 1 year ago

What does it mean in Option A that Lambda deploys SQS?
upvoted 1 times

✉️ **mfsec** 1 year ago

Selected Answer: AC

AC - SQS
upvoted 2 times

✉️ **Zek** 1 year, 1 month ago

support A,C. <https://www.examtopics.com/discussions/amazon/view/74009-exam-aws-certified-solutions-architect-professional-topic-1/>
upvoted 1 times

✉️ **MasterP007** 1 year, 2 months ago

A & C - Deploy & Subscribe SQS.
upvoted 1 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: AC

A and C
upvoted 3 times

✉️ **masetromain** 1 year, 2 months ago

Selected Answer: AC

Option A is correct because deploying the SQS queue with the Lambda function to other regions will allow the application to process URLs in those regions and compare differences in site localization.

Option C is correct because subscribing the SQS queue in each region to the SNS topic in the existing region will allow the application to publish URLs to the existing SNS topic and have those URLs processed in other regions.

Option B is incorrect because subscribing the SNS topic in each region to the SQS queue in the existing region would not allow URLs to be processed in other regions.

Option D is incorrect because configuring the SQS queue to publish URLs to SNS topics in each region would not ensure that the URLs are processed in those regions.

Option E is incorrect because deploying the SNS topic and Lambda function to other regions without the SQS queue would not allow the application to process URLs in those regions.

upvoted 3 times

✉️ **zhangyu20000** 1 year, 2 months ago

AC is correct
upvoted 1 times

Question #134

Topic 1

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instances. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution.

Which strategy should the solutions architect use?

- A. Use AWS Lambda to run the application. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- B. Use AWS Batch to run the application. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- D. Use Amazon EC2 Spot Instances to run the application. Use AWS CodeDeploy to deploy and run the application every 4 hours.

Correct Answer: C

Community vote distribution



✉ **zhangyu20000** Highly Voted 1 year, 2 months ago
C is correct. only eventbridge can run scheduled task
upvoted 12 times

✉ **TonytheTiger** Most Recent 4 days, 11 hours ago
Option C : <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/run-event-driven-and-scheduled-workloads-at-scale-with-aws-fargate.html>
upvoted 1 times

✉ **ninomfr64** 2 months, 2 weeks ago
A = CW Log cannot invoke lambda every 4 hours
B = Step Function cannot invoke batch job every 4 hour (unless you use an EventBridge scheduled event)
C = correct (but I do not like when Fargate is mentioned as a standalone service, as it is a serverless compute option for some services)
D = CodeDeploy cannot run an application every 4 hours
upvoted 1 times

✉ **cox1960** 2 months, 3 weeks ago
none. "highly CPU intensive" means no Fargate. scheduling means eventbridge.
upvoted 1 times

✉ **holymancolin** 3 months ago
<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-lambda-supports-functions-that-can-run-up-to-15-minutes/>
Lambda's max running time is 15 mins, cannot support up to 20mins application.
upvoted 1 times

✉ **haha001** 3 months, 1 week ago
<https://aws.amazon.com/tutorials/scheduling-a-serverless-workflow-step-functions-amazon-eventbridge-scheduler/>
Step Function cannot schedule a job. Step Function needs EventBridge as the scheduler.
upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago
Selected Answer: C
B is not possible as Step Function can not be used to run scheduled a job every 4 hour
upvoted 1 times

✉ **task_7** 6 months, 2 weeks ago
Selected Answer: D
containers are well-suited for applications that are built in microservices architecture, where each service is a self-contained unit that performs a specific task. These types of applications are typically designed to be scalable and easy to deploy, making them a good fit for containerization.
I feel D is the best option
upvoted 2 times

✉ **teo2157** 1 month, 1 week ago
you can't guarantee with spot instances that they're available every 4 hours, C is the answer
upvoted 2 times

✉ **uC6rW1aB** 7 months ago
Selected Answer: C

I think Both B , C is missing some key point

Option B does not explain how to AWS Step Functions to trigger an AWS Batch job regularly, in this case 4 hours per run.

Option C does not explain how to use EventBridge to call the Fargate task, which is not native support, it might involve Lambda to achieve.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C. schedule -> eventbridge

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

Selected Answer: C

If there wasn't a schedule element I would choose AWS Batch because it pretty much loads a container and does the job, especially since it's like a 20-minute job. However the step functions part doesn't help with the scheduling part, hence I go for C

upvoted 4 times

 **rbm2023** 10 months, 3 weeks ago

Selected Answer: C

The application is a Linux binary which can be packaged into a container, then run on AWS Fargate and scheduled using Event Bridge.

Use a base image that matches your application's runtime environment

FROM ubuntu:latest

Copy the Linux binary into the container

COPY myapp /usr/local/bin/myapp

Set the entry point to execute the binary

ENTRYPOINT ["/usr/local/bin/myapp"]

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: C

C - Fargate is the best choice here

upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: C

C. Use AWS Fargate to run the application. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.

AWS Fargate is a serverless compute engine for containers that allows running containerized workloads without managing the underlying EC2 instances. This eliminates the need to provision, configure, and scale clusters of virtual machines to run containers.

Amazon EventBridge (formerly CloudWatch Events) allows scheduling tasks using cron or rate expressions, which can be used to invoke the Fargate task every 4 hours. This will allow for cost-effective and scalable solution, as the infrastructure is managed by AWS and the application can run in a serverless fashion, only incurring costs when the task is running.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

The other options are not appropriate in this scenario:

Option A: Running the application on AWS Lambda would not be appropriate, as Lambda is designed to run event-driven, short-lived functions, and not CPU-intensive, long-running tasks.

Option B: AWS Batch is a service for running batch jobs, and it may not be the most appropriate service for this scenario, as the application is not a batch job but a long running task.

Option D: Using Amazon EC2 Spot Instances would not be the best option for this scenario because the application is running for up to 20 minutes and EC2 Spot instances can be terminated at any time.

upvoted 4 times

Question #135

Topic 1

A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch. Currently, the game consists of the following components deployed in a single AWS Region:

- Amazon S3 bucket that stores game assets
- Amazon DynamoDB table that stores player scores

A solutions architect needs to design a multi-Region solution that will reduce latency, improve reliability, and require the least effort to implement.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Cross-Region Replication. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.
- B. Create an Amazon CloudFront distribution to serve assets from the S3 bucket. Configure S3 Same-Region Replication. Create a new DynamoDB table in a new Region. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC).
- C. Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
- D. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets. Create a new DynamoDB table in a new Region. Use the new table as a replica target for DynamoDB global tables.

Correct Answer: C

Community vote distribution



zozza2023 1 year, 2 months ago

Selected Answer: C

DynamoDB global tables + S3 replication+Cloudfront
upvoted 13 times

masetromain 1 year, 2 months ago

Option C is the correct answer because it meets the requirements of reducing latency, improving reliability and requiring minimal effort to implement.

By creating another S3 bucket in a new Region, and configuring S3 Cross-Region Replication between the buckets, the game assets will be replicated to the new Region, reducing latency for users accessing the assets from that region. Additionally, by creating an Amazon CloudFront distribution and configuring origin failover with two origins accessing the S3 buckets in each Region, it ensures that the game assets will be served to users even if one of the regions becomes unavailable.

Configuring DynamoDB global tables by enabling Amazon DynamoDB Streams, and adding a replica table in a new Region, will also improve reliability by allowing the player scores to be replicated and updated in multiple regions, ensuring that the scores are available even in the event of a regional failure.

upvoted 5 times

masetromain 1 year, 2 months ago

Option A is not correct because using the new table as a replica target for DynamoDB global tables will not improve reliability. The same applies for Option D, which only uses S3 Same-Region Replication, which will not reduce latency for users in other regions.

Option B is not correct because configuring asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC) is not the best solution for this use case. It would require additional configuration and management effort.

upvoted 2 times

ninomfr64 2 months, 2 weeks ago

Selected Answer: C

A = "Configure S3 Cross-Region Replication" but doesn't create a new bucket in another region.

B = "Configure S3 Same-Region Replication" without creating a second bucket and this should be cross-region. AWS DMS with CDC is not a good fit here, global table is the right option here

C = correct

D = we need the new bucket in a different region

upvoted 1 times

✉ career360guru 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 2 times

✉ shaaam80 4 months ago

Selected Answer: C

Answer C.

Regarding DynamoDB Streams -

Global tables use DynamoDB Streams to replicate data across different Regions. When you create a replica for a global table, a stream is created by default. Any changes to a replica are replicated to all the other replicas within the same global table within a second using DynamoDB Streams.

upvoted 1 times

✉ blackgamer 5 months ago

The answer is A. C added unnecessary complexities such as Amazon DynamoDB Streams and Origin Failover.

upvoted 1 times

✉ ninomfr64 2 months, 2 weeks ago

Option A doesn't mention creating a new bucket in a different region

upvoted 1 times

✉ Jay_2pt0_1 4 months, 3 weeks ago

I initially thought it was C, but I was torn between A and C. You may be right.

upvoted 1 times

✉ uC6rW1aB 7 months ago

Selected Answer: A

other option are incorrect.

B: Configure S3 Same-Region Replication.---> It's not meet multi-region requirement.

C: Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Region. ---> It's not support for this kinda failover

D: Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets. ---> It's not meet multi-region requirement.

upvoted 2 times

✉ ninomfr64 2 months, 2 weeks ago

C is correct, Origin Group allows failover see

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

upvoted 1 times

✉ dkcloudfguru 7 months ago

option c is the easiest way to do

upvoted 1 times

✉ ProMax 7 months, 1 week ago

Selected Answer: A

Creating an Amazon CloudFront distribution will reduce latency for global users by serving assets from the closest edge location. S3 Cross-Region Replication will ensure that game assets are available in another region, improving reliability. Creating a new DynamoDB table in a new region and using it as a replica target for DynamoDB global tables will enable multi-region replication, improving reliability.

upvoted 1 times

✉ SK_Tyagi 7 months, 3 weeks ago

Selected Answer: C

Option C has another differentiator - DynamoDBStreams that will assist in Reliability

upvoted 1 times

✉ ggrodskiy 8 months, 2 weeks ago

Correct A.

CloudFront does not support origin failover with two origins accessing the S3 buckets in each Region. According to the AWS documentationhttps://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html, origin failover only works within the same Region, not across Regions. This means that you can only configure origin failover with two origins that are in the same Region as the CloudFront distribution. If you want to use origin failover with S3 buckets in different Regions, you need to create multiple CloudFront distributions, one for each Region, and configure them to use the same domain name with geolocation routing<https://blog.ippon.tech/when-a-cloudfront-origin-must-fail-for-testing-high-availability/>.

upvoted 1 times

✉ venvig 7 months, 1 week ago

Referred to your AWS doc link. I don't see any condition that states that the origins in the origin group cannot be from two different regions.

Can you provide the statement from the AWS doc that you are referring to please ?

upvoted 1 times

✉ NikkyDicky 9 months, 1 week ago

Selected Answer: C

weird question wording, but C fit more
upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: C

Create another S3 bucket in a new Region, and configure S3 Cross-Region Replication between the buckets
upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

C is correct. S3 cross replicate, CloudFront, Dynamodb global database and origin failover
upvoted 2 times

Question #136

Topic 1

A company has an on-premises website application that provides real estate information for potential renters and buyers. The website uses a Java backend and a NoSQL MongoDB database to store subscriber data.

The company needs to migrate the entire application to AWS with a similar structure. The application must be deployed for high availability, and the company cannot make changes to the application.

Which solution will meet these requirements?

- A. Use an Amazon Aurora DB cluster as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- B. Use MongoDB on Amazon EC2 instances as the database for the subscriber data. Deploy EC2 instances in an Auto Scaling group in a single Availability Zone for the Java backend application.
- C. Configure Amazon DocumentDB (with MongoDB compatibility) with appropriately sized instances in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.
- D. Configure Amazon DocumentDB (with MongoDB compatibility) in on-demand capacity mode in multiple Availability Zones as the database for the subscriber data. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones for the Java backend application.

Correct Answer: D

Community vote distribution



✉ uC6rW1aB 7 months ago

Selected Answer: C

C correct
DocumentDB only have on-demand instance but not on-demand capacity mode, the mode is for DynamoDB
upvoted 10 times

✉ gofavad926 3 weeks, 2 days ago

Selected Answer: C

C, documented. No exists the on-demand capacity mode
upvoted 1 times

✉ AimarLeo 2 months, 1 week ago

'Appropriately sized instances' Means on-demand ? that is quite vague..
upvoted 1 times

✉ ninomfr64 2 months, 2 weeks ago

Selected Answer: C

A = Aurora supports MySQL and PostgreSQL, not MongoDB. App changes are not allowed
B = This could work but DocumentDB provides managed MongoDB instance that is preferable
C = correct
D = there isn't on-demand capacity mode, in 2022 launched MondoDB Elastic Cluster that eliminates the need to choose, manage or upgrade instances and allows to scale up to 4PiB storage whereas instance based scales up to 128TiB.

I thing this question is pre elastic cluster as this is ambiguous between C and D

upvoted 1 times

✉ jpa8300 3 months ago

Selected Answer: D

DocumentDB does indeed support on-demand capacity mode (Contrary to what other users say here)
<https://aws.amazon.com/blogs/database/running-spiky-workloads-and-optimizing-costs-by-more-than-90-using-amazon-dynamodb-on-demand-capacity-mode/>

On-Demand is ideally to a use case where you have unpredictable or variable database workloads, like this case, it is not said anywhere the expected workload, so it is better to start with On-demand , and later when you know the workload you can cahnge it.

upvoted 1 times

✉ buriz 2 months, 4 weeks ago

what you have linked here is a dynamodb article not a documentDB one, documentDB does not support on-demand capacity mode -
<https://aws.amazon.com/documentdb/faqs/>

"You can scale the compute resources allocated to your instance in the AWS Management Console by selecting the desired instance and clicking the "modify" button. Memory and CPU resources are modified by changing your instance class."

upvoted 1 times

✉ **ninomfr64** 2 months, 2 weeks ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see <https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

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

This is DynamoDB, not DocumentDB. The choices only mention DocumentDB.

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: C

There is no on-demand capacity mode for DocumentDB, though there is on-demand vCPU based pricing available.

upvoted 1 times

✉ **ninomfr64** 2 months, 2 weeks ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see <https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

✉ **ProMax** 7 months, 1 week ago

Selected Answer: C

Amazon DocumentDB does NOT have on-demand capacity mode, so its option C.

upvoted 3 times

✉ **ninomfr64** 2 months, 2 weeks ago

There is no on-demand capacity for DocumentDB, however Elastic Cluster option is provided "Elastic Clusters enables you to elastically scale your document database to handle millions of writes and reads, with petabytes of storage capacity" see <https://aws.amazon.com/documentdb/faqs/#:~:text=to%20learn%20more.-,Elastic%20Clusters,-What%20is%20Amazon>

upvoted 1 times

✉ **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: D

I was leaning towards Option C but "Appropriately sized instances" is vague since the question does not state the size of Mongo DB. On-demand instances serve the purpose here, they are offered by DocumentDB, see the link <https://aws.amazon.com/documentdb/pricing/>

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

its a c

upvoted 2 times

✉ **easystoo** 9 months, 3 weeks ago

C-C-C-C-C-C-C

On-demand capacity mode as suggested in D may not provide the same level of high availability as multi-Availability Zone deployments. So it's C-C-C-C-C-C-C for me.

upvoted 2 times

✉ **SkyZeroZx** 10 months ago

Selected Answer: C

See best practices for amazon documentdb - instance sizing in docs.

Additionally there is no on-demand capacity mode.

upvoted 2 times

✉ **F_Eldin** 10 months, 3 weeks ago

Selected Answer: C

DocumentDB does indeed support on-demand capacity mode (Contrary to what other users say here)

<https://aws.amazon.com/blogs/database/running-spiky-workloads-and-optimizing-costs-by-more-than-90-using-amazon-dynamodb-on-demand-capacity-mode/>

but this mode is good for spiky workloads and does not address the high availability requirement

upvoted 3 times

✉ **F_Eldin** 10 months, 3 weeks ago

The correct link <https://www.appliytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/743016963590682>

upvoted 2 times

✉️ [Removed] 4 months, 3 weeks ago

The content mentioned in your link and the original comment are both mentioning things related to DynamoDB. Your link is even worse which is describing DynamoDB but say it is for DocumentDB. Please study hard

upvoted 1 times

✉️ leehjworking 10 months, 3 weeks ago

Selected Answer: C

See best practices for amazon documentdb - instance sizing in docs.

upvoted 1 times

✉️ Sarutobi 11 months, 3 weeks ago

Selected Answer: C

Going wit C. I still call the DocumentDB used in mode C "on-demand mode" because you have to select the Ec2 instance; the pricing documentation still uses that name. There is an Elastic cluster for DocumentDB. Could it be that option D "on-demand capacity mode" is referring to Elastic mode?

upvoted 2 times

✉️ OCHT 12 months ago

Selected Answer: C

Amazon DocumentDB does not support an on-demand capacity mode. You can only choose from different instance classes that have fixed compute and memory resources. However, you can scale your instances up or down as needed, and you can also pause and resume your instances to save costs. Amazon DocumentDB also automatically scales your storage and I/O based on your data size and workload.

upvoted 1 times

✉️ mfsec 1 year ago

Selected Answer: C

C - there is no on-demand capacity mode.

upvoted 1 times

✉️ zejou1 1 year ago

Selected Answer: C

Amazon DocumentDB best practice to choose an instance type with enough RAM to fit your working set (i.e., data and indexes) in memory. Having properly sized instances will help optimize for overall performance and potentially minimize I/O cost.
https://docs.aws.amazon.com/documentdb/latest/developerguide/best_practices.html

Also, you would already need to have it as on-demand; first thing is to size it appropriately

upvoted 1 times

Question #137

Topic 1

A digital marketing company has multiple AWS accounts that belong to various teams. The creative team uses an Amazon S3 bucket in its AWS account to securely store images and media files that are used as content for the company's marketing campaigns. The creative team wants to share the S3 bucket with the strategy team so that the strategy team can view the objects.

A solutions architect has created an IAM role that is named `strategy_reviewer` in the Strategy account. The solutions architect also has set up a custom AWS Key Management Service (AWS KMS) key in the Creative account and has associated the key with the S3 bucket. However, when users from the Strategy account assume the IAM role and try to access objects in the S3 bucket, they receive an Access Denied error.

The solutions architect must ensure that users in the Strategy account can access the S3 bucket. The solution must provide these users with only the minimum permissions that they need.

Which combination of steps should the solutions architect take to meet these requirements? (Choose three.)

- A. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to the account ID of the Strategy account.
- B. Update the `strategy_reviewer` IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.
- C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the `strategy_reviewer` IAM role.
- D. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to an anonymous user.
- E. Update the custom KMS key policy in the Creative account to grant encrypt permissions to the `strategy_reviewer` IAM role.
- F. Update the `strategy_reviewer` IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.

Correct Answer: BCF*Community vote distribution*

ACF (100%)

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: ACF

B wrong - full permissions ? when question asks for minimum permissions.
 D wrong - anonymous user ? anonymous does not work
 E wrong - encrypt permissions ? No Strategy account needs decrypt permissions
 So, A,C,F

upvoted 12 times

 **God_Is_Love** 1 year, 1 month ago

first the source bucket needs to give grant access thru bucket policy and KMS key policy (A,C options)
 Secondly, Strategy IAM role needs to give access to read from S3 bucket and also KMS key (Option F)

upvoted 3 times

 **leehjworking**  10 months, 3 weeks ago

Selected Answer: ACF

B full permission ? X
 D anonymous? X
 E encryption not needed for strategy team

upvoted 6 times

 **career360guru**  3 months, 2 weeks ago

Selected Answer: ACF

A, C and F

upvoted 1 times

 **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: ACF

By rule of elimination
 BDE are wrong. God_Is_Love is spot on

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: ACF

its ACF

upvoted 2 times

OCHT 1 year ago

Selected Answer: ACF

Option B suggests updating the strategy_reviewer IAM role to grant full permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key. This option is not ideal because it grants more permissions than necessary. The requirement is to provide users with only the minimum permissions they need to view objects in the S3 bucket.

Option D suggests creating a bucket policy that includes read permissions for the S3 bucket and setting the principal of the bucket policy to an anonymous user. This option is not ideal because it would allow anyone to read objects in the S3 bucket, which could pose a security risk.

Option E suggests updating the custom KMS key policy in the Creative account to grant encrypt permissions to the strategy_reviewer IAM role. This option is not necessary because the requirement is for users in the Strategy account to be able to view objects in the S3 bucket, not to encrypt them.

upvoted 3 times

mfsec 1 year ago

Selected Answer: ACF

ACF is the best choice

upvoted 2 times

taer 1 year ago

Selected Answer: ACF

A. Create a bucket policy that includes read permissions for the S3 bucket. Set the principal of the bucket policy to the account ID of the Strategy account.

C. Update the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role.

F. Update the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key.

upvoted 2 times

zozza2023 1 year, 2 months ago

Selected Answer: ACF

A C AND F

upvoted 3 times

Untamables 1 year, 2 months ago

Selected Answer: ACF

<https://repost.aws/knowledge-center/cross-account-access-denied-error-s3>

upvoted 3 times

masetromain 1 year, 2 months ago

Selected Answer: ACF

A, C, and F are the correct options.

upvoted 4 times

masetromain 1 year, 2 months ago

A, C, and F are the correct options.

Option A creates a bucket policy that includes read permissions for the S3 bucket and sets the principal of the bucket policy to the account ID of the Strategy account. This ensures that users in the Strategy account have the necessary permissions to access the S3 bucket.

Option C updates the custom KMS key policy in the Creative account to grant decrypt permissions to the strategy_reviewer IAM role. This ensures that the users in the Strategy account have the necessary permissions to decrypt the objects stored in the S3 bucket.

Option F updates the strategy_reviewer IAM role to grant read permissions for the S3 bucket and to grant decrypt permissions for the custom KMS key. This ensures that the users in the Strategy account have the necessary permissions to read the objects in the S3 bucket and to decrypt them using the custom KMS key.

The other options are not correct because they either grant unnecessary permissions (B, D) or grant permissions in the wrong way (E).

upvoted 2 times

zhangyu20000 1 year, 2 months ago

ACF is correct

upvoted 2 times

Question #138

Topic 1

A life sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data center to process genomics data. Sequencing data is generated and stored on a local storage area network (SAN), and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turnaround time from weeks to days.

The company has a high-speed AWS Direct Connect connection. Sequencers will generate around 200 GB of data for each genome, and individual jobs can take several hours to process the data with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day.

Which solution meets these requirements?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.
- C. Use AWS DataSync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow. Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data.

Correct Answer: C

Community vote distribution

C (76%)

D (24%)

 **dev112233xx**  1 year ago

Selected Answer: C

Almost voted D because of the Storage Gateway + SAN combination.. but seems like it's not correct since S3 events cannot trigger Batch jobs directly, you need a Lambda function! S3 events can be only Lambda,SNS or SQS..

upvoted 18 times

 **Kampton** 11 months, 3 weeks ago

Agree - The Lambda function acts as a bridge between the S3 event and AWS Batch, allowing you to trigger AWS Batch jobs in response to S3 events.

upvoted 3 times

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: D

Guys its Tricky one between C and D and answer is D! (Modernization question)

Look at this two below blogs :

<https://aws.amazon.com/blogs/storage/using-aws-storage-gateway-to-modernize-next-generation-sequencing-workflows/>

Thanks to tinyflame who made me do my research on this :-)

Yes, SAN -> Storage Gateway Only

NAS -> Data Sync or Storage Gateway

<https://aws.amazon.com/blogs/storage/from-on-premises-to-aws-hybrid-cloud-architecture-for-network-file-shares/>

upvoted 8 times

 **God_Is_Love** 1 year, 1 month ago

On Premise NAS and file servers to S3. --> Use DataSync solution

On Premise SMB or NFS file share to S3 --> Use Storage/File Gateway solution

upvoted 4 times

 **titi_r** 3 weeks, 2 days ago

@God_Is_Love, both articles you've provided are NOT mentioning "SAN" at all. You cannot copy data from SAN using storage GW, but you do it with DataSync ran from within a server, which is connected to that SAN. Research more on what SAN is and how does it work :)

upvoted 1 times

 **ninomfr64**  2 months, 2 weeks ago

Selected Answer: C

A = 200GB very now and then doesn't need Snowball Edge
B = Data Pipeline is ETL and not suitable in hybrid scenarios
C = correct (DataSync does the job, also the app is already container based and it works well with Batch that is suited for HPC kind of workload - genomic sequencing is a typical HPC workload)
D = even tough Storage Gateway does the job you cannot directly trigger a AWS Batch job from an S3 event, you need either a Lambda in the middle or enable EventBridge notification and create a rule that triggers the AWS Batch Job

upvoted 2 times

✉ **cox1960** 2 months, 3 weeks ago

... "The main requirement is that the data needs to be accessible over the network in a file format like NFS that DataSync supports."

upvoted 1 times

✉ **cox1960** 2 months, 3 weeks ago

C - Amazon Q says "While it does not directly support SAN (storage area network), you can use AWS DataSync to transfer data from files stored on a SAN volume to AWS storage services like Amazon S3."

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C is better option. Though D is also possible but as the jobs are already container based C would be better.
Question is not clear whether containers used on-premise are docker based containers.

upvoted 2 times

✉ **mosalahs** 3 months, 2 weeks ago

Selected Answer: C

Data Transfer --- > Data Sync
Data Integration --- > Storage GW
Data Orchestration --- > Data Pipeline

upvoted 2 times

✉ **Maygam** 4 months ago

Selected Answer: C

D doesn't seem to be correct as AWS Batch is not a destination for AWS S3 events.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>

upvoted 2 times

✉ **uC6rW1aB** 7 months ago

Selected Answer: C

Option C: Use AWS DataSync to transfer data to Amazon S3. DataSync is designed for fast, easy and secure data transfer. This option also uses S3 events to trigger an AWS Lambda function, which launches an AWS Step Functions workflow and runs a Docker container using AWS Batch. This option takes into account data transfer, processing and container management, and should be the most suitable solution.
Option D: Use AWS Storage Gateway's file gateway to transfer data to Amazon S3. Storage Gateway is suitable for hybrid cloud environments, but in this case, since the company already has a high-speed AWS Direct Connect connection, it will be more efficient to use DataSync.

upvoted 1 times

✉ **Ganshank** 7 months, 3 weeks ago

C.

Of the given options C is probably the closest. Step Functions can be used to model the workflow. D does not specify this. DataSync can be used to transfer data [<https://docs.aws.amazon.com/datasync/latest/userguide/s3-cross-account-transfer.html>].

upvoted 1 times

✉ **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: D

I choose D. My rationale - 200GB data for 1 genome sequence, Lets say DirectConnect is 1Gbps line, DataSync cannot efficiently transfer the data to get the processing under 1 day.

Agree with God_Is_Love's hypothesis

upvoted 1 times

✉ **vn_thanh tung** 7 months, 1 week ago

S3 event can't trigger direct AWS Batch job. => C

upvoted 1 times

✉ **nynomfr64** 2 months, 2 weeks ago

Assuming DX is 1Gbps, it takes about 27 minutes to transfer 200GB. also, I don't see how Storage Gateway can speedup things. My point is that here both DataSync and Storage Gateway can do the job, but you cannot trigger Batch job directly from S3 object event. Thus C

upvoted 1 times

✉ **RGR21** 8 months ago

Does the AWS DataSync support SAN?

upvoted 1 times

✉ **ggrodsckiy** 8 months, 2 weeks ago

Correct D.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C

D would be an option if using volume gateway and lambda to trigger batch
datasync dont need to support NAS. agent can copy off of NFS or SMB mount of the NAS drive.

upvoted 1 times

 **Jackhemo** 9 months, 3 weeks ago

Selected Answer: C

I answered D, but Olabiba.ai says C, because:
Here's why option C is the most suitable choice:

Overall, option C provides a scalable and efficient solution for the company to process genomics data on AWS, meeting their capacity and turnaround time requirements.

upvoted 1 times

 **Buggie** 10 months ago

Lambda can run only for 15 minutes.

upvoted 1 times

 **rbm2023** 10 months, 3 weeks ago

Selected Answer: C

You should use the datasync option. The option that says, to use the S3 events to trigger the batch is not fully correct, you need a lambda in order to have this type of integration in this case option D is incorrect.

upvoted 1 times

Question #139

Topic 1

A company runs a content management application on a single Windows Amazon EC2 instance in a development environment. The application reads and writes static content to a 2 TB Amazon Elastic Block Store (Amazon EBS) volume that is attached to the instance as the root device. The company plans to deploy this application in production as a highly available and fault-tolerant solution that runs on at least three EC2 instances across multiple Availability Zones.

A solutions architect must design a solution that joins all the instances that run the application to an Active Directory domain. The solution also must implement Windows ACLs to control access to file contents. The application always must maintain exactly the same content on all running instances at any given point in time.

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

- A. Create an Amazon Elastic File System (Amazon EFS) file share. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application, join the instance to the AD domain, and mount the EFS file share.
- B. Create a new AMI from the current EC2 Instance that is running. Create an Amazon FSx for Lustre file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to join the instance to the AD domain and mount the FSx for Lustre file system.
- C. Create an Amazon FSx for Windows File Server file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application and mount the FSx for Windows File Server file system. Perform a seamless domain join to join the instance to the AD domain.
- D. Create a new AMI from the current EC2 instance that is running. Create an Amazon Elastic File System (Amazon EFS) file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three Instances. Perform a seamless domain join to join the instance to the AD domain.

Correct Answer: B

Community vote distribution

C (95%) 5%

God_Is_Love **Highly Voted** 1 year, 1 month ago

Selected Answer: C

EFS is Linux/Mac based, So, A,D are out.
Lustre stands for Linux cluster, So B is out. Left is C which is correct (Amazon FSx for Windows)

upvoted 13 times

rootcode **Most Recent** 2 months ago

Selected Answer: C

C is the correct option
upvoted 1 times

career360guru 3 months, 2 weeks ago

Selected Answer: C

Option C as it is windows based OS.
upvoted 1 times

uC6rW1aB 7 months ago

Selected Answer: C

Option B FSx for Lustre is not for Linux POSIX-compliant
Option C correct
upvoted 2 times

dkclougdguru 7 months ago

C FSx for windows is a good fit for this
upvoted 1 times

Sam202 9 months ago

FSx for Lustre can only be used by Linux-based instances.
upvoted 1 times

NikkyDicky 9 months, 1 week ago

Selected Answer: C

C for windows
upvoted 1 times

 **SkyZeroZx** 10 months ago

Selected Answer: C

EFS and FSx for Lustre == Linux
FSx Windows File == Windows
upvoted 2 times

 **mfsec** 1 year ago

Selected Answer: C

EFS and Windows is not straight forward. C is the best solution.
upvoted 2 times

 **zejou1** 1 year ago

Selected Answer: C

Amazon FSx is built on Windows Server... Access Control Lists (ACLs)... To control user access, Amazon FSx integrates with your on-premises Microsoft Active Directory as well as with AWS Microsoft Managed AD.
<https://aws.amazon.com/fsx/windows/features/?nc=sn&loc=2>

All others don't work - forget about the "least management" statement - it says "implement Windows ACLS to control..." all others are thrown out.

upvoted 3 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: C

Option D suggests using an EFS file system, which is a shared file system that can be mounted on multiple EC2 instances, but this requires additional configuration to keep the content in sync across all instances.

Option C is the optimal choice because Amazon FSx for Windows File Server supports Windows ACLs and seamlessly integrates with Active Directory to join instances to a domain. This option minimizes management overhead by reducing the complexity of managing multiple EFS file shares or writing scripts to synchronize content across EC2 instances.

upvoted 2 times

 **Musk** 1 year, 2 months ago

Selected Answer: C

FSX for WIndows is the only option. The rest of options are not supported.

upvoted 2 times

 **jojom19980** 1 year, 2 months ago

Selected Answer: C

FSx for Lustre can only be used by Linux-based instances.

upvoted 2 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: D

good answer are C or D but as it says LEAST management overhead ==> D as in C we will need a user data script

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

sorry D is uncorrect as it use Elastic File System (Amazon EFS) itch is not windows so Iswitch to C

upvoted 1 times

 **lxrdm** 9 months, 1 week ago

Also that means each instance launched from the AMI will have 2TB EBS volume.. which is not ideal

upvoted 1 times

 **ARLV** 1 year, 2 months ago

@masetromain is this a good exam study guide? Like how many questions were from here. Any help would be appreciated. Thank you
upvoted 1 times

 **Untamables** 1 year, 2 months ago

Selected Answer: C

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_join_instance.html
upvoted 1 times

 **masetromain** 1 year, 2 months ago

Selected Answer: C

I switch for C: Create an Amazon FSx for Windows File Server file system. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances. Implement a user data script to install the application and mount the FSx for Windows File Server file system. Perform a seamless domain join to join the instance to the AD domain.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

This solution meets the requirements with the least management overhead because it utilizes Amazon FSx for Windows File Server, which is a fully managed service that allows you to easily set up a highly available and scalable file server. The Auto Scaling group ensures that the application is running on at least three instances across multiple Availability Zones, providing high availability and fault tolerance. The user data script can be used to automate the setup and configuration of the instances when they are launched, and it can be used to join the instances to the AD domain, so that the instances can be managed and access to the file contents can be controlled using Windows ACLs.

upvoted 2 times

 **masetromain** 1 year, 2 months ago

The other choices are not correct because:

Option A: An Amazon Elastic File System (Amazon EFS) file share is not a windows file system and it does not support Windows ACLs.

Option B: Amazon FSx for Lustre is a high-performance file system optimized for compute-intensive workloads, it is not a windows file system and it does not support Windows ACLs.

Option D: An Amazon Elastic File System (Amazon EFS) file share is not a windows file system and it does not support Windows ACLs.

In both cases, creating a new AMI from the current EC2 instance that is running it doesn't help to solve the problem as it won't provide a scalable solution that runs on at least three instances across multiple Availability Zones.

upvoted 3 times

Question #140

Topic 1

A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer.

The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- B. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template in an Amazon S3 bucket. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the template. Use an SDK in the Lambda function to send the email message.
- C. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplace. Store the email template in Amazon Simple Email Service (Amazon SES) with parameters for the customer data. Create an AWS Lambda function to call the SES template and to pass customer data to replace the parameters. Use the AWS Marketplace SMTP server to send the email message.
- D. Set up Amazon Simple Email Service (Amazon SES) to send email messages. Store the email template on Amazon SES with parameters for the customer data. Create an AWS Lambda function to call the SendTemplatedEmail API operation and to pass customer data to replace the parameters and the email destination.

Correct Answer: B

Community vote distribution

D (97%)

✉️  **God_Is_Love**  1 year, 1 month ago

Selected Answer: D

SendTemplatedEmail
SendEmail
SendRawEmail are email api methods used in SES
upvoted 11 times

✉️  **masetromain**  1 year, 2 months ago

Selected Answer: D

The correct answer is D.

In this solution, the company can use Amazon SES to send email messages, which will minimize operational overhead as SES is a fully managed service that handles sending and receiving email messages. The company can store the email template on Amazon SES with parameters for the customer data and use an AWS Lambda function to call the SendTemplatedEmail API operation, passing in the customer data to replace the parameters and the email destination. This solution eliminates the need to set up and manage an SMTP server on EC2 instances, which can be costly and time-consuming.

Option A and B are not correct because it requires to set up an SMTP server on EC2 instances, which is not necessary and will increase operational overhead.

Option C is not correct because it stores the email template in Amazon SES with parameters for the customer data which is not possible.
upvoted 9 times

✉️  **Maria2023** 9 months, 3 weeks ago

Ok, so according to chatgpt C is not correct because "Option C is not correct because it stores the email template in Amazon SES with parameters for the customer data which is not possible."

However, D says exactly the same - so D is not correct as well?

Do not fully trust chatgp

upvoted 7 times

✉️  **titi_r** 3 weeks, 2 days ago

ChatGPT also is saying "Option A and B are not correct because it requires to set up an SMTP server on EC2 instances", but those options are "A" and "C", not "A" and "B". Seems there is some mismatch with the options.

upvoted 1 times

✉️  **career360guru**  3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ SK_Tyagi 7 months, 3 weeks ago

Selected Answer: D

D - Can send templated email with request parameters

upvoted 1 times

✉ Jonalb 9 months ago

Selected Answer: D

DDDDDDDD

upvoted 1 times

✉ NikkyDicky 9 months, 1 week ago

Selected Answer: D

its a d

upvoted 1 times

✉ Maria2023 9 months, 3 weeks ago

Selected Answer: B

I vote for B due to the fact that I cannot see an option to "Store the email template on Amazon SES with parameters for the customer data" Other than that it looks like a good option but it's just not working

upvoted 1 times

✉ SK_Tyagi 7 months, 3 weeks ago

https://docs.aws.amazon.com/ses/latest/APIReference-V2/API_CreateEmailTemplate.html

upvoted 1 times

✉ carpa_jo 3 months, 1 week ago

D is correct.

Regarding your concerns about email templates on SES with parameters see: <https://docs.aws.amazon.com/ses/latest/dg/send-personalized-email-api.html>

upvoted 1 times

✉ SkyZeroZx 9 months, 3 weeks ago

Selected Answer: D

keyword = SendTemplatedEmail API

upvoted 1 times

✉ mfsec 1 year ago

Selected Answer: D

Template - easy one.

upvoted 1 times

✉ zozza2023 1 year, 2 months ago

Selected Answer: D

D should be the answer

upvoted 3 times

✉ zhangyu20000 1 year, 2 months ago

D is correct - https://docs.aws.amazon.com/ses/latest/APIReference/API_SendTemplatedEmail.html

upvoted 2 times

Question #141

Topic 1

A company is processing videos in the AWS Cloud by Using Amazon EC2 instances in an Auto Scaling group. It takes 30 minutes to process a video. Several EC2 instances scale in and out depending on the number of videos in an Amazon Simple Queue Service (Amazon SQS) queue.

The company has configured the SQS queue with a redrive policy that specifies a target dead-letter queue and a maxReceiveCount of 1. The company has set the visibility timeout for the SQS queue to 1 hour. The company has set up an Amazon CloudWatch alarm to notify the development team when there are messages in the dead-letter queue.

Several times during the day, the development team receives notification that messages are in the dead-letter queue and that videos have not been processed properly. An investigation finds no errors in the application logs.

How can the company solve this problem?

- A. Turn on termination protection for the EC2 Instances
- B. Update the visibility timeout for the SQS queue to 3 hours
- C. Configure scale-in protection for the instances during processing
- D. Update the redrive policy and set maxReceiveCount to 0.

Correct Answer: D

Community vote distribution

C (75%) D (21%) 4%

 **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: C

The correct answer is C. The company can solve the problem by configuring scale-in protection for the instances during processing. This will ensure that the instances are not terminated while they are processing videos. This will prevent the messages from moving to the dead-letter queue and ensure that videos are processed properly.

Option A is incorrect because turning on termination protection for the EC2 instances will not solve the problem as it will impact the ability of the Auto Scaling group to scale instances in and out based on the number of videos in the queue.

Option B is incorrect because the company has specified a visibility timeout of 1 hour, which is enough time for the instances to process a video and there is no need to update the timeout to 3 hours.

Option D is incorrect because the company has set the maxReceiveCount to 1 and changing it to 0 will not solve the problem. maxReceiveCount allowed range is 1 to 1000.

upvoted 25 times

 **[Removed]** 8 months, 3 weeks ago

fully agree, option d is incorrect because 0 is an invalid value for maxReceiveCount

upvoted 1 times

 **Bwutch** 10 months, 3 weeks ago

ChatGPT confirms this reasoning.

upvoted 7 times

 **VerRi** Most Recent 1 month, 1 week ago

Selected Answer: D

If Option D is a typo, then D

upvoted 1 times

 **Greanny** 2 months, 1 week ago

B.

The best solution for this problem is to update the visibility timeout for the SQS queue to 3 hours. This is because when the visibility timeout is set to 1 hour, it means that if the EC2 instance doesn't process the message within an hour, it will be moved to the dead-letter queue. By increasing the visibility timeout to 3 hours, this should give the EC2 instance enough time to process the message before it gets moved to the dead-letter queue. Additionally, configuring scale-in protection for the EC2 instances during processing will help to ensure that the instances are not terminated while the messages are being processed.

upvoted 2 times

 **tmlong18** 2 months, 3 weeks ago

Selected Answer: D

Option D is a typo.

I seen the same question in udemy but the Option D is 10

upvoted 2 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C is correct.

upvoted 2 times

 **severlight** 4 months, 3 weeks ago

Selected Answer: C

setting MaxReceiveCount to 0 doesn't make and send and it impossible, because messages would be send to DLQ without any attempt to consume them from source queue

upvoted 1 times

 **Russ99** 6 months, 3 weeks ago

Selected Answer: D

checked 4 A1, C is definitely not the correct answer: Option C: Configuring scale-in protection for the instances during processing will not prevent messages from being moved to the dead-letter queue if they cannot be processed on the first attempt.

upvoted 1 times

 **venvig** 7 months, 1 week ago

Selected Answer: C

Refer <https://aws.amazon.com/blogs/aws/new-instance-protection-for-auto-scaling/>

From the above link, "an instance might be handling a long-running work task, perhaps pulled from an SQS queue. Protecting the instance from termination will avoid wasted work" - This is what the question is also alluding to.

This is how one would make use of the functionality.

You change the protection status of one or more instances by calling the SetInstanceProtection function. If you wanted to use this function to protect long-running, queue-driven worker processes from scale-in termination, you could set up your application as follows (this is pseudocode):

```
while (true)
{
    SetInstanceProtection(False);
    Work = GetNextWorkUnit();
    SetInstanceProtection(True);
    ProcessWorkUnit(Work);
    SetInstanceProtection(False);
}
```

upvoted 4 times

 **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: C

Going with C only because D has value of maxReceiveCount set to 0

upvoted 2 times

 **rtguru** 8 months, 3 weeks ago

I go with C

upvoted 1 times

 **YodaMaster** 9 months, 1 week ago

Selected Answer: B

B.

AWS "recommends setting your queue's visibility timeout to six times your function timeout" which makes 3 hours perfect.

source: <https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>

upvoted 2 times

 **ajeeshb** 4 weeks, 1 day ago

But this for a queue to use with lambda. Here it is EC2 in ASG

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

C more likely

upvoted 1 times

 **Maria2023** 9 months, 3 weeks ago

I couldn't find any way to configure scale-in protection for the instances during processing except to do it manually, which is going to be an insane exercise. Eventually, that can be done by the application as part of the processing but I would then expect some more context in the answer.

upvoted 1 times

 **dev112233xx** 10 months, 3 weeks ago

Selected Answer: D

D makes sense

I think D answer has a typo! probably they didn't copy the text properly

<https://repost.aws/knowledge-center/lambda-retrying-valid-sqs-messages>

upvoted 4 times

 **F_Eldin** 10 months, 3 weeks ago

Selected Answer: D

Option C, configuring scale-in protection for the instances during processing, is not directly related to the problem. Scale-in protection prevents instances from being terminated during an Auto Scaling event, but it does not address the issue of messages being moved to the dead-letter queue without successful processing.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-instance-protection.html>

I think D is tyoe and should read :

D. Update the redrive policy and set maxReceiveCount to 10.

upvoted 1 times

 **Parsons** 11 months, 2 weeks ago

Selected Answer: D

D should be "set maxReceiveCount to 10." It, Maybe a typo.

Explanation:

This setting ensures that any message that failed to be processed will be sent back to the queue to be picked up by other consumers and re-processed.

Why C is incorrect?

Well, the Auto Scaling group responds to the number of messages on the queue, scale-in protection is not cost-effective when there are no messages on the SQS queue.

upvoted 2 times

 **rbm2023** 10 months, 3 weeks ago

there are no errors in the application logs, this leave us to believe that the instances are being terminated by the auto scaling during the processing of the videos. any workaround in the SQS layer might not sove the problem

upvoted 2 times

 **pauloC** 11 months, 3 weeks ago

Selected Answer: C

I couldn't find SQS guidance for EC2 but there is for Lambda. We recommend setting your queue's visibility timeout to six times your function timeout, plus the value of MaximumBatchingWindowInSeconds . This allows time for your Lambda function to process each batch of events and to retry in the event of a throttling error.

I think you can apply this here as the process takes 30 minutes and 3 hours is 6X this.

<https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>

upvoted 1 times

Question #142

Topic 1

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access.

The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user.

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

- A. Create an internal Application Load Balancer (ALB). Create a target group. Select the Lambda function to call. Use the ALB DNS name to call the API from the VPC.
- B. Remove the DNS entry that is associated with the API in API Gateway. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone. Update the API in API Gateway with the CNAME record. Use the CNAME record to call the API from the VPC.
- C. Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.
- D. Deploy the Lambda functions inside the VPC. Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda functions. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

Correct Answer: D

Community vote distribution

C (100%)

✉  **zozza2023**  1 year, 2 months ago

Selected Answer: C

should be C as on the question has said 'no need for public IP' ==> private in API gateway = VPC endpoint
upvoted 9 times

✉  **bjexamprep**  4 months ago

Selected Answer: C

Bad question design. None of the answers is correct.
None of the answers mentions how to satisfy the requirement of "All APIs need to be called with an authenticated user".
Another requirement "make the set of APIs accessible only from a VPC". "the set" doesn't mean the whole set. Here "the set" means a part of the whole set.
A: The set of APIs are still publicly accessible.
B: Removing DNS entry doesn't remove the public accessibility.
C: This is making the whole set of APIs private. If this answer can be specific to "the set" APIs, this could be a good answer.
D: Using EC2 instances is always a bad answer.
upvoted 5 times

✉  **AimarLeo**  2 months, 1 week ago

All given answers are not ideal.. the closest one is C BUT.. .when mentioning the requirement to have only 'a set of API to be private' means 'not all'.. turning the endpoint from public to private will turn all to Private ,,, which is not fully correct as per the question.. I suppose the given answer or question missing an info.. or AWS starts playing with AI
upvoted 2 times

✉  **carpa_jo** 3 months, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>
upvoted 1 times

✉  **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C
upvoted 1 times

✉  **venvig** 7 months, 1 week ago

Selected Answer: C

Refer <https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/>
upvoted 1 times

✉  **Explorer_30** 7 months, 1 week ago

Answer is C as explained in <https://repost.aws/knowledge-center/api-gateway-vpc-connections>

upvoted 1 times

✉ **SK_Tyagi** 7 months, 3 weeks ago

Selected Answer: C

Regional to Private fits the use-case

upvoted 1 times

✉ **rtguru** 8 months, 3 weeks ago

the best possible answer from all the options is C

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

it's C, although it begs the questions about APIs that need to stay public...

upvoted 2 times

✉ **mfsec** 1 year ago

Selected Answer: C

C. Update the API endpoint from Regional to private in API Gateway.

upvoted 1 times

✉ **masetromain** 1 year, 2 months ago

Selected Answer: C

The correct answer is C. Update the API endpoint from Regional to private in API Gateway. Create an interface VPC endpoint in the VPC. Create a resource policy, and attach it to the API. Use the VPC endpoint to call the API from the VPC.

This solution will meet the requirements with the least amount of effort because it utilizes the built-in features of API Gateway and VPC to restrict access to the API. With this method, no additional infrastructure or configurations are necessary.

A and B are not correct because they would require additional infrastructure and configurations.

D is not correct because it would require provisioning an EC2 instance and installing an Apache server, introducing additional complexity and management overhead.

upvoted 3 times

✉ **zhangyu20000** 1 year, 2 months ago

C is correct

upvoted 1 times

Question #143

Topic 1

A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront.

The company recently expanded to serve users in the us-east-1 Region, and these new users report that viewing their respective weather maps is slow from time to time.

Which combination of steps will resolve the us-east-1 performance issues? (Choose two.)

- A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
- B. Create a new S3 bucket in us-east-1. Configure S3 cross-Region replication to synchronize from the S3 bucket in eu-west-1.
- C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
- D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.
- E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution. Use Lambda@Edge to modify requests from North America to use the new origin.

Correct Answer: BD

Community vote distribution



✉️ **sambb** Highly Voted 1 year, 1 month ago

Selected Answer: BD

A: Global Accelerator can't have an s3 bucket as endpoint
 C: People are complaining about time to retrieve maps. Transfert acceleration is used to accelerate PUT requests to an s3 bucket located in a distant region.
 E: An accelerator as cloudfront origin does not make much sense, because cloudfront is already using the AWS network. Global Accelerator is usually for Layer 4 networking and/or static anycast IPs
 upvoted 14 times

✉️ **masetromain** Highly Voted 1 year, 2 months ago

Selected Answer: BD

B is correct because it involves creating a new S3 bucket in the us-east-1 region and configuring cross-Region replication to synchronize from the existing S3 bucket in eu-west-1. This will allow users in us-east-1 to access the weather maps from a closer location, improving performance.
 D is correct because it involves using Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1. This will also allow users in us-east-1 to access the weather maps from a closer location, improving performance.

A and E are not correct because they do not involve creating a new S3 bucket in us-east-1, which is necessary for improving performance for the users in that region. C is not correct because it involves using the S3 Transfer Acceleration endpoint, which is a different service and not necessary for this scenario.

upvoted 6 times

✉️ **pangchn** Most Recent 5 days, 19 hours ago

Selected Answer: BD

BD
 C using S3 Transfer Acceleration is good but this answer option itself is wrong due to the statement that pointing to a regional endpoint, where it doesn't exist. Once enable, it is just a global endpoint URL
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration-examples.html>
 upvoted 1 times

✉️ **jpa8300** 3 months ago

Selected Answer: AC

If you want to improve latency , you always look for Global Accelerator fro the readings and Transfer accelerator for the updates.
 Yes, it is possible to configure AWS Global Accelerator to distribute traffic from an S3 bucket in one AWS Region (eu-west-1) to endpoint groups in another AWS Region (us-east-1) for TCP ports 80 and 443. This configuration can be useful for improving the performance and availability of your S3 bucket for users in both regions.
 This way you save money in the storage, you don't need to duplicate the storage. And for persons that chose option D, if you update the bucket there, those objects will not be replicated to the other region since replication works only in one way.
 upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: BD

Option B & D

upvoted 1 times

 **bjexamprep** 4 months ago

Selected Answer: BD

This is not a good question design. Does that mean the application use CloudFront in EU and does not use CloudFront in the US? How weird it is!!!

upvoted 3 times

 **Jrhp** 4 months, 1 week ago

Selected Answer: BD

Exactly case from this blog post <https://aws.amazon.com/blogs/networking-and-content-delivery/dynamically-route-viewer-requests-to-any-origin-using-lambdaedge/>

upvoted 4 times

 **rtguru** 8 months, 3 weeks ago

BD, I was initially looking at BE, I think global accelerator is used more for write requests.

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: BD

BD makes more sense

upvoted 2 times

 **SmileyCloud** 9 months, 1 week ago

Selected Answer: BD

<https://godof.cloud/dynamic-origin-s3-spa/>

Use case

upvoted 1 times

 **Eshu2009** 1 year ago

BE- global accelerators improve performance by providing edge location for onboarding traffic.

upvoted 3 times

 **Eshu2009** 1 year ago

Q: Can I use AWS Global Accelerator for object storage with Amazon S3?

A: You can use Amazon S3 Multi-Region Access Points to get the benefits of Global Accelerator for object storage. S3 Multi-Region Access Points use Global Accelerator transparently to provide a single global endpoint to access a data set that spans multiple S3 buckets in different AWS Regions. This allows you to build multi-region applications with the same simple architecture used in a single region, and then to run those applications anywhere in the world. Application requests made to an S3 Multi-Region Access Point's global endpoint automatically route over the AWS global network to the S3 bucket with the lowest network latency. This allows applications to automatically avoid congested network segments on the public internet, improving application performance and reliability.

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: BD

I'll go with BD

upvoted 1 times

 **kiran15789** 1 year, 1 month ago

Selected Answer: BD

Since only one additional region we don't need global accelerators

upvoted 4 times

 **bititan** 1 year, 1 month ago

Selected Answer: BC

S3 transfer acceleration is more efficient

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: BD

A and E are not correct as there isn't a need to use AWS Global Accelerator

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

BD is correct

upvoted 1 times

Question #144

Topic 1

A solutions architect is investigating an issue in which a company cannot establish new sessions in Amazon Workspaces. An initial analysis indicates that the issue involves user profiles. The Amazon Workspaces environment is configured to use Amazon FSx for Windows File Server as the profile share storage. The FSx for Windows File Server file system is configured with 10 TB of storage.

The solutions architect discovers that the file system has reached its maximum capacity. The solutions architect must ensure that users can regain access. The solution also must prevent the problem from occurring again.

Which solution will meet these requirements?

- A. Remove old user profiles to create space. Migrate the user profiles to an Amazon FSx for Lustre file system.
- B. Increase capacity by using the update-file-system command. Implement an Amazon CloudWatch metric that monitors free space. Use Amazon EventBridge to invoke an AWS Lambda function to increase capacity as required.
- C. Monitor the file system by using the FreeStorageCapacity metric in Amazon CloudWatch. Use AWS Step Functions to increase the capacity as required.
- D. Remove old user profiles to create space. Create an additional FSx for Windows File Server file system. Update the user profile redirection for 50% of the users to use the new file system.

Correct Answer: C

Community vote distribution



⊕ **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/cli/latest/reference/fsx/update-file-system.html>
EventBridge invoking lambda to update settings will prevent too from occurring again
upvoted 6 times

⊕ **masetromain** 1 year, 2 months ago

Selected Answer: B

B is correct. It can prevent the issue from happening again by monitoring the file system with the FreeStorageCapacity metric in Amazon CloudWatch and using Amazon EventBridge to invoke an AWS Lambda function to increase the capacity as required. This ensures that the file system always has enough free space to store user profiles and avoids reaching maximum capacity.
A: Removing old user profiles may not be sufficient to create enough space and does not prevent the problem from happening again.
C: AWS Step Functions cannot be used to increase capacity, it is a service for creating and running workflows that stitch together multiple AWS services.
D: Creating an additional FSx for Windows File Server file system and updating user profile redirection for a portion of the users may not be sufficient to prevent the problem from happening again and does not address the current capacity issue.
upvoted 6 times

⊕ **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B
upvoted 1 times

⊕ **rtguru** 8 months, 3 weeks ago

B is the correct answer
upvoted 1 times

⊕ **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

it's B
upvoted 1 times

⊕ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword == update-file-system
upvoted 1 times

⊕ **leehjworking** 10 months, 3 weeks ago

Selected Answer: C

Is it necessary to implement new cloudwatch metric? And using step functions seems to be able to increase storage capacity, according to the following reference.

<https://docs.aws.amazon.com/step-functions/latest/dg/supported-services-awssdk.html#supported-services-awssdk-list>

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

Perhaps the metric is used to trigger the step functions

upvoted 1 times

✉️ **OCHT** 11 months, 2 weeks ago

Selected Answer: D

B. Increasing capacity using the update-file-system command is not applicable to FSx for Windows File Server. The command is for Amazon EFS, not FSx for Windows File Server.

upvoted 1 times

✉️ **rbm2023** 10 months, 3 weeks ago

StorageCapacity

Use this parameter to increase the storage capacity of an FSx for Windows File Server, FSx for Lustre, FSx for OpenZFS, or FSx for ONTAP file system. Specifies the storage capacity target value, in GiB, to increase the storage capacity for the file system that you're updating.

https://docs.aws.amazon.com/fsx/latest/APIReference/API_UpdateFileSystem.html

Example using the CLI

`aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --storage-capacity 10240`

upvoted 4 times

✉️ **yama234** 11 months, 2 weeks ago

B

As you need additional storage, you can increase the storage capacity that is configured on your FSx for Windows File Server file system. You can do so using the Amazon FSx console, the Amazon FSx API, or the AWS Command Line Interface (AWS CLI).

upvoted 3 times

✉️ **Cloud_noob** 12 months ago

Selected Answer: B

<https://chat.openai.com/chat>

upvoted 2 times

✉️ **mfsec** 1 year ago

Selected Answer: B

B is correct

upvoted 2 times

✉️ **zozza2023** 1 year, 2 months ago

Selected Answer: B

B seems to be the correct answer.

the unique possible solution is to add storage capacity using CLI

upvoted 4 times

✉️ **pitakk** 1 year, 2 months ago

Selected Answer: B

To increase the storage capacity for an FSx for Windows File Server file system, use the AWS CLI command update-file-system.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-capacity.html> It's B.

upvoted 2 times

✉️ **zhangyu20000** 1 year, 2 months ago

B is correct. It can prevent issue happen again with EventBridge and Lambda

A: not make sense at all

C: Cannot use Step Function to increase capacity

D: not prevent happen again

upvoted 2 times

Question #145

Topic 1

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues in response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance. Create an Auto Scaling group of EC2 instances behind an Application Load Balancer. Configure the Auto Scaling group to have a minimum of three instances.
- B. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance. Point the EC2 instance to the new path for file processing.
- C. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.
- D. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function. Configure the Lambda function to add the metadata and update the delivery system.

Correct Answer: B

Community vote distribution

C (77%)

B (23%)

 **masetromain**  1 year, 2 months ago

Selected Answer: C

C is correct. Using AWS Transfer Family to create an FTP server that places the files in Amazon S3 and using S3 event notifications through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function will ensure that the archive always receives the files and that the central system is always updated. This solution maximizes scalability and eliminates the need for manual intervention, such as rebooting the EC2 instance.

Option A and B still use EC2 instance, which is the source of the problem. Option D requires modification to the handheld devices which is not possible.

upvoted 12 times

 **venvig**  7 months, 1 week ago

Selected Answer: B

I agree that "C" is the ideal design.

But here the question states that :

Ec2 instance is running the SFTP server.

File is uploaded from handheld devices to a file system in the Ec2 instance.

The Ec2 instance then adds metadata to the file.

The file is then placed in s3.

The condition states that:

The company cannot deploy a new application.

Based on the condition, if I use lambda to add meta data, then its like deploying a new application.

(We don't know if the application can be seamlessly rewritten in lambda. Will it finish under 15 mins ? etc.,)

If we strictly interpret this as not being able to introduce any new logic or components (like a Lambda function for metadata processing), then Option (B) is the answer.

Option B essentially replaces the FTP server with AWS Transfer Family and uses Amazon EFS as the file storage, which can scale and handle more connections. The existing EC2 instance, which already has the logic for metadata addition, would simply point to this new file path on EFS. This minimizes changes to the existing application logic.

upvoted 6 times

 **kgcain** 5 months, 2 weeks ago

From the app description, I am sure that it should work under 15min.

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

the text is: "The handheld devices cannot be modified, so the company cannot deploy a new application". Following your comment, you can't use neither the AWS Transfer Family. This is also new :D

upvoted 1 times

 **EApeer** **Most Recent** 2 weeks, 2 days ago

B is the best answer. The system is such that each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. This means that we need a file storage that the data are stored hierarchically in a top-down network of folders. And a file system that has adaptive throughput to resolve the dropped connections and memory issues. EFS will be the suitable solution component. S3 however has all the data stored on the same flat plane requiring more comprehensive metadata (labels) to make it manageable.

upvoted 1 times

 **kz407** 2 weeks, 4 days ago

Selected Answer: C

It says "so the company cannot deploy a new application".

This means that it's the handheld devices they can't deploy a new application into. While B works, It still relies on one EC2 instance, which is a part of the problem.

upvoted 1 times

 **gofavad926** 3 weeks, 2 days ago

Selected Answer: C

C, transfer family + S3

upvoted 1 times

 **zanhsieh** 2 months ago

Selected Answer: C

C.

A: No. FTP is not HTTP / HTTPS. FTP -> NLB. HTTP / HTTPS -> ALB.

B: No. This needs extra steps (DataSync?) to move to S3, and the billing team would still complain about not always updated since it will be certain lag-behind time.

C: Correct.

D: No. S3 event notification can directly trigger Lambda.

upvoted 1 times

 **JMAN1** 3 months, 1 week ago

Selected Answer: C

C. does not require handheld device to be changed. And it solves EC2 dropped Connection by using S3.

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **Chung234** 5 months, 3 weeks ago

Selected Answer: B

The answer is A.

Q: Can I use FTP with an internet-facing endpoint?

A: No, when you enable FTP, you will only be able to use VPC hosted endpoint's internal access option. If traffic needs to traverse the public network, secure protocols such as SFTP or FTPS should be used.

Source: <https://aws.amazon.com/aws-transfer-family/faqs/>

upvoted 2 times

 **ele** 1 month, 1 week ago

ALB is a load balancer that operates at Layer 7. Only HTTP and HTTPS can be used as ALB protocols.
Therefore, it is not possible to set ALB at the front of the FTP server.

upvoted 1 times

 **rtguru** 8 months, 3 weeks ago

This one of those tricky questions. I'm not sure if to go with A or C

upvoted 1 times

 **rrrrrrrrr1** 9 months ago

IDK yall, it does say clearly "cannot deploy a new application" and the only instance of that is A.

I Agree C is better but IDK the semantics here

upvoted 1 times

✉  **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

its a c

upvoted 1 times

✉  **Maria2023** 9 months, 3 weeks ago

Selected Answer: C

Since AWS Transfer Family supports Amazon S3 Access Point then it's a standard scenario - FTP->S3->Event->Lambda. Scalable and serverless

upvoted 2 times

✉  **Jackhemo** 9 months, 3 weeks ago

Selected Answer: C

olabiba.ai says C.

1. Scalability: By using AWS Transfer Family to create an FTP server that places the files directly in Amazon S3, you can leverage the scalability and durability of S3. S3 is designed to handle high volumes of data and can scale seamlessly as your company expands.

2. Reliability: With S3 as the destination for the files, you can ensure that the archive always receives the files. S3 provides high durability and availability, reducing the chances of data loss.

3. System updates: By using an S3 event notification through Amazon SNS, you can trigger an AWS Lambda function whenever a new file is uploaded to S3. This Lambda function can then add the necessary metadata and update the delivery system, ensuring that the central system is always updated.

4. No modification to handheld devices: Since the handheld devices cannot be modified, this solution allows the devices to continue uploading files through FTP. The only change is the destination, which is now the S3 bucket.

upvoted 1 times

✉  **mfsec** 1 year ago

Selected Answer: C

C is the most efficient

upvoted 3 times

✉  **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is correct

upvoted 3 times

✉  **zhangyu20000** 1 year, 2 months ago

C is correct

upvoted 2 times

Question #146

Topic 1

A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost.

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

- A. Provision an Aurora Replica in a different Region.
- B. Set up AWS DataSync for continuous replication of the data to a different Region.
- C. Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the data to a different Region.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule a snapshot every 5 minutes.

Correct Answer: A

Community vote distribution

A (100%)

 **masetromain**  1 year, 2 months ago

Selected Answer: A

A is correct. Provision an Aurora Replica in a different Region will meet the requirement of the application being able to recover to a separate AWS Region in the event of an application failure, and no data can be lost, with the least amount of operational overhead.

- B. AWS DataSync can replicate data, but it is not a fully managed service and requires more configuration and management.
- C. AWS DMS is a fully managed service for migrating data between databases, but it may require additional configuration and management to continuously replicate data in real-time.
- D. Amazon DLM can be used for scheduling snapshots, but it does not provide real-time replication and may not meet the requirement of no data loss in case of a failure.

upvoted 7 times

 **career360guru**  3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

its an A

upvoted 2 times

 **Goatin** 10 months, 3 weeks ago

When you provision an Aurora Replica in a different AWS Region, the replica is kept in sync with the primary database using Aurora's replication capabilities. In the event of a failure in the primary Region, you can promote the Aurora Replica to become the new primary database, which allows you to continue operations with no data loss.

However, provisioning and maintaining an Aurora Replica in a different AWS Region requires ongoing management and monitoring to ensure that it stays in sync with the primary database

upvoted 3 times

 **mfsec** 1 year ago

Selected Answer: A

Replica

upvoted 4 times

 **God_Is_Love** 1 year, 1 month ago

Selected Answer: A

B,C are on premises usecase solutions. D is wrong because 5 minute worth of data could be lost against the requirement. So A is correct. In fact replica works as standby if primary DB fails.

upvoted 4 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 4 times

 **zhangyu20000** 1 year, 2 months ago

- A is correct
- B: cannot use DataSync for Aurora backup
- C: too complex
- D: DLM is for EBS backup. Here use managed Aurora server, no access to EBS

upvoted 2 times

Question #147

Topic 1

A financial services company receives a regular data feed from its credit card servicing partner. Approximately 5,000 records are sent every 15 minutes in plaintext, delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption. This feed contains sensitive credit card primary account number (PAN) data. The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing. The company also needs to remove and merge specific fields, and then transform the record into JSON format. Additionally, extra feeds are likely to be added in the future, so any design needs to be easily expandable.

Which solutions will meet these requirements?

- A. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Invoke another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3. Invoke a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing.
- B. Invoke an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue. Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages. Have the application process each record, and transform the record into JSON format. When the queue is empty, send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance.
- C. Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match. Invoke an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, have the ETL job send the results to another S3 bucket for internal processing.
- D. Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match. Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements. Define the output format as JSON. Once complete, send the results to another S3 bucket for internal processing and scale down the EMR cluster.

Correct Answer: C

Community vote distribution

C (100%)

 **God_Is_Love**  1 year, 1 month ago

Selected Answer: C

Extract Data from S3 + mask + Send to another S3 + Transform/Process + Load into S3
All these are ETL, ELT tasks which should ring Glue

EMR is more focused on big data processing frameworks such as Hadoop and Spark,
while Glue is more focused on ETL, More over 5000 records every 15 minutes is not sooo big data..So I choose C
upvoted 18 times

 **tycho** 12 months ago

EMR and Glue are the same; Glue is managed cluster by AWS , EMR customer manages the clutster
upvoted 1 times

 **masetromain**  1 year, 2 months ago

Selected Answer: C

C is correct. It will process the data in batch mode using Glue ETL job which can handle large amount of data and can be scheduled to run periodically. This solution is also easily expandable for future feeds.

A: It uses multiple Lambda functions, SQS queue and S3 temporary location which will increase operational overhead.
B: Using Fargate may not be the most cost-effective solution and also it may not handle large amount of data.
D: Athena and EMR both are powerful tools but they are more complex and can be more costly than Glue.
upvoted 6 times

 **career360guru**  3 months, 2 weeks ago

Selected Answer: C

Option C
upvoted 1 times

 **totten** 6 months, 1 week ago

Selected Answer: C

Option C is the most suitable solution for the described scenario:

- 1) AWS Glue Crawler and Custom Classifier: Use AWS Glue to create a crawler and custom classifier to understand and catalogue the data feed formats. This step ensures that AWS Glue can work with the incoming data effectively.
- 2) AWS Glue ETL Job: Create an AWS Lambda function that triggers an AWS Glue ETL job when a new data file is delivered. This ETL job can perform the required transformation, including masking, field removal, and converting records to JSON format. AWS Glue is a suitable service for data preparation and transformation.
- 3) Output to S3 Bucket.

This approach is scalable, easily expandable to handle additional feeds in the future, and leverages AWS Glue's capabilities for data transformation and processing. It also maintains a clear separation of tasks, making it a robust and efficient solution for the given requirements.

upvoted 2 times

 **dkcloudguru** 7 months ago

C is the good option EMR(Big data, Spark, Hadoop) is for near real-time data processing and it isn't a good fit in this case

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

its a C

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: C

EMR is big data but not is need in this case
then AWS Glue + Lambdas + S3 is good option
C

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: C

C makes the most sense.

upvoted 2 times

 **Musk** 1 year, 2 months ago

The question is at what point Athena and EMR are a better choice because it is a lot of data to store and process

upvoted 1 times

 **Sarutobi** 1 year, 1 month ago

That, I agree. Honestly, I will use it from day one, regardless.

upvoted 1 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: C

C is correct.

upvoted 4 times

 **zhangyu20000** 1 year, 2 months ago

C is correct

upvoted 1 times

Question #148

Topic 1

A company wants to use AWS to create a business continuity solution in case the company's main on-premises application fails. The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company's on-premises applications use operating systems that are compatible with Amazon EC2.

Which solution will achieve the company's goal with the LEAST operational overhead?

- A. Install the AWS Replication Agent on the source servers, including the MySQL servers. Set up replication for all servers. Launch test instances for regular drills. Cut over to the test instances to fail over the workload in the case of a failure event.
- B. Install the AWS Replication Agent on the source servers, including the MySQL servers. Initialize AWS Elastic Disaster Recovery in the target AWS Region. Define the launch settings. Frequently perform failover and fallback from the most recent point in time.
- C. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the database. Create a DMS replication task to copy the existing data to the target DB cluster. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized. Install the rest of the software on EC2 instances by starting with a compatible base AMI.
- D. Deploy an AWS Storage Gateway Volume Gateway on premises. Mount volumes on all on-premises servers. Install the application and the MySQL database on the new volumes. Take regular snapshots. Install all the software on EC2 Instances by starting with a compatible base AMI. Launch a Volume Gateway on an EC2 instance. Restore the volumes from the latest snapshot. Mount the new volumes on the EC2 instances in the case of a failure event.

Correct Answer: C

Community vote distribution



✉️ **kexybelo** 4 months ago

Selected Answer: B

itexamstest.com

no discussion B :)

upvoted 26 times

✉️ **hedylyru** 3 months, 4 weeks ago

Very helpful exam dumps for the aws certification exam.

upvoted 1 times

✉️ **GoKhe** 3 months, 3 weeks ago

which one? I am not able to open itexamstest.com if you meant it.

upvoted 1 times

✉️ **God_Is_Love** 1 year, 1 month ago

Selected Answer: B

Tricky one. This is not an on premise migration use case which prompts for answer C. Its a current situation of on premise application which the company wants to continue its state in the requirement of using AWS as DR solution.

<https://docs.aws.amazon.com/images/drs/latest/userguide/images/drs-failback-arc.png>

<https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html>

upvoted 21 times

✉️ **God_Is_Love** 1 year, 1 month ago

Moreover, B has least operational overhead of just initiating DR solution with replicating agents. C has operational overhead with DMS , SCT ,CDC,migration etc

upvoted 4 times

✉️ **swadeey** 4 months ago

I also agreed with the answer but then see this "The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store" just database and physical server has other applications which not mentioned. Also from DR the statement gets changed to Migrate

upvoted 1 times

✉️ **ninomfr64** 2 months, 2 weeks ago

Selected Answer: B

A = to use AWS DRS you first need to set it up in each AWS Region in which you want to use it. installing AWS Replication agent is not enough
B = correct (to me the sentence "Frequently perform failover and fallback from the most recent point in time" is ambiguous as this points to

actual failover/failback and not to drills)

C = SCT is not needed with same engine db migration. also, install the rest of the software is not enough for app DR

D = Volume Gateway can be used in a Back and Restore DR scenario, but the option D is very confused. Anyway, Storage Gateway for DR requires more overhead with respect to AWS DRS

upvoted 2 times

✉ **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B is right option.

Option C only addresses DB instance replication and DR, it does not meet requirements of replicating other applications running on on-premise.

upvoted 1 times

✉ **swadeey** 4 months ago

Selected answer C changed from B

The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store.

upvoted 1 times

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

Selected Answer: B

Elastic Disaster Recovery does the job

upvoted 1 times

✉ **AMohanty** 7 months, 1 week ago

C

We are looking for a Business Continuity Solution

Meaning RTO should be low

upvoted 1 times

✉ **chikorita** 7 months ago

but how is failover happening

the very own purpose of DR is its automatic failover which is supported by option B

upvoted 1 times

✉ **cmoreira** 7 months, 1 week ago

Selected Answer: B

Answer is B.

Questions mentions "least operational overhead" (efforts in the future), and B mentions "Frequently performing...".

However, that is the best-practice for AWS DR (as misleading as it sounds):

<https://docs.aws.amazon.com/drs/latest/userguide/failback-overview.html>

upvoted 1 times

✉ **Gabehcoud** 7 months, 2 weeks ago

Selected Answer: B

the question is a bit misleading, first part says "company is planning for business continuity" the later part of the sentence says "applications are migrating".

nevertheless, we should focus on the word business continuity. Going by that "no migration" is required so choose B.

that is my analysis.

upvoted 3 times

✉ **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

B for BC

upvoted 1 times

✉ **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword = AWS Elastic Disaster Recovery

B

upvoted 1 times

✉ **rbm2023** 10 months, 3 weeks ago

Selected Answer: B

The company is looking for a disaster recovery solution and not a full migration to cloud. In my view the answer should use Elastic Disaster Recovery and not DMS.

References

<https://www.cloudthat.com/resources/blog/scalable-cost-effective-cloud-disaster-recovery-with-aws-drs-elastic-disaster-recovery>

<https://catalog.us-east-1.prod.workshops.aws/workshops/080af3a5-623d-4147-934d-c8d17daba346/en-US/introduction>

https://docs.aws.amazon.com/pt_br/mgn/latest/ug/Network-Settings-Video.html

upvoted 2 times

✉ **OCHT** 11 months, 2 weeks ago

Selected Answer: C

it appears that option C has the least operational overhead since it involves creating AWS DMS replication servers and a target Amazon Aurora MySQL DB cluster to host the database, creating a DMS replication task to copy existing data to the target DB cluster, creating a local AWS SCT CDC task to keep data synchronized, and installing the rest of the software on EC2 instances by starting with a compatible base AMI. The other options involve additional steps such as setting up replication for all servers (option A), initializing AWS Elastic Disaster Recovery and frequently performing failover and fallbacks (option B), or deploying an AWS Storage Gateway Volume Gateway and mounting volumes on all on-premises servers (option D).

upvoted 3 times

✉ **dev112233xx** 1 year ago

Selected Answer: C

C seems correct to me (DMS with SCT and CDC)

upvoted 1 times

✉ **mfsec** 1 year ago

Selected Answer: B

B has less operational overhead.

upvoted 3 times

✉ **taer** 1 year ago

Selected Answer: B

B, tricky

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

Selected Answer: B

<https://aws.amazon.com/disaster-recovery/>

upvoted 3 times

Question #149

Topic 1

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS account. Assign a unique external ID to the resource policy.
- B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.
- C. In the company's AWS account, create an IAM user. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user. Share the access keys with the auditors.
- D. In the company's AWS account, create an IAM group that has the required permissions. Create an IAM user in the company's account for each auditor. Add the IAM users to the IAM group.

Correct Answer: B

Community vote distribution

B (100%)

 **tatdatpham**  1 year, 2 months ago

Selected Answer: B

Option B is the best solution. This solution creates an IAM role that trusts the auditors' AWS account and attaches the required IAM policies to the role. This ensures that the auditors have read-only access to the company's AWS account while ensuring that the company's AWS account is secure and complies with AWS security best practices. Additionally, the unique external ID assigned to the role's trust policy adds an extra layer of security.

upvoted 7 times

 **duriselvan**  1 month, 2 weeks ago

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

upvoted 1 times

 **duriselvan** 1 month, 2 weeks ago

To create an IAM role that trusts the auditors' AWS account, you can do the following:

Sign in to the AWS Management Console and open the IAM console.

In the navigation pane, choose Roles, and then choose Create role.

Choose the Custom trust policy role type.

In the Custom trust policy section, enter or paste the following trust policy:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::<auditor-account-id>:root"
},
>Action": "sts:AssumeRole"
}
]
}
```

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **dkcloudguru** 7 months ago

B is correct

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

its a b

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

In the company's AWS account, create an IAM role that trusts the auditors' AWS account.

upvoted 3 times

 **zozza2023** 1 year, 2 months ago

Selected Answer: B

B seems to be the right answer

upvoted 3 times

 **masetromain** 1 year, 2 months ago

Selected Answer: B

The correct answer is B. In the company's AWS account, create an IAM role that trusts the auditors' AWS account. Create an IAM policy that has the required permissions. Attach the policy to the role. Assign a unique external ID to the role's trust policy.

This solution meets the requirement of providing the external auditors with secure, read-only access to the company's AWS account while also complying with AWS security best practices. In this solution, an IAM role is created that trusts the auditors' AWS account and has an IAM policy with the required permissions attached to it. The role's trust policy should include a unique external ID for added security. This allows the external auditors to assume the role and access the resources with the permissions specified in the policy, without the need to share access keys or create individual IAM users for each auditor.

upvoted 3 times

 **masetromain** 1 year, 2 months ago

Option A is incorrect because it grants access to all resources in the company's AWS account and does not provide a way to restrict the permissions that the external auditors have.

Option C is incorrect because it creates an IAM user in the company's account and shares the API access keys with the external auditors, which is not secure and does not comply with AWS security best practices.

Option D is incorrect because it creates an IAM user in the company's account for each auditor, which would be tedious and difficult to manage for the company. It would be more secure and efficient to use an IAM role that trusts the auditors' AWS account instead of creating individual users for each auditor.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

B is correct

upvoted 2 times

Question #150

Topic 1

A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.

Which solution will meet these requirements with the LEAST latency?

- A. Create a two-node DynamoDB Accelerator (DAX) cluster. Configure an application to read and write data by using DAX.
- B. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
- C. Create a three-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
- D. Create a single-node DynamoDB Accelerator (DAX) cluster. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.

Correct Answer: A

Community vote distribution

B (90%) 10%

✉️ **Untamables** 1 year, 2 months ago

Selected Answer: B

3 nodes are required for a DAX cluster to be fault-tolerant.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.concepts.cluster.html>

upvoted 15 times

✉️ **Ganshank** 7 months, 2 weeks ago

This is a poorly framed question with very little attention to how applications are architected in real life. Here's my reasoning:
This being a trading platform, you have a high volume of writes and reads, and stale data is essentially worse than useless. This automatically eliminates all but A, because of the way DAX performs. DAX caches data from the first query, and subsequent queries will continue to receive that cached data regardless of whether it has been updated in DynamoDB. This behavior continues till cache eviction. The only way around it is to read and write data using DAX.

Here's the curveball - the solution must be HA, which eliminates A and D, leaving only B & C. And between B & C, you really want to use DAX for reading and DynamoDB for writing. So final answer is B - if you want to get certified.

Applying this solution in real world however will cause you a lot of pain and grief!

upvoted 10 times

✉️ **jainparag1** 4 months, 2 weeks ago

Caching in DAX is always write through. Correct answer is B.

upvoted 2 times

✉️ **frfavoreto** 6 months, 4 weeks ago

Totally agree.

But an additional issue with the question is the fact that it requires High Availability, not Fault Tolerance. These are quite different concepts and, at least up to this point, there would be no need for 3x DAX instances (in theory).

upvoted 1 times

✉️ **saggy4** 1 month, 3 weeks ago

Selected Answer: B

DAX is cache and can only be used to read so A and C are out.

Between B and D the question says Highly Available so we will select B (three node) instead of D (single node).

So correct answer B

upvoted 2 times

✉️ **ninomfr64** 2 months, 2 weeks ago

A = 2 nodes DAX is not fault-tolerant

B = correct (write-around strategy ensure lower latency)

C = write-through strategy can have higher latency

D = 1 node DAX is not fault-tolerant

upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

Selected Answer: B

Option B is the best option. Though Option A is also possible solution.

upvoted 1 times

✉ **MRamos** 4 months ago

Selected Answer: B

The breakpoint is latency.

You write through DAX, but for latency sensitive apps, AWS instruct write directly on DynamoDB instead on DAX.

"For applications that are sensitive to latency, writing through DAX incurs an extra network hop. So a write to DAX is a little slower than a write directly to DynamoDB. If your application is sensitive to write latency, you can reduce the latency by writing directly to DynamoDB instead. For more information, see Write-around."

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.consistency.html#DAX.consistency.strategies-for-writes>

upvoted 1 times

✉ **amarbeg** 4 months, 1 week ago

Option A would be the least latency solution for this use case. Using a two node DAX cluster with the application reading and writing via DAX provides:

Caching of both reads and writes within the DAX cluster nodes. This eliminates the need to go directly to DynamoDB for reads and writes, reducing latency.

Redundancy with two nodes to ensure high availability of the cache.

The other options would lead to some reads or writes still going directly to DynamoDB rather than being fully served from the lower latency cached data in DAX. This could increase latency compared to option A. A single node DAX cluster would work but lacks the redundancy needed for high availability.

DAX is fully managed, in-memory cache for DynamoDB that delivers low-latency data access. By caching the entire dataset in-memory across nodes, it can serve requests much faster than going to the DynamoDB tables on every request. The AWS documentation provides more details on how to configure DAX and monitor latency metrics.

upvoted 1 times

✉ **covabix879** 6 months, 1 week ago

Selected Answer: A

Question only ask for High Availability, not Fault Tolerant. You need 3 nodes only for the latter. You must write through to keep data getting stale as mentioned by Ganshank. I would go with two-node cluster as strong consistency adds extra latency as number of clusters increase. So for this question best answer should be A.

upvoted 1 times

✉ **dkcloudguru** 7 months ago

Option B is correct: DAX is also used for caching so it improves the performance and for production 3 nodes are strongly recommended so I'll go with B.

upvoted 2 times

✉ **duriSelvan** 7 months ago

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

upvoted 1 times

✉ **duriSelvan** 7 months ago

sorry guys A is wrong ans: B is correct ans Important

For production usage, we strongly recommend using DAX with at least three nodes, where each node is placed in different Availability Zones. Three nodes are required for a DAX cluster to be fault-tolerant.

A DAX cluster can be deployed with one or two nodes for development or test workloads. One- and two-node clusters are not fault-tolerant, and we don't recommend using fewer than three nodes for production use. If a one- or two-node cluster encounters software or hardware errors, the cluster can become unavailable or lose cached data.

upvoted 1 times

✉ **duriSelvan** 7 months ago

A is Ans :

Read replicas serve two additional purposes:

Scalability. If you have a large number of application clients that need to access DAX concurrently, you can add more replicas for read-scaling. DAX spreads the load evenly across all the nodes in the cluster. (Another way to increase throughput is to use larger cache node types.)

High availability. In the event of a primary node failure, DAX automatically fails over to a read replica and designates it as the new primary. If a replica node fails, other nodes in the DAX cluster can still serve requests until the failed node can be recovered. For maximum fault tolerance, you should deploy read replicas in separate Availability Zones. This configuration ensures that your DAX cluster can continue to function, even if an entire Availability Zone becomes unavailable.

upvoted 1 times

✉ **AMohanty** 7 months, 1 week ago

A

Once you enable DAX you can't directly write onto or Read from Dynamo DB.

upvoted 2 times

✉ **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 1 times

✉️ **Just_Ninja** 9 months ago

Selected Answer: B

AWS recommend 3 nodes for production workloads.

So it must B

upvoted 1 times

✉️ **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

B for DAX HA

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

Selected Answer: B

DAX is used mostly to accelerate data reading, so that leaves us with B and D, Fault tolerance leaves B as the right choice

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

Start Learning for free